

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335



AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

CENTRALNY OŚRODEK SZKOLENIA
im. gen. dyw. Stefana Roweckiego „GROTA”

**PRZEGLĄD
BEZPIECZEŃSTWA
WEWNĘTRZNEGO**

WARSZAWA 18 (10) 2018

Rada naukowa

prof. dr hab. Brunon Hołyst
dr hab. Krzysztof Indecki
dr hab. Jerzy Konieczny
prof. dr hab. Andrzej Mania
dr hab. Stanisław Sulowski
prof. dr hab. Sebastian Wojciechowski
prof. dr hab. Konstanty A. Wojtaszczyk

Recenzenci PBW 18

dr hab. Robert Borkowski
dr hab. Krzysztof Kociubiński
dr Rafał Leśkiewicz
dr hab. Ryszard Machnikowski
prof. dr hab. Piotr Majer
dr Krzysztof Malesa
prof. dr hab. Andrzej Misiuk
dr hab. Bronisław Młodziejowski
dr Witold Ostant
dr hab. Waldemar Zubrzycki

**INTERNAL
SECURITY
REVIEW**

WARSAW 18 (10) 2018

Zespół redakcyjny Anna Przyborowska (redaktor naczelna)
Elżbieta Dąbrowska (sekretarz Redakcji)
Anna Przyborowska, Grażyna Osuchowska
(redakcja, korekta)
Izabela Laskus, Radosław Kostyra (skład)

Przekład artykułów na język angielski:

Joanna Dębowska
Anna Łasińska
Marek Świerczek

**© Copyright by Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota”
Emów 2018**

ISSN 2080-1335

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane
All the articles published in the magazine are subject to reviews

Deklaracja o wersji pierwotnej:

Wersja drukowana czasopisma jest jego wersją pierwotną

Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

„Przegląd Bezpieczeństwa Wewnętrznego” (PBW) znajduje się na liście czasopism naukowych Ministra Nauki i Szkolnictwa Wyższego z liczbą 5 punktów za umieszczone w nim publikacje. PBW można odnaleźć także w *Index Copernicus Journal Master List* z liczbą 48,72 punktów. Czasopismo jest również dostępne w bazach: *Central European Journal of Social Science and Humanities* i Polska Bibliografia Naukowa (PBN).

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota” w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

Redakcja

tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 645
e-mail: redakcja.pbw@abw.gov.pl
www.abw.gov.pl

Numer zamknięto i oddano do druku w marcu 2018 r.

Druk: Biuro Logistyki
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 22 58 57 657

SPIS TREŚCI TABLE OF CONTENTS

I. ARTYKUŁY I ROZPRAWY

Andrzej Krzak

Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego 11

Jolanta Darczewska

Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy 40

Danuta Gibas-Krzak

Rosyjska koncepcja Eurazjatyckiego Systemu Obrony Powietrzno-Kosmicznej. Analiza problemu 68

II. STUDIA I ANALIZY

Anna Łasińska

Wybrane techniki obrazowania stosowane w kryminalistyce 89

Sławomir Gładysz

Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego 120

Marcin Gołaszewski, Paulina Markowicz, Justyna Jastrzębska

Postrzeżenie badań poligraficznych w Polsce oraz ich użyteczność w służbach i innych obszarach działalności 151

Marek Świerczek

Wewnętrzne źródła porażki Oddziału II Sztabu Generalnego Wojska Polskiego w starciu z Państwowym Zarządem Politycznym przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej podczas operacji dezinformacyjnej sowieckiego kontrwywiadu, znanej jako „afery MOCR-Trust” 168

III. RECENZJE

Krzysztof Izak

Charles Townshend, „Terroryzm” 203

Marek Świerczek

Konrad Paduszek, „Zajrzeć do mózgu Lenina. Wywiad II Rzeczypospolitej a postrewolucyjna Rosja” 215

IV. ARTICLES AND DISSERTATIONS**Andrzej Krzak**

Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict 221

Jolanta Darczewska

Active measures as the Russian hybrid aggression in a retrospect. Chosen aspects 244

Danuta Gibas-Krzak

Russian concept of the Eurasian Aerospace Defense System. Analysis of the problem 266

V. STUDIES AND ANALYSES**Anna Łasińska**

Selected imaging techniques applied in forensic science 283

Sławomir Gładysz

Counter-terrorism powers of national authorities 310

Marcin Gołaszewski, Paulina Markowicz, Justyna Jastrzębska

Social perceptions of polygraph examinations in Poland, their utility in security agencies and other fields of activity 337

Marek Świerczek

The internal sources of the defeat of the Second Department of Polish General Staff in the confrontation with the State Political Directorate under the People's Commissariat of interior affairs of the Russian Soviet Federative Socialist Republic during the disinformation operation of the Soviet counterintelligence known as the „MOCR-Trust affair” 352

VI. REVIEWS**Krzysztof Izak**

Charles Townshend, „Terrorism” 381

Marek Świerczek

Konrad Paduszek, „Look into Lenin’s brain. Intelligence of the Second Republic of Poland and post-revolutionary Russia” 392

O autorach 397

About authors 398

Siódma edycja ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa 399

Ogólnopolski konkurs Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych. Edycja VIII – 2018. Ogłoszenie i warunki konkursu 401

Informacje dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego” 403

I
ARTYKUŁY I ROZPRAWY

Andrzej Krzak

Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego

Wstęp

Od zakończenia zimnej wojny obserwuje się gwałtowne zmiany w taktyce i prowadzeniu konfliktów oraz wojen. Zauważalne jest narastające wzajemne przenikanie się i łączenie technik wojny regularnej i nieregularnej. Współczesne konflikty militarne, zarówno o charakterze regionalnym, jak i znacznie szerszym zasięgu, cechuje kompleksowość zastosowania i praktycznego wykorzystania wszelkich możliwych środków walki. Już wstępne analizy wskazują na wzajemne zależności zachodzące pomiędzy poszczególnymi fazami realizacji planu oraz celów polityczno-wojskowych przyjętych przez agresora na poziomie taktycznym, operacyjnym i strategicznym. Przy czym wspomnianą kompleksowość trzeba rozumieć dużo szerzej. Należałoby raczej użyć pojęcia *hybrydyzacja* lub *hybrydowość* nowego pola walki. Niemniej jednak to zjawisko nie jest niczym nowym, jeśli chodzi o sposób prowadzenia wojen, i nie sprowadza się tylko do przeprowadzania operacji w wymiarze militarnym, lecz także do wielu działań o charakterze informacyjnym, politycznym i ekonomicznym. Nie dotyczy też wyłącznie struktur siłowych zaatakowanego państwa, przede wszystkim oddziałuje na szerokie warstwy społeczeństwa, grupy narodowe, etniczne i religijne. Ta różnorodność elementów wchodzących w taką formę działalności destrukcyjnej stała się niezwykle popularnym tematem dyskursu politycznego i publicystycznego oraz została współcześnie zdefiniowana jako *działania hybrydowe* lub *wojna hybrydowa*¹.

Zmiana środowiska międzynarodowego po zimnej wojnie spowodowała, że świat stanął przed nowymi wyzwaniami dotyczącymi szeroko rozumianego bezpieczeństwa. Zniknęło zagrożenie globalnym konfliktem pomiędzy dwoma ówczesnymi supermocarstwami i blokami państw. Wygasło również widmo nuklearnej zagłady, które w znacznym stopniu było obecne w myśleniu o bezpieczeństwie jeszcze na początku lat 80. XX wieku. Na plan pierwszy wysunęły się nowe problemy odnoszące się do bezpieczeństwa międzynarodowego.

Bezpośrednio po upadku bloku komunistycznego wydawało się, że głównym zagrożeniem bezpieczeństwa w nadchodzącej epoce będą konflikty o charakterze etnicznym, narodowościowym i religijnym. Kolejne kryzysy przeradzające się w długotrwałe wojny na obszarze byłego Związku Sowieckiego oraz Jugosławii zdawały się potwierdzać te prognozy. Zwracano uwagę na „odmrażanie” konfliktów, które

¹ A. Dębczak, C. Pawlak, J. Keplin, *Analityczny model oceny hybrydowości współczesnych konfliktów*, „Zeszyty Naukowe AON” 2015, nr 2, s. 45.

ponownie ujawniły się w związku ze zmianą sytuacji geopolitycznej w poszczególnych regionach świata. Państwa, które znalazły się w nowej rzeczywistości, nie radziły sobie z rozwiązywaniem narastających problemów. Dotychczasowy układ skupiony wokół dwóch mocarstw stojących na stanowisku utrzymania równowagi sił rozpadł się i na placu boju pozostał tylko jeden gracz, który, jak się wydawało, nie mając groźnego adwersarza, z powodzeniem narzuci swój model demokracji. Jednak sytuacja, jaka się wytworzyła po zakończeniu zimnej wojny, dość szybko zweryfikowała te nadzieje: okazało się, że zarówno organizacje międzynarodowe, jak i najsilniejsze mocarstwo świata nie mogą uporać się z licznymi i gwałtownie zachodzącymi zmianami. Konflikty i wojny z początku lat 90. ubiegłego stulecia spowodowały konieczność dokonania przewartościowań w sposobie myślenia i kształtowania problematyki odnoszącej się do szeroko rozumianego bezpieczeństwa. Sytuacja uległa dalszym komplikacjom po zainicjowaniu procesów globalizacyjnych². Doktryny, strategie oraz stare armie zimnowojenne odeszły do lamusa. Doszło do znaczących zmian w postrzeganiu roli państwa i sił zbrojnych w nowej rzeczywistości.

W tych okolicznościach rozwinęły się teoretyczne nurty nowej wizji świata oparte przede wszystkim na jednobiegunowej dominacji Stanów Zjednoczonych. Skupiają się one na utrzymaniu, kontroli oraz poszerzaniu obszaru demokracji, wolnego rynku i zachodniego sposobu życia³. Wzorzec amerykańskiego stylu bycia, a co za tym idzie – także postrzegania demokracji – stał się główną determinantą polityki tego supermocarstwa w ostatniej dekadzie XX w. i na początku następnego stulecia. Kolejne administracje nie zamierzały zmieniać ani swojej polityki, ani linii polityki zagranicznej nastawionej na umacnianie przewagi zdobytej po upadku świata dwubiegunowego, wypracowanej po zakończeniu zimnej wojny. Tym samym niedopuszczalne stało się zezwolenie Rosji na odbudowę pozycji militarnej i politycznej, jaką miał ZSRR, a która mogłaby zagrozić pozycji Stanów Zjednoczonych. Normalizacja sytuacji wewnętrznej po rządach jelicynowskich i program pierwszej prezydentury Putina budziły uzasadnione obawy USA. Zwłaszcza, że nowy władca Kremla jasno sprecyzował swój program: uznał, że pogrzebanie świata zimnowojennego i ZSRR było największą, parafrazując jego słowa, katastrofą dla Rosjan. Amerykańscy politycy, mimo że z obawą spoglądali na poczynania Putina, to raczej nie dawali wiary temu, że Rosja rzeczywiście może zagrozić ich krajowi. Mieli też inne zmartwienia – przede wszystkim odradzający się terroryzm i wojujący islam. Również liczni dyktatorzy, przede wszystkim ze świata arabskiego, stanowili zagrożenia amerykańskiej polityki XXI w., szczególnie w obliczu narastającej ofensywy Al-Kaidy. Operacje wojskowe przeprowadzane przez USA, które miały nie dopuścić do rozwoju globalnego terroru, nie tylko nie zlikwidowały niebezpieczeństwa, lecz także przyśpieszyły konsolidację organizacji radykalnych i doprowadziły do powstania jednego centrum terrorystycznego. Wkrótce

² В.Н. Горбунов, С.А. Богданов, *О характере вооружённой борьбы в XXI веке*, „Военная мысль” 2009, nr 3, s. 2–3.

³ M.A. Piotrowski, *Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych*, „Sprawy Międzynarodowe” 2015, nr 2, s. 8.

się okazało, że wypracowane metody i sposoby zwalczania nowego przeciwnika przy wykorzystaniu przewagi militarnej oraz technologicznej były mało efektywne i kompletnie nieprzydatne.

W opisywanym okresie dominowało przekonanie, że polityka wojskowa USA będzie nadal definiowana przez pryzmat tzw. rewolucji w sprawach wojskowych (Revolution in Military Affairs – RMA⁴), która miała im przynieść utrzymanie przewagi technologicznej, informacyjnej i nuklearnej. Ten pogląd, lansowany od początku ostatniej dekady XX w., odnosił się do wykorzystania nowoczesnych technologii informacyjnych, dowodzenia, wywiadu⁵, środków rażenia oraz koncepcji działań taktycznych, operacyjnych i strategicznych, dzięki którym było możliwe prowadzenie błyskawicznych operacji połączonych przez wszystkie rodzaje sił zbrojnych, a także wykonywanie uderzeń w każdym miejscu pola walki, o dowolnej porze dnia i nocy oraz w dowolnych warunkach terenowych i atmosferycznych⁶.

Jednak po przeprowadzeniu pełniejszych i dokładniejszych badań okazuje się, że to wcale nie Amerykanie są ojcami koncepcji (myśli, teorii) RMA. Jej korzeni należy szukać na przełomie lat 70. i 80. XX wieku w ZSRR. Wówczas to część radzieckich dowódców i teoretyków wojskowości wypracowała niezwykle interesującą i nowatorską, jak na tamte czasy, koncepcję rewolucji wojskowo-technicznej, a ówczesny szef Sztabu Generalnego Sił Zbrojnych Związku Radzieckiego marsz. Nikołaj Ogarkow twierdził, że skuteczność prowadzenia działań wojennych w przyszłości będzie determinowana przez supernowoczesne, pozanuklearne technologie⁷.

Poglądy rosyjskiego szefa sztabu nie wpłynęły jednak na ówczesną teorię radzieckiej sztuki wojennej. Pomimo ogromnego skoku cywilizacyjnego i postępu naukowo-technicznego napędzającego budowę wciąż to nowych systemów uzbrojenia w XX w., rosyjscy teoretycy tej sztuki nie zdołali określić charakteru przyszłych wojen. Rosyjska teoria i praktyka w zakresie sztuki wojennej zatrzymała się na poziomie wojen minionego pokolenia, o czym może świadczyć *Doktryna wojenna Federacji Rosyjskiej*⁸ przyjęta w 1999 r.

W wyniku zaawansowanego rozwoju gospodarczego oraz rewolucji informacyjnej i technologicznej na przełomie wieków nastąpiło formowanie się nowych baz: technicznej i naukowej, które stały się podstawą wyznaczającą nowe trendy w prowadzeniu przyszłych wojen, a których fundament stanowią wysoko zaawansowane technologie oraz systemy informacyjne. Niezwykle istotną rolę odegrały: mikroelektronika, optoelektronika, technika sensorowa, a także nowe technologie produkcji

⁴ Patrz: J. Blaker, *Understanding the revolution in military affairs: A guide to America's 21st century defense*, Washington 1997; E.C. Sloan, *The Revolution in Military Affairs: Implications for Canada and NATO*, Montreal 2002.

⁵ M. Lekowski, *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*, „Bezpieczeństwo Narodowe” 2011, nr 19, s. 267.

⁶ R.O. Hundley, *Past Revolutions, Future Transformations. What can the history of revolution in military affairs tell us about transforming the U.S. military?*, Washington 2009, s. 9–10.

⁷ M. Vickers, R. Martinage, *The Revolution in War*, Washington 2004, s. 8–9.

⁸ И. Капитанец, *Битва за мировой океан*, Москва 2002, s. 50–51.

i zastosowania materiałów wysokojakościowych⁹. Dzięki tym osiągnięciom powstały nowoczesne systemy uzbrojenia i wyposażenia, które są w stanie całkowicie zmienić charakter walki zbrojnej i w ogóle wojny jako takiej¹⁰. Ale oprócz technologii nowoczesnych, jak się wkrótce miało okazać, również i prymitywne modele prowadzenia walki, łączące nowoczesne zdobycze technologiczne z przestarzalami systemami uzbrojenia, mogą stanowić równie zabójcze narzędzie.

Zupełnie inaczej natomiast przebiegały badania nad konfliktami i wojnami na Zachodzie. Rzeczywistość i wyzwania wymusiły wypracowanie nowej taktyki i doktryny prowadzenia walki w zmienionych warunkach zarówno militarnych, jak i politycznych. Część wojskowych twierdziła, że RMA oraz inne techniki prowadzenia walk w związku z pojawieniem się nowych wyzwań i zagrożeń nie spełniają już oczekiwań i że należy szukać nowych rozwiązań. Stwierdzono też, że sytuacja polityczno-wojskowa będzie generowała następne konflikty, których nie będzie można rozwiązać przy zastosowaniu dotychczasowych metod i form prowadzenia działań bojowych. Krytykowano także poglądy, które opierały się na wykorzystywaniu – w przypadku rozwiązywania sytuacji kryzysowych – dyplomacji. Uważano bowiem, że pokojowe rozstrzygnięcie konfliktów może być efektywne tylko w niektórych, ściśle określonych sytuacjach. Jednak wszystkie dotychczasowe wydarzenia skłaniały do wniosku, że rozpad struktur państwowych, narastająca frustracja oraz brak perspektyw nie tylko dla pojedynczych państw, lecz także całych regionów, i dominacja Stanów Zjednoczonych będą zasadniczymi powodami wybuchających konfliktów. Te poglądy zdawały się potwierdzać konflikty w Iraku i Afganistanie, w które szczególnie intensywnie zaangażowały się kolejne administracje amerykańskie.

To, co wydawało się proste i wynikało z ogromnej przewagi politycznej, gospodarczej i militarnej USA, okazało się bardziej skomplikowane niż przewidywali politycy, planiści, wojskowi i eksperci wywiadu. Stany Zjednoczone zostały uwikłane w długoletni konflikt, który wydaje się nie mieć końca. Żadne zmiany w taktyce i myśli wojskowej dotyczące zastosowania nowych systemów uzbrojenia nie przyniosły oczekiwanych rezultatów, a zwłaszcza osiągnięcia takiej przewagi, która w końcu przechyliłaby szalę zwycięstwa na stronę amerykańską.

Na kanwie doświadczeń z przełomu XX i XXI w. zrodziła się teoria zagrożeń i wojen asymetrycznych oraz tzw. wojen złożonych i wojen czwartej generacji (4GW). Ten ostatni typ wojen, najkrócej je charakteryzując, obejmuje działania, które zmierzają do osłabienia przeciwnika przy użyciu metod całkowicie odmiennych od tych, jakimi operuje wroga strona¹¹. Zatem w sferach strategicznej i operacyjnej będzie tu mowa o takich zjawiskach, jak: utrata monopolu państwa na prowadzenie wojny, powrót do świata kultur i państw w stanie konfliktu, wewnętrzny podział społeczeństwa (etniczny, religijny, według grup interesów), poszukiwanie głównego celu uderzenia

⁹ В.Н. Горбунов, С.А. Богданов, *О характере вооружённой борьбы...*, s. 5.

¹⁰ И. Капитанец, *Битва за...*, s. 50–51.

¹¹ H. Królikowski, *Siły operacji specjalnych (Wojska Specjalne) w konfliktach hybrydowych*, „Bezpieczeństwo. Teoria i Praktyka” 2016, nr 3, s. 24.

psychologicznego (wola walki, opinia publiczna) oraz dysproporcja pomiędzy inwestycjami a rezultatami. W sferze taktycznej natomiast będzie to skutkowało przesunięciem koncentracji wysiłku z frontu przeciwnika na jego tyły i wykorzystaniem potencjału przeciwnika przeciwko niemu¹².

Profesor Jacek Reginia-Zacharski podkreśla, że w wojnach tego typu wzrasta rola czynnika pozapaństwowego, dysponującego znacznymi środkami i jednocześnie wykorzystującego samo zjawisko wojny do bogacenia się. Ponadto w takich wojnach biorą udział zarówno organizacje terrorystyczne, jak i grupy zorganizowanej przestępczości oraz korporacje ponadnarodowe¹³. W pewnym sensie wojnę 4GW można zdefiniować jako wojnę hybrydową, jeśli weźmie się pod uwagę główne założenia tej teorii. Świat zmienił się do tego stopnia, że wymusił na głównych aktorach stosunków międzynarodowych prowadzenie wojen w sposób zgoła odmienny od tego, który proponowali dotychczas uznani myśliciele i teoretycy sztuki wojennej. Wiadomo tylko jedno: strategie, taktyki i działania bojowe z udziałem masowych armii, znane z mniej lub bardziej odległej przeszłości, jak na razie pozostają przeszłością. Wydaje się, że poszukiwanie nowych koncepcji i sposobów prowadzenia wojny jest podyktowane rosnącymi rozbieżnościami między ideami umieszczonymi w kontekście RMA a praktyką polityki bezpieczeństwa wielu państw, w tym przede wszystkim Stanów Zjednoczonych. Musiało to doprowadzić do krytyki paradygmatu bezpieczeństwa, który był oparty na podstawowym znaczeniu wykorzystania technologii w systemach obrony poszczególnych państw, a także modeli prowadzenia współczesnych działań bojowych. Główny zarzut formułowany od kilku lat – to niemożność znalezienia takiego rozwiązania, które doprowadziłoby do przewyciężenia impasu, w jakim znalazła się współczesna sztuka wojenna. Impasu, który jest efektem rosnącej złożoności współczesnych (i prawdopodobnie przyszłych) wojen oraz konfliktów, a także sposobów i metod ich prowadzenia oraz rozstrzygania. Należy zauważyć, że pat, w jakim znaleźli się współcześni uczestnicy walki, jest podstawową cechą wojen XXI w., w których ani przewaga technologiczna czy psychologiczna (ideowa), ani dowódczo-organizacyjna nie są (i najprawdopodobniej nie będą) elementami decydującymi w osiągnięciu sukcesu końcowego¹⁴. Nie wiadomo jednak, czy za kilka miesięcy, a może lat, nie trzeba będzie oprzeć potencjału militarnego na masowych armiach i czy do łask nie wrócą podręczniki opisujące wielkie operacje z udziałem grup armii i frontów. Nie powinno się więc raczej zapominać o tym, że oprócz praktyki odnoszącej się do wojen nieregularnych, partyzanckich, ludowych, nielinearnych, złożonych, operacji specjalnych i innych istnieją klasyczne poglądy na organizację i sposób prowadzenia walki.

¹² Tamże.

¹³ Patrz: J. Reginia-Zacharski, *Wojna w świecie współczesnym. Uczestnicy, cele, modele, teorie*, Łódź 2014, s. 294–304.

¹⁴ A. Gruszczyk, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapala (red. nauk.), Warszawa 2011, s. 9.

Hybrydowość współczesnych konfliktów i wojen w ujęciu rosyjskiej oraz zachodniej myśli wojskowej

Koncepcja wojen hybrydowych nie jest niczym nowym w dziejach wojen i myśli wojskowej, przy czym obecnie należy ją rozumieć w dużo szerszym kontekście, a nie tylko jako sposób prowadzenia walki¹⁵. Wydaje się ona kolejnym amerykańskocentrycznym ujęciem współczesnych wojen oraz stanowi próbę rozwikłania „dylematu amerykańskiej potęgi” i poszukiwania odpowiedzi na pytanie, dlaczego USA nie potrafiły wykorzystać pozycji światowego hegemonu i rozstrzygnąć konfrontacji ze znacznie słabszymi przeciwnikami na swoją korzyść¹⁶. Bezsilność Stanów Zjednoczonych jest wynikiem wielu złożonych zjawisk zachodzących we współczesnym środowisku bezpieczeństwa. „Imperialna pycha” (*imperial hubris*) oraz „hegemoniczne zadufanie” (*hegemonic presumption*) – to tylko niektóre z przyczyn porażki, jaką poniosły USA w ostatnich dwóch dekadach. Ponadto brak jednej wypróbowanej strategii działania i efektywnych technik taktycznych wydają się kolejnymi przyczynami braku sukcesów. Stąd mnogość różnych koncepcji i teorii prowadzenia wojen, które zamiast rozwiązać dylematy, w rzeczywistości powodują jeszcze większy chaos zarówno w ujęciu naukowym, jak i praktycznym. Niewątpliwie poszukiwania uniwersalnego modelu nowych form prowadzenia działań militarnych w środowisku, w którym nie ma przeciwnika państwowego, doprowadziły do konieczności znalezienia efektywnego antidotum na bezsilność największego i jedyne supermocarstwa. Pomimo licznych badań i ciągłych poszukiwań, nie znaleziono niestety rozwiązania, które przyniosłoby sukces militarny wraz z gwarancją zakończenia wojny. Wręcz przeciwnie – toczące się wojny oraz przyszłe konflikty będą procesami długotrwałymi, a przewaga technologiczna, gospodarcza czy wojskowa nie będą gwarantowały osiągnięcia celów i realizacji interesów w wymiarze strategicznym lub politycznym¹⁷.

¹⁵ Liczne propozycje doktrynalne odnoszące się do konstrukcji teorii hybrydowości w prowadzeniu współczesnych wojen wydają się kolejnym etapem poszukiwań uniwersalnej metody prowadzenia efektywnych działań bojowych na każdym szczeblu funkcjonowania sił zbrojnych oraz instytucji odpowiedzialnych za szeroko rozumiane bezpieczeństwo militarne państwa. Teoretycy zachodni, rozważając różne warianty walki o zachodni (amerykański) model demokracji, nie biorą pod uwagę wielu niezwykle istotnych czynników politycznych i wojskowych. Jakby zapomnieli o takich sprawach, jak szybko zachodzące zmiany na polu walki, konieczność improwizacji, pozostawienia inicjatywy dowódczej (zwłaszcza na poziomie taktycznym) albo uznawali je za zbędne. Tworzenie sztywnych norm doktrynalnych jest zabiegiem dość ciekawym, ale i ryzykownym, zwłaszcza że za kilka miesięcy ktoś może wymyślić albo zaproponować kolejną „hybrydę”. Łączenie różnych form działań bojowych od zarania dziejów było praktykowanym sposobem prowadzenia wojen. Dlatego musi obecnie dziwić tak nachalne budowanie nowych teorii, które nagle miałyby się stać jakąś nową metodą prowadzenia konfliktu militarnego. Politycy i wojskowi, a zwłaszcza ci drudzy, wielokrotnie zachwycali się nowym pomysłem na wygraną wojny, będąc pod presją konieczności zakończenia wieloletniego konfliktu. Jednak najczęściej rozstrzygnięcie znajdowało się nie w zastosowaniu nowych technik walki, tylko w umiejętnym połączeniu wielu elementów, zarówno militarnych, jak i pozamilitarnych.

¹⁶ N. Freier, *The Defense Identity Crisis: It's a Hybrid World*, „Parameters” 2009, nr 3, s. 82.

¹⁷ A. Gruszczyk, *Hybrydowość współczesnych wojen...*, s. 10.

Etymologia pojęcia hybrydowość prowadzi do łacińskiego słowa *hybrida*, które oznacza ‘mieszaniec’, czyli istotę powstałą ze skrzyżowania dwóch genetycznie różnych osobników należących do różnych gatunków, ras lub odmian¹⁸. „Hybrydowość” można zdefiniować również jako:

(...) właściwość powstałą w wyniku skrzyżowania lub zmieszania cech, elementów należących do różnych, często odmiennych strukturalnie i odległych genetycznie, przeciwstawnych przedmiotów, organizmów lub stanów. Hybrydyzacja oznacza więc scalenie odmiennych istotowo cech wokół jednego, odrębnego bytu, przy zachowaniu specyficznych własności gatunkowych decydujących o „wyższości” nowego, hybrydowego organizmu pod względem np. odporności na choroby, wytrzymałości czy większych zdolności adaptacyjnych¹⁹.

Do obiegu naukowego pojęcie wojna hybrydowa wprowadził emerytowany oficer marines ppłk Frank G. Hoffman²⁰, według którego to zjawisko jest (...) *zbieżnością (...) fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów (...) sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone*²¹. Jednak terminem wojny hybrydowe posługiwano się w dyskursie naukowym także w latach 90. XX w., m.in. za sprawą historyka z chicagowskiego Uniwersytetu DePaul oraz Instytutu Studiów Strategicznych USA, Thomasa R. Mockaitisa²². Amerykański historyk, opisując wojny okresu kolonialnego toczone przez Wielką Brytanię, zauważył, że oprócz klasycznych walk konwencjonalnych prowadzono wówczas działania o charakterze przeciwpartyzanckim i terrorystycznym, z zastosowaniem kombinowanych form prowadzenia operacji bojowych²³.

W 1998 r. termin wojny hybrydowe pojawił się w pracach poświęconych historii Korpusu Marines. Komandor Robert Walker określił jednostki Korpusu jako

¹⁸ *Słownik wyrazów obcych PWN*, J. Tokarski (red.), Warszawa 1980, s. 290.

¹⁹ A. Gruszczyk, *Hybrydowość współczesnych wojen...*, s. 11.

²⁰ Pojęcia działania hybrydowe oraz wojna hybrydowa zostały użyte również w 2002 r. w pracy mjr. Williama J. Nemetha pt. *Future war and Chechnya: A case for hybrid warfare*. Zostały one jednak zawężone do oceny społeczeństwa czeczeńskiego oraz niektórych form prowadzenia działań przez czeczeńskich rebeliantów. Dlatego też trudno przyjąć, że zaproponowany przez tego autora aparat pojęciowy w pełni oddaje złożoność zjawiska hybrydowości jako nowej formy prowadzenia działań militarnych, nie uwzględnia on bowiem całej złożoności tego zjawiska, a jest raczej dość nieudolną próbą analizy konfliktu czeczeńsko-rosyjskiego. Jednak niewątpliwie za ceną należy uznać ocenę możliwości ówczesnej armii rosyjskiej i jej doktryny walki, jako przestarzałej i kompletnie nieprzydatnej w nowych realiach ówczesnego pola walki. Zob. Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 14, s. 40, wydanie specjalne.

²¹ F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, nr 52, s. 34.

²² Mockaitis podkreślał również hybrydowy charakter brytyjskich sił ekspedycyjnych, które były wspierane komponentem dyplomatycznym oraz działaniami politycznymi. Zob. T.R. Mockaitis, *British Counterinsurgency in the Post-imperial Era*, London 1995, s. 16–17, 30 i 38.

²³ M.A. Piotrowski, *Konflikt nigdy nie jest prosty...*, s. 10.

hybrydowe, a operacje, które były prowadzone z ich udziałem, jako działania hybrydowe²⁴. Również inni zachodni eksperci próbowali sformułować nowy paradygmat badawczy wobec zachodzących zmian w odniesieniu do współczesnych konfliktów militarnych. Przykładem może być płk Daniel T. Lasica, który uważał, że „hybrydowość” należy rozumieć jako kombinację strategii i taktyki, łączącą różne formy działań militarnych²⁵. Z kolei płk John J. McCuen proponuje przyjęcie, że wojna hybrydowa jest niczym innym, jak powiązaniem składowych wojny symetrycznej i asymetrycznej²⁶. Tak zaproponowane pojęcie sprowadza ten typ wojny do zjawiska odnoszącego się do walki zbrojnej w ramach toczącego się konfliktu lub wojny zastępczej, czyli formuły różnych sposobów prowadzenia działań bojowych w zależności od miejsca i zaangażowanych w niej przeciwników.

Należy przy tym zauważyć, że w samej Rosji do 2014 r. nie używano terminu wojna hybrydowa, a jedynie rzadko go wymieniano w literaturze przedmiotu. Pojawiał się on tylko w kontekście rozważań o działaniach, jakie prowadziły siły zbrojne Stanów Zjednoczonych oraz ich koalicjantów w Iraku i Afganistanie, dla zobrazowania nowej formy wojny toczonej przez Zachód. Dopiero konflikt ukraiński spopularyzował amerykańską wersję wojny hybrydowej, która na stałe zagościła zarówno w publicystyce, jak i w dyskursie politycznym (naukowym) w Rosji. Rzecz oczywista, Rosjanie chętnie przyswoili sobie pojęcia i terminy, które są nierozzerwalnie związane z nowymi wojnami, w tym również z hybrydowością konfliktów. Nie oznacza to jednak, że rosyjscy teoretycy nie opracowali własnego aparatu pojęciowego opisującego zjawisko hybrydowości wojen. Dla przykładu można podać trzy definicje wojen hybrydowych w ujęciu rosyjskich ekspertów. Pierwsza z nich to definicja S.F. Wikułowa i Je.Ju. Chruszałjowa, którzy twierdzą, że wojny hybrydowe to kompleksowe i metodyczne oddziaływanie nie tylko militarne (lecz także polityczne, ekonomiczne i społeczne) charakteru w ramach stosunków międzynarodowych²⁷.

²⁴ Patrz: R.G. Walker, *SPEC FI: the United States Marine Corps and Special Operations*, Monterey 1998; M.A. Piotrowski, *Konflikt nigdy nie jest prosty...*, s. 11.

²⁵ M. Wojnowski, *Mit „wojny hybrydowej”*. *Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przeгляд Bezpieczeństwa Wewnętrznego” 2016, nr 14, s. 9, wydanie specjalne.

²⁶ Według amerykańskiego teoretyka, decydenci i eksperci wojskowi stanęli przed koniecznością rozstrzygnięcia nie lada dylematu: jak efektywnie prowadzić walkę w nowych warunkach, mając przeciwko sobie przeciwnika, którym nie są podmioty państwowe, a różnego rodzaju organizacje zbrojne (paramilitarne)? Jak zatem wygrać wojnę, gdy klasyczne formy walki zawodzą? Kolejnym problemem w jego rozważaniach było znalezienie takiego modelu postępowania, który umożliwiłby zaprowadzenie porządku (ustabilizowanie sytuacji) na obszarach kontrolowanych przez siły interwenujące. Za podstawę rozważań zostały przyjęte konflikty w Indochinach (Wietnamie), Somalii, a także w Libanie. Zob. J.J. McCuen, *Hybrid Wars*, „Military Review” 2008, t. 2, s. 107–108.

²⁷ Według nich wojna hybrydowa to: (...) комплексное применение различных методов (не только военного, но и экономического, социального, политического характера) воздействия на противника в рамках межгосударственного противоборства (...). Zob. С.Ф. Видулов, Е.Ю. Хрусталёв, *Методологические основы и специфика военно-экономического анализа*, „Экономический анализ: теория и практика” 2014, nr 7, s. 5–6.

Inną definicję, zbliżoną do Hoffmanowskiej, prezentuje znany rosyjski politolog Aleksandr Aleksandrowicz Bartosz. Według niego wojna hybrydowa to mnogość różnego rodzaju działań prowadzonych przez agresora za pomocą form konwencjonalnych (klasycznych) i nieregularnych, przy jednoczesnym wsparciu komponentu pozamilitarnego. Natomiast trzecia jest prezentowana przez Władimira Nikołajewicza Akulinina oraz Natalię Siergiejewnę Jepifanową, którzy biorąc pod uwagę kontekst wojskowo-polityczny, uważają, że przez wojnę hybrydową należy rozumieć zastosowanie na terytorium potencjalnego przeciwnika różnorodnej taktyki wojskowej i politycznej oraz społeczno-ekonomicznych działań destabilizacyjnych²⁸.

Klasyczna definicja *hybrid warfare* wydaje się jednak niedoprecyzowana i zawężająca znaczenie opisywanego zjawiska. Często także jest błędnie interpretowana. Po pierwsze odnosi się głównie do prowadzenia działań przez zorganizowane siły zbrojne; po drugie współcześnie definiowane zjawisko hybrydowości cechuje się prowadzeniem operacji na wielu płaszczyznach i uczestnictwem w nich przede wszystkim podmiotów pozapaństwowych; po trzecie wreszcie – na co wskazują eksperci – w przypadku wojen hybrydowych brakuje elementu wypowiedzenia wojny oraz wprowadzenia innych stanów nadzwyczajnych, takich jak stan wyjątkowy lub wojenny. Biorąc zatem pod uwagę mnogość, charakter i skalę działań, jakie niesie za sobą tzw. wojna hybrydowa, oraz to, że zazwyczaj jest ona celowo ograniczana i utrzymywana na poziomie poniżej jednoznacznie dającego się ocenić progu dla regularnej wojny, należałoby jednak stosować pojęcia: działania hybrydowe lub operacje o charakterze hybrydowym zamiast wojna hybrydowa.

Niestety, począwszy od 2014 r., czyli od konfliktu na Ukrainie, pojęcie wojna hybrydowa ze względu na jego silne oddziaływanie na opinię publiczną zarówno w wymiarze narodowym, jak i globalnym jest nadużywane. Jeszcze innym nadużyciem jest tworzenie licznych odniesień do tego konfliktu, charakteryzowanego jako wojna hybrydowa, która jest prowadzona przez Rosję przeciwko niezawisłemu i suwerennemu państwu. Należy zatem zadać podstawowe pytanie: czy konflikt ukraiński jest klasycznym przykładem wojny hybrydowej, jak tego chcą zachodni teoretycy (dziennikarze i politycy), czy też zjawisko hybrydowości prowadzenia działań militarnych jest nową formą współczesnych wojen i zostało zastosowane w praktyce przez rosyjskich przywódców i decydentów wojskowych w ramach polityki ukierunkowanej na odtworzenie mocarstwowej pozycji Rosji oraz dokonanie zmian w układzie sił w skali globalnej? Można też zadać wiele innych pytań zmierzających do zweryfikowania zachodnioeuropejskiej tezy, że Rosja od dawna przygotowywała się do agresji oraz że tzw. doktryna Gierasimowa stanowi jeden z koronnych dowodów potwierdzających tę tezę.

²⁸ Гибридная война – это широкий диапазон действий, осуществляемых противником с использованием военных и иррегулярных формирований, с одновременным привлечением гражданских компонентов. Zob. В.Н. Акулинин, Н.С. Епифанова, Концепция гибридной войны в практике межгосударственного противостояния, „Национальные интересы: приоритеты и безопасность” 2015, nr 36, s. 54.

Współcześnie przypisuje się Rosji szczególną rolę w kreowaniu i prowadzeniu nowej formy działań, jaką mają być tzw. wojny hybrydowe. Wielu ekspertów z uporem stara się przekonać opinię społeczną, że Rosja, a właściwie jej polityczni i wojskowi decydenci, od wielu lat przygotowywała plany i strategie prowadzenia działań hybrydowych. Ta teza wydaje się jednak fałszywa. Aby dokładnie przeanalizować powyższy problem, należy założyć, że każde państwo (mocarstwo czy też państwo małe lub średniej wielkości) z reguły tworzy i wprowadza w życie wiele dokumentów normatywnych, w których określa swoje priorytety w dziedzinie obronności i bezpieczeństwa. Są to doktryny, strategie i koncepcje bezpieczeństwa narodowego lub wojennego (wojskowego). Najogólniej rzecz ujmując, chodzi o dokumenty, które stanowią podstawę systemu bezpieczeństwa danego państwa. Z założenia muszą one być spójne nie tylko z polityką zagraniczną (bezpieczeństwa), lecz także przede wszystkim z planowaniem operacyjnym, szkoleniem i rozwojem sił zbrojnych. Dlatego też nikogo nie powinno dziwić, że Rosja modyfikuje i udoskonala swoje akty prawne odnoszące się do szeroko rozumianego bezpieczeństwa militarnego i racji stanu. Analizując politykę kreowaną przez to państwo, należy zatem pamiętać o profesjonalnym podejściu do problematyki związanej z szeroko rozumianym bezpieczeństwem współczesnego państwa rosyjskiego.

Rosyjska teoria nowych wojen. Koncepcja Gierasimowa

Kilkadziesiąt miesięcy wstecz media zalała fala informacji, z których wynikało, że Rosjanie od dawna (przynajmniej od 2008 r.) przygotowywali agresję na Ukrainę. Ta wiadomość została przyjęta bez słowa krytyki i na trwałe zagościła w dyskursie publicystycznym, a co gorsza – naukowym. Nikt nie neguje, że Rosja w ciągu ostatnich kilku lat, zmieniając swoją doktrynę wojenną i strategię bezpieczeństwa narodowego, wyraźnie daje do zrozumienia, że nie ma zamiaru czekać na dalszy rozwój wydarzeń z założonymi rękami. Nikt też nie może podważyć tego, że polityczni przywódcy państwa rosyjskiego prowadzą stosunkowo klarowną politykę, której celem jest zmiana świata jednobiegunowego i powrót Rosji na pozycję supermocarstwa. Warto pamiętać o tym, że pomimo ponawianych prób, armia rosyjska nie zdołała się wyzwolić ze sztywnych kanonów i przeświadczenia rodem z II wojny światowej, iż „masa ludzka i sprzętowa” zdoła skutecznie zniwelować postęp technologiczny. A wzorce, które ją kształtowały, przez kolejne dekady były uznawane za niepodważalny kanon. I wydawało się, że ten pogląd znalazł potwierdzenie w związku ze zmiążdżeniem małej Gruzji. Ocena konfliktu gruzińskiego, jaką przeprowadzono w rosyjskim Sztabie Generalnym, wykazała, że armia rosyjska nie tylko nie jest w stanie prowadzić operacji militarnych w dłuższej perspektywie czasowej, lecz także że nie będzie mogła efektywnie walczyć ze stosunkowo silnym przeciwnikiem. Jej doktryna szkoleniowa okazała się przestarzała; ponadto rosyjskie siły zbrojne nie miały nowoczesnych systemów dowodzenia i łączności, sprzęt bojowy był archaiczny, a przewaga w ludziach i technice bojowej była

tylko złudzeniem. Na kanwie tej oceny koniecznością stało się przeprowadzenie reform systemowych i modernizacyjnych. Doświadczenia z wojny z Gruzją, liczne afery korupcyjne i marazm wokół reform sił zbrojnych z pierwszej dekady XXI w. uzmysłowiły W. Putinowi, że konieczność zmian zarówno w sferze doktrynalnej, jak i organizacyjnej, odnoszących się do szeroko rozumianego bezpieczeństwa militarnego, musi stać się priorytetem kierownictwa politycznego państwa. Oprócz konieczności przeprowadzenia reform samych sił zbrojnych, niezbędne stało się stworzenie nowej doktryny szkoleniowej dostosowanej do współczesnego pola walki. Opierając się na priorytetach polityki bezpieczeństwa i zasadniczych celach, jakie Rosja stawiała sobie w polityce zagranicznej, podjęto prace nad sformułowaniem rosyjskiej wizji przyszłych wojen i sposobów prowadzenia działań militarnych w warunkach współczesnych.

Trzeba jednak podkreślić, że koncepcja wojny nowej generacji była tematem diskutowanym na długo przed wojną z Gruzją. Warto przypomnieć poglądy W. Kapitańca opublikowane w pracy *Битва за мировой океан* wydanej w 2002 r. Twierdził on, że pomimo ogromnego skoku cywilizacyjnego i postępu naukowo-technicznego stymulującego tworzenie nowych systemów uzbrojenia w XX w., rosyjscy teoretycy sztuki wojennej nie zdołali u jego schyłku określić charakteru przyszłych wojen²⁹. Stąd też w XXI w. mamy do czynienia z nową koncepcją wojen, tzw. wojen szóstej generacji (6GW), w której zasadnicza rola miała przypadać broni precyzyjnego rażenia i obrony, a nie jak w przeszłości – masowemu wojskom lądowym. Według jego oceny cały potencjał uderzeniowy agresora będzie skierowany na sparaliżowanie obiektów gospodarki przez wykonanie silnych uderzeń lotniczych i zmasowanych uderzeń broni precyzyjnego rażenia różnorodnego bazowania, z uwzględnieniem operacji prowadzonych w ramach globalnej lub regionalnej walki informacyjnej³⁰. Ponadto Kapitaniec twierdził, że nowe wojny nie będą prowadzone wyłącznie na lądzie, w powietrzu i na morzu, ale przede wszystkim w przestrzeni kosmicznej. Nie będą też miały charakteru przewlekłego³¹, z użyciem dużych mas wojsk i sprzętu. Cały proces walki zbrojnej będzie przebiegał kompaktowo, szybko i będzie miał postać zmasowanych uderzeń bronią precyzyjnego rażenia na obiekty wojskowo-gospodarcze potencjalnego przeciwnika³²,

²⁹ И. Капитанец, *Битва за...*, s. 50–51.

³⁰ Tamże, s. 51–52.

³¹ Rosyjski teoretyk, używając określenia „przewlekły”, odniósł się do doświadczeń z okresu Wielkiej Wojny, kiedy po krótkiej fazie wojny manewrowej armie masowe przeszły do wyniszczających działań pozycyjnych.

³² Siła żywa przeciwnika może nie być celem uderzeń. Zamiast niej będą atakowane obiekty gospodarcze i obiekty administracji państwowej na całej głębokości terytorium państwa. Nie będą również atakowane państwowe rezerwy strategiczne utworzone na bazie wojsk lądowych, gdyż w wojnach nowej generacji nie będą one stanowiły zagrożenia państwa – agresora, które prowadzi wojnę z użyciem broni precyzyjnego rażenia. Tym samym odpada konieczność okupowania obszaru przeciwnika pozbawionego gospodarki, którego system polityczny najpewniej wkrótce się załamie. Te poglądy najwyraźniej wskazują na to, że ich autor bazował przede wszystkim na analizie dwóch konfliktów, tj. II wojny w Zatoce Perskiej oraz tzw. wojny NATO–Jugosławia.

z szerokim zastosowaniem środków walki radioelektronicznej (WRE). Zauważył przy tym, że w wyniku takich działań może wystąpić ryzyko przekształcenia tego typu konfliktu w wojnę jądrową³³.

Jednak najciekawsze poglądy Kapitańca odnoszą się do działań w ramach wojny informacyjnej. Twierdzi on bowiem, że wraz ze wzrostem nasycenia współczesnego pola walki środkami walki radioelektronicznej zachodzi pilna potrzeba podjęcia adekwatnych działań zaradczych ukierunkowanych na paraliżowanie środków emisji elektromagnetycznej przeciwnika. Pod pojęciem operacji WRE w nowej wojnie będzie postrzegany kompleks przedsięwzięć i działań skierowanych na radioelektroniczne sparaliżowanie agresora oraz ochronę własnych wojsk i systemów uzbrojenia przed radioelektronicznym oddziaływaniem potencjalnego przeciwnika. Najpewniej komponentami tego typu operacji będą: ogniowe niszczenie systemów WRE przeciwnika i źródeł każdego promieniowania elektromagnetycznego, sparaliżowanie całego systemu środków radioelektronicznych, ochrona własnych źródeł promieniowania elektromagnetycznego oraz radioelektroniczna osłona przed uderzeniami precyzyjnego rażenia. Działania realizowane w ramach operacji WRE, w połączeniu z ogniem i manewrem, będą prowadzone jednocześnie podczas uderzeniowej operacji powietrzno-kosmiczno-morskiej i operacji strategicznej ukierunkowanej na odparcie agresji. Z kolei działania informacyjne miały się stać aktywną składową komponentu uderzeniowego środków precyzyjnego rażenia, a zasób informacyjny państw – jednym z najważniejszych elementów systemów strategicznych sił uderzeniowych i strategicznych sił obronnych państwa. Będzie on obejmował wszystkie obszary (przestrzeń) walki (kosmos, cyberprzestrzeń, powietrze, ląd oraz morze) i będzie się koncentrował na zabezpieczeniu: sieci, systemów telekomunikacyjnych, radionawigacyjnych, dowodzenia wojskami i energetycznych, transportu, finansów itp.

Do narzędzi walki informacyjnej zostaną włączone także kosmiczne środki rozpoznania, które staną się głównymi źródłami informacji zarówno podczas planowania, jak i organizacji oraz prowadzenia działań bojowych. Z przestrzeni kosmicznej będzie stale (nieprzerwanie) i w szerokim zakresie prowadzone rozpoznanie: radiotechniczne, radiolokacyjne, podczerwone, radiacyjne, chemiczne, fotograficzne i telewizyjne, które będzie dostarczało niezbędne informacje w czasie rzeczywistym.

Przeciwdziałanie informacyjne³⁴ zostanie zrealizowane przez panowanie w przestrzeni informacyjnej oraz trwałą ochronę informacyjną własnych systemów uderzeniowych i obronnych³⁵.

Głównym celem walki informacyjnej według I. Kapitańca będzie utrzymanie niezbędnego poziomu własnego bezpieczeństwa informacyjnego i zmniejszenie

³³ И. Капитанец, *Битва за...*, s. 53–54.

³⁴ Pod pojęciem przeciwdziałanie informacyjne w wojnach przyszłości należy rozumieć nową strategiczną formę walki, w której będą stosowane specjalne formy i metody oddziałujące na środowisko informacyjne przeciwnika i chroniące własną przestrzeń w celu osiągnięcia strategicznych celów wojny.

³⁵ И. Капитанец, *Битва за...*, s. 69.

poziomu tego bezpieczeństwa u przeciwnika. Postawiony cel może zostać osiągnięty dzięki realizacji wielu wzajemnie powiązanych zadań, z których najważniejsze to: sparaliżowanie zasobu informacyjnego i pola informacyjnego przeciwnika oraz ochrona własnych zasobów i pola.

Przeciwdziałanie informacyjne będzie zatem realizowane w następujących kierunkach i obszarach walki:

- z systemami dowodzenia na różnych szczeblach,
- między systemami uderzeniowymi i obronnymi,
- tworzenia systemu informacyjnego w całej przestrzeni powietrzno-kosmicznej,
- zabezpieczenia informacyjnego dla własnych systemów ofensywnych i obronnych³⁶.

Cele wojskowo-polityczne w wojnie szóstej generacji³⁷ będzie można osiągnąć tylko przez zastosowanie na szeroką skalę precyzyjnej broni ofensywnej systemów rozpoznawczo-informacyjnych i WRE. W związku z tym koniecznością stanie się integracja tych komponentów w jeden wspólny system bojowy łączący pole informacyjne w kosmosie, powietrzu, na morzu, na lądzie oraz w cyberprzestrzeni, który będzie mógł zmienić charakter przyszłych działań wojennych.

Przedstawione powyżej rozważania I. Kapitańca wskazują na to, że na długo przed zmianami, jakie przyniosła reforma Sił Zbrojnych Federacji Rosyjskiej, rosyjscy eksperci dostrzegali konieczność zmian w związku z zachodzącymi przeobrażeniami w środowisku przyszłego konfliktu militarnego. Na szczególną uwagę zasługuje wzrost znaczenia walki informacyjnej. Po analizie wspomnianej tzw. doktryny Gierasimowa należy stwierdzić, że znaczna część poglądów I. Kapitańca została zaadaptowana do współczesnej teorii rosyjskiej myśli wojskowej, zwłaszcza w odniesieniu do form i sposobów prowadzenia działań militarnych w konfliktach i wojnach początku XXI wieku. Niewątpliwie niektóre aspekty tej wizji zostały wykorzystane również w trakcie opracowywania i wdrażania nowej doktryny szkoleniowej w reformowanych Siłach Zbrojnych FR.

³⁶ Tamże.

³⁷ Pojęcie wojna szóstej generacji (ros. война шестого поколения) odnosi się do klasyfikacji proponowanej przede wszystkim przez rosyjskich teoretyków wojskowości. Zakładają oni podział na dwie podstawowe kategorie wojen: epoki przedjądrowej oraz jądrowej. Do pierwszego okresu zalicza się cztery generacje (broń biała – wojna w skali taktycznej; proch – wojna w skali operacyjno-taktycznej; broń gwintowana – wojny w skali operacyjno-strategicznej; samopowtarzalne uzbrojenie, armie masowe – wojny w skali strategicznej). Natomiast drugi okres obejmuje dwie generacje, tj. uzbrojenie jądrowe (zagrożenie dla świata) – okres zimnej wojny – oraz wojnę bezkontaktową – operacje w trzech zasadniczych wymiarach na lądzie, w powietrzu i kosmosie, a także rozwój broni precyzyjnego rażenia. Jej celem miało być zniszczenie podstawowych funkcji państwa i gospodarki, a ponadto systemów dowodzenia i kierowania oraz najważniejszych obiektów militarnych. Zob. И.В. Бочарников, С.В. Лемешев, Г.В. Люткене, *Современные концепции войн и практика военного строительства*, Москва 2013, s. 62; H. Sołkiewicz, *Wojna przyszłości – wojną niekontaktową (wg aktualnych poglądów rosyjskich)*, „Zeszyty Naukowe Akademii Marynarki Wojennej” 2009, nr 1, s. 72–73; В.И. Слипченко, *Войны нового поколения: дистанционные бесконтактные*, Москва 2004, s. 44–58.

I. Kapitaniec nie był jedynym rosyjskim ekspertem, który dużo wcześniej podjął się analizy zmieniających się realiów wojny i konfliktu militarnego oraz prezentacji rosyjskiego punktu widzenia na tę problematykę. Podobne poglądy prezentował również nieżyjący już generał major Władimir Slipczenko. On również uważał, że przyszłe wojny będą się opierały na walce bezkontaktowej przy użyciu broni (systemów) precyzyjnego rażenia³⁸. Odmiennie zdanie na temat przyszłych konfliktów wojennych reprezentował natomiast inny rosyjski wojskowy, generał armii Machmut Gariejew, który bazując na doświadczeniach wojny z Gruzją z sierpnia 2008 r., uważał, że tylko zmasowany atak sił konwencjonalnych, ewentualnie wsparty przez nowoczesne środki, będzie charakteryzował przyszłe starcia³⁹.

Do wystąpienia gen. Gierasimowa i zaprezentowania jego poglądów dotyczących teorii przyszłych wojen, co nastąpiło podczas konferencji naukowej 25 stycznia 2013 r. w Akademii Nauk Wojskowych w Moskwie, liczne grono rosyjskich naukowców przedstawiało wiele teorii różnych form prowadzenia wojen i konfliktów przyszłości. Jedną z najciekawszych były poglądy Ju.Je. Gorbaczewa odnoszące się do wojny w cyberprzestrzeni. W artykule opublikowanym w 2013 r. pod tytułem *Кибервойна уже идет*⁴⁰ stwierdził on, że w związku z rewolucyjnym rozwojem technologii informatycznych już od dawna trwa wojna w sieci, a ponadto, że informatyzacja systemów uzbrojenia, łączności i dowodzenia oraz innych dziedzin życia będzie miała zasadniczy wpływ na sposób prowadzenia przyszłych wojen. Gorbaczew konstatuje, że żaden rodzaj walki nie obejdzie się bez operacji sieciocentrycznych. Zauważa też, że osiągnięcie przewagi w wojnie przyszłości będzie uzależnione od zdobycia jej w sieci. W tych poglądach wtórował mu Dmitrij Rogozin, który wręcz stwierdził, że (...) *bez wykorzystania robotyki, efektywnego rozpoznania (wywiadu), automatyzacji systemów uzbrojenia, dowodzenia oraz łączności nie sposób ani współcześnie, ani też w przyszłości prowadzić walkę zbrojną*⁴¹.

Kolejną teorią, niezwykle kontrowersyjną, jest teoria tzw. *консциентальных войн*, czyli wojen społecznych lub oddziałujących na podświadomość, autorstwa W. Potiechina i J. Gromyki. Według tych rosyjskich naukowców jest to kombinacja przedsięwzięć zawierająca w sobie elementy wojen: psychologicznej (w zakresie form), cywilizacyjnej (ze względu na treść) oraz informacyjnej (w zakresie wykorzystania środków i narzędzi)⁴². Zasadniczym celem tego typu wojen jest doprowadzenie elit i całych narodów do ubezwłasnowolnienia przez zastosowanie różnorodnych technik oddziaływania informacyjnego i psychologicznego, tak aby same

³⁸ И.В. Бочарников, С.В. Лемешев, Г.В. Люткене, *Современные концепции войн...*, s. 61–62.

³⁹ М.А. Гареев, *Проблемы стратегического сдерживания в современных условиях*, „Военная мысль” 2009, nr 4, s. 3–6.

⁴⁰ Патрз: Ю.Е. Горбачев, *Кибервойна уже идет*, „Независимое военное обозрение” 2013, nr 13.

⁴¹ С.Г. Чекинов, С.А. Богданов, *О характере и содержании войны нового поколения*, „Военная мысль” 2013, nr 10, s. 14.

⁴² Д.О. Rogozin, *Перейти от заклинаний и воззваний к практической деятельности*, „Военно-промышленный курьер” 2013, nr 14.

poddały się agresorowi. Rosyjscy uczeni twierdzą, że współczesna Rosja od co najmniej kilkunastu lat jest poddawana mechanizmom charakterystycznym dla tego rodzaju działań⁴³.

W tym kontekście rozważań rosyjskich ekspertów i naukowców wystąpienie oraz artykuł gen. Walerija Gierasimowa z początku 2013 r. stanowi jednocześnie zarys i systematyzację poglądów rosyjskich decydentów politycznych i wojskowych zarówno na zmiany zachodzące w stosunkach międzynarodowych, jak i na przyszłe konflikty i wojny. Było ono niewątpliwie zaprezentowaniem rosyjskiego punktu widzenia i w pewnym sensie założeń politycznych oraz doktrynalnych, m.in. w zakresie kierunków polityki zagranicznej, a także wykorzystania potencjału militarnego i pozamilitarnego Federacji.

W. Gierasimow uważa, że po tzw. kolorowych rewolucjach świat uległ tak znacznym zmianom, że linia między wojną a stabilnym pokojem została zatarta⁴⁴. Również podstawowy paradygmat wojny polegający na pokonaniu sił zbrojnych i woli przeciwnika, zajęciu jego terytorium i zmuszeniu do przyjęcia pokoju musi ustąpić nowym rozwiązaniom, przynajmniej jeśli chodzi o narzędzia, metody i sposoby osiągnięcia tego celu⁴⁵. Zatem wojny przyszłości z pewnością będą prowadzone nie tylko przy wykorzystaniu potencjału militarnego, lecz także innych narzędzi i sposobów prowadzących do destrukcji przeciwnika. Nie rezygnuje się z metod konwencjonalnych, jednak muszą one zostać wsparte operacjami o charakterze wywiadowczym, politycznym, psychologicznym, ekonomicznym, informacyjnym, humanitarnym oraz społecznym, które prowadzi się wraz z wykorzystaniem „potencjału protestu”⁴⁶. Szczególne miejsce w tych działaniach powinny mieć wszelkiego rodzaju operacje sił specjalnych oraz wywiadu i kontrwywiadu. Na każdym etapie prowadzenia wojny akcje realizowane przez wyspecjalizowane grupy i pododdziały sił specjalnych oraz wywiad mają odgrywać rolę najważniejszą. Wszystkie te formacje aktywnie uczestniczą w pozamilitarnych przedsięwzięciach z zakresu wojny informacyjnej i psychologicznej. Zasadniczo przyszła wojna będzie się składała z trzech–czterech głównych etapów: pierwszy – to przygotowanie wywiadowcze, rozpoznanie, infiltrowanie oraz prowadzenie aktywnych działań psychologicznych oraz informacyjnych (dezinformacja, dywersja, sabotaż, terroryzm, infiltracja, anarchizacja obszaru potencjalnego celu agresji); drugi – to aktywna i trwała destabilizacja wewnętrzna oraz izolacja celu na arenie międzynarodowej; trzeci – działania zbrojne z wykorzystaniem sił specjalnych, oddziałów najemniczych, paramilitarnych i buntowniczych, prowadzące do opanowania części terytorium celu agresji (działania prowadzone bez wypowiedzenia wojny); czwarty – operacje z użyciem wszystkich rodzajów wojsk, których celem jest

⁴³ И.В. Бочарников, С.В. Лемешев, Г.В. Люткине, *Современные концепции войн...*, s. 64–65.

⁴⁴ Tamże, s. 65–67.

⁴⁵ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, nr 8, s. 2.

⁴⁶ M. Wojnowski, *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 13, s. 14.

zniszczenie militarno-ekonomicznego potencjału zaatakowanego państwa przy zastosowaniu systemów precyzyjnych uderzeń oraz metod i form właściwych w prowadzeniu wojny psychologicznej oraz informacyjnej⁴⁷.

Walerij Gierasimow podkreślał szczególną rolę działań asymetrycznych i nieregularnych na każdym etapie konfliktu. Oprócz działań partyzanckich, sabotażowych czy charakterystycznych dla akcji terrorystycznych zaliczył do nich również wykorzystanie tzw. potencjału protestu, czyli sił opozycji wewnętrznej oraz mniejszości narodowych i religijnych w danym kraju⁴⁸. Wykorzystanie tych sił wobec ewentualnego przeciwnika pozwoli na destabilizację celu agresji i osłabienie jego potencjału nie tylko militarnego, lecz także politycznego i gospodarczego. Aby to zrealizować, zdaniem Gierasimowa należy sięgnąć po narzędzia z arsenału wojny informacyjnej i psychologicznej. Te rozważania nie są, co należy podkreślić, żadnym novum w rosyjskiej teorii wojen. Prowadzenie działań nieregularnych i operacji o charakterze wywrotowym, dywersyjnym, sabotażowym czy terrorystycznym praktykowano przez ponad 70 lat istnienia Związku Sowieckiego. Dezinformacja, inspiracja, manipulowanie społeczeństwami⁴⁹ (środki aktywne), dywersja, akty terroru (skrytobójstwa), działania nieregularne (tzw. wywiad aktywny) na trwałe weszły do arsenału wykorzystywanego przez Rosjan nie tylko wobec przeciwników politycznych, lecz także przeciwko państwom sąsiednim i wszystkim tym, które sklasyfikowano jako wrogie⁵⁰. Szczególne zaniepokojenie powinno budzić to, że położono wyjątkowo duży nacisk na stosowanie narzędzi z zakresu wojny informacyjnej na każdym etapie przyszłych wojen. W ujęciu Gierasimowa szeroko rozumiana walka informacyjna to odrębny rodzaj konfrontacji prowadzonej za pośrednictwem środków informacyjno-technicznych i informacyjno-psychologicznych praktycznie we wszystkich sferach działalności państwa (politycznej, ekonomicznej, dyplomatycznej, humanitarnej, wojskowej) oraz podczas wojny⁵¹.

Koncepcja wojny nowej generacji stała się przedmiotem rozważań również dwóch wybitnych ekspertów wojskowych: pułkownika Siergieja Czekinowa i generała lejtnanta w stanie spoczynku Siergieja Bogdanowa. Wspólnie dokonali oni oceny tendencji, które mają dominować w walce zbrojnej w XXI wieku. Według nich w bieżącym stuleciu nastąpił wzrost znaczenia broni skonstruowanej na podstawie sztucznej inteligencji, nanotechnologii oraz zrobotyzowanych kompleksów

⁴⁷ Gierasimow podkreślał, że w wojnach przyszłości nastąpi dalsza robotyzacja pola walki, dlatego za niezbędne uznał prowadzenie prac badawczych nad wykorzystaniem sztucznej inteligencji w systemach bojowych. Zob. *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces*, „Military Review” 2016, January–February, s. 26.

⁴⁸ В. Герасимов, *Ценность науки...*, s. 3.

⁴⁹ M. Wojnowski, *Koncepcja „wojny nowej generacji”...*, s. 15.

⁵⁰ Patrz: J. Darczewska, P. Żochowski, *Środki aktywne. Rosyjski towar eksportowy*, Warszawa 2017.

⁵¹ M. Snegovaya, *Putin's Information Warfare in Ukraine. Soviet origins of Russia's Hybrid Warfare*, Washington 2015, s. 11–12; M. Galeotti, *Hybrid War or Gibrinaya Voina? Getting Russia's non-linear military challenge right*, b.m.w. 2016, s. 44–47.

broni perspektywicznej generacji⁵². Chodzi szczególnie o broń geofizyczną (która umożliwia oddziaływanie na litosferę, atmosferę i jonosferę, wpływanie na zmiany klimatyczne i erupcję wulkanów, inicjowanie trzęsień ziemi i gwałtownych zmian odnoszących się do zjawisk pogodowych⁵³), a także broń wiązkową, laserową, plazmową i psychotroniczną.

Ponadto w opinii rosyjskich ekspertów rewolucja technologiczna przyniosła istotny wzrost roli sił i środków działających w sferze powietrzno-kosmicznej (co przewidział m.in. I. Kapitaniec) oraz zwiększenie znaczenia informacji we wszystkich fazach działań militarnych. Nastąpiło również skrócenie zarówno czasu przygotowania operacji, jak i realizacji zadania (lub zadań) bojowych. Było to możliwe dzięki zastosowaniu nowoczesnych systemów dowodzenia pozwalających dowódcy na wgląd w sferę działania pojedynczego żołnierza znajdującego się na polu walki⁵⁴.

S. Czekinow i S. Bogdanow, uwzględniając tezy Walerija Gierasimowa, w październiku 2013 r. przedstawili rozszerzoną i autorską koncepcję wojny nowej generacji. Zaproponowany przez nich model został zawarty w ośmiu następujących po sobie fazach:

- 1) prowadzenie działań asymetrycznych;
- 2) dezinformacja przywództwa politycznego i dowództwa sił zbrojnych przez tzw. aktywne oddziaływanie za pomocą kombinowanych – jawnych i tajnych – działań (operacji) specjalnych prowadzonych zarówno przez szeroko rozumiane media, jak i wyspecjalizowane agendy, w tym służby specjalne;
- 3) zdeintegrowanie systemu politycznego i wojskowego (np. przez zastraszanie, oszukiwanie i korumpowanie przedstawicieli elit przywódczych i wojska);
- 4) zastosowanie na skalę operacyjno-strategiczną narzędzi wojny informacyjnej i psychologicznej wraz z oddziaływaniem wywrotowym i dywersyjno-sabotażowym (terrorystycznym);
- 5) ustanowienie strefy zakazu lotów nad terytorium zaatakowanego państwa, blokada dróg, mostów i węzłów komunikacyjnych, z jednoczesnym wykorzystaniem organizacji o charakterze najemniczym oraz przeciwników ustroju społecznego i porządku politycznego kraju stanowiącego cel agresji;
- 6) konwencjonalne działania bojowe poprzedzone operacjami sił specjalnych i oddziaływaniem radioelektronicznym (WRE), psychologicznym oraz wywiadowczym;
- 7) zintensyfikowanie działań militarnych, ze wsparciem narzędzi wojny informacyjnej;
- 8) przejęcie kontroli nad obiektami newralgicznymi i punktami oporu; likwidacja zgrupowań przeciwnika, zajęcie, oczyszczenie i utrzymanie zajętego obszaru (przez końcowe operacje sił lądowych i powietrzno-desantowych)⁵⁵.

⁵² В. Герасимов, *Ценность науки...*, s. 2–3; М. Snegovaya, *Putin's Information Warfare in Ukraine...*, s. 15–17; P. Eronen, *Russian Hybrid Warfare: How to Confront a New Challenge to the West*, Washington 2016, s. 7.

⁵³ M. Wojnowski, *Mit „wojny hybrydowej”...*, s. 16.

⁵⁴ Tamże.

⁵⁵ С.Г. Чекинов, С.А. Богданов, *О характере и содержании войны...*, s. 16–23.

Jak można zauważyć, obie propozycje, tj. Gierasimowa oraz Czekinowa i Bogdanowa, wzajemnie się uzupełniają i jednocześnie stanowią usystematyzowany rosyjski pogląd na przyszłe pole walki zarówno w wymiarze taktycznym, jak i strategicznym. Co istotne, są też próbą odpowiedzi na propozycje zachodnie, zwłaszcza teoretyków amerykańskich. Jeśli spróbować szczegółowej analizy teoretycznych podstaw definicji Hoffmanowskiej oraz koncepcji Gierasimowa, a także Czekinowa i Bogdanowa, to dostrzega się, że zasadnicze różnice nie wynikają z odrębnych poglądów na sposób prowadzenia działań militarnych, tylko z mentalności autorów oraz z ich postrzegania rzeczywistości, co jest ściśle związane z historią i kulturą narodów, które reprezentują.

Wojna hybrydowa a konflikt ukraiński

Niewątpliwie konflikt ukraiński charakteryzuje się wieloma cechami zbieżnymi z klasyczną definicją opisującą omawiane zjawisko. Czy ta zbieżność musi jednak stanowić o tym, że współcześnie oraz w przyszłości będzie się określać wojnę na Ukrainie jako podręcznikowy przykład wojny hybrydowej i równocześnie wskazywać Rosję jako państwo, które po raz pierwszy zastosowało jej elementy w praktyce? Jeśli nawet zgodzić się z tezą, że zaangażowanie FR w konflikt przybrało cechy prowadzenia działań hybrydowych, to wątpliwości co do charakteru konfliktu nadal pozostaną. Nie ulega wątpliwości, że Rosja zajęła Krym i stosowała w toku swoich działań nowe formy i sposoby prowadzenia operacji charakterystycznych dla konfliktów hybrydowych. Również i jej zaangażowanie w rebelię we wschodnich prowincjach Ukrainy pozostaje bezdyskusyjne. Jednak wiele aspektów Hoffmanowskiej terminologii nie pokrywa się z wydarzeniami, do których doszło w ramach ukraińskiego konfliktu. Zatem dalsze definiowanie tych wydarzeń wydaje się uproszczeniem i jest raczej elementem szeroko zakrojonej wojny informacyjnej prowadzonej zarówno przez Rosję, jak i Zachód oraz samą Ukrainę. Trzeba więc podkreślić, że konflikt ukraiński należy definiować raczej jako wojnę domową lub wojnę buntowniczą, w której zastosowano nowe, połączone formy i sposoby prowadzenia działań militarnych zarówno konwencjonalnych (jednak bez udziału bezpośredniego podmiotów prawa międzynarodowego), jak i innych metod pozamilitarnych. Zwłaszcza termin *wojna domowa* znajduje uzasadnienie. W jego klasycznym rozumieniu mamy bowiem do czynienia z konfliktem politycznym i etnicznym realizowanym przy pomocy walki zbrojnej w obrębie jednego państwa. Przy czym udział gracza (podmiotu) zewnętrznego nie narusza podstaw zasadności użycia tego terminu do opisu zdarzeń związanych z konfliktem ukraińskim. W przeszłości mieliśmy co najmniej kilka przykładów wojny domowej z udziałem nawet kilku podmiotów zewnętrznych, a przebieg tych konfliktów charakteryzował się wystąpieniem podstawowych cech zjawiska hybrydowości wojen. Z pewnością takim przykładem może być wojna domowa w Hiszpanii w latach 1936–1939. W tym przypadku można mówić o klasycznym przykładzie starcia zbrojnego pomiędzy dwiema opcjami politycznymi, które w walce stosowały różne formy działań bojowych i korzystały z różnych metod, w tym pozamilitarnych. Oprócz

działań klasycznych występowały tu elementy wojny partyzanckiej, działań nieregularnych (dywersji, sabotażu), wojny informacyjnej i psychologicznej. Jednej i drugiej stronie pomocy udzielili aktorzy zewnętrzni, którzy również prowadzili nie tylko walkę zbrojną, lecz także psychologiczną oraz informacyjną, chociaż intensywność i zasięg tych walk były ograniczone możliwościami technologicznymi. Można więc teoretycznie znaleźć wiele podobieństw między konfliktami ukraińskim i hiszpańskim:

- po pierwsze, i wojna na Ukrainie, i w Hiszpanii stanowią poligon zarówno dla Rosji, jak i dla Zachodu;
- po drugie, i w jednym, i w drugim konflikcie biorą udział jednostki paramilitarne, nieregularne i ochotnicze, w tym aktorzy zewnętrzni;
- po trzecie, strony konfliktu prowadzą zacieklą walkę o rząd dusz i jednocześnie intensywnie oddziałują na światową opinię publiczną;
- po czwarte, w przypadku obu wojen są prowadzone działania konwencjonalne i nieregularne (partyzanckie).

Warto zauważyć, że elementem różnicującym obie wyżej wymienione wojny jest charakter stron konfliktu. W przypadku Hiszpanii mamy do czynienia z przeciwnikami politycznymi, nie ma ingerencji państwa sąsiedniego, a u podstaw wojny leży przede wszystkim konflikt ideologiczny i – w pewnym zakresie – religijny oraz społeczny. U podstaw wydarzeń na Ukrainie natomiast w pierwszej fazie mieliśmy do czynienia z konfliktem politycznym ze znacznym zaangażowaniem państwa – sąsiada, który na kolejnych etapach przerodził się (lub raczej rozwinął) w konflikt etniczny mający charakter buntu (formy wojny buntowniczej charakterystycznej dla wojen domowych). Z pewnością występują tu również liczne różnice natury historycznej. Są to przede wszystkim uwarunkowania właściwe dla Hiszpanii połowy lat 30. XX w. oraz dla Ukrainy drugiej dekady XXI wieku. Dlatego, co należy podkreślić, przykład hiszpańskiej wojny domowej stanowi w tym wypadku tylko i wyłącznie hipotezę wskazującą na pewne podobieństwa, jeśli chodzi o zjawisko wojny domowej.

Powracając do rozważań nad hybrydowością konfliktu ukraińskiego, należy zauważyć, że jest on przykładem zastosowania nowych form prowadzenia działań kombinowanych charakterystycznych dla nowych wojen XXI wieku. Casus Ukrainy jednoznacznie udowadnia, że efektywność wykorzystania różnych form oddziaływania militarnego i pozamilitarnego (hybrydowego) w ramach prowadzonych operacji okazał się skuteczny⁵⁶ tylko dlatego, że celem agresji było państwo słabe, niemające trwałych

⁵⁶ Krzysztof Wąsowski uważa (za: *Military Balance 2015*), że w trakcie działań prowadzonych przez Rosję na Ukrainie wystąpiły trzy cechy wojny hybrydowej. Zaliczył do nich: 1) prowadzenie działań konwencjonalnych, psychologicznych, informacyjnych i operacji sił specjalnych; 2) oddziaływanie w cyberprzestrzeni; 3) oddziaływanie w sferach politycznej i gospodarczej. Jednocześnie wyszczególnił aż dziewięć grup (atrybutów) charakterystycznych dla metod hybrydowych, do których zaliczył m.in.: asymetryczność, niejednoznaczność i wojnę przez pośredników (nieregularność). Taki podział, chociaż interesujący i z pewnością autorski, jest w swej zawartości merytorycznej mieszaniną różnych form i metod prowadzenia działań militarnych i pozamilitarnych, dość dowolnie przypisanych. Powoduje również chaos pojęciowy i problemowy. Zob. K. Wąsowski, *Istota i uniwersalność rosyjskiego modelu wojny hybrydowej wykorzystanego na Ukrainie*, „Sprawy

instytucji demokratycznych, i – co najważniejsze – rozdarte licznymi konfliktami wewnętrznymi, które pogłębiały się w krótkiej historii tego państwa. Niebagatelne znaczenie dla rozwoju konfliktu miał tu również brak doświadczeń państwowotwórczych i tym samym wzorców, które wsparłyby elity polityczne w procesie transformacji systemowej. Ukraina, od samego początku istnienia, budując swoją państwowość, przyjęła wzorce wschodnie. Dlatego tylko kwestią czasu pozostawało, kiedy dojdzie do konfliktu wewnętrznego, który, jak się okazało, omal nie doprowadził do rozpadu tego kraju.

Rosja niewątpliwie doskonale przygotowała się do wydarzeń, do których doszło w 2014 r. Wykorzystała słabość swojego sąsiada: wcześniej dobrze rozpoznała jego scenę polityczną i wręcz stymulowała niektóre sytuacje. Działając na podstawie sprawdzonych wzorców, w bezkruwawy sposób przejęła kontrolę nad Krymem. Była to praktyczna realizacja niektórych elementów doktryny Gierasimowa. Według niesprawdzonych informacji, zarówno przed rozpoczęciem działań aneksyjnych, jak i w trakcie operacji krymskiej znaczna część Ukrainy została obłożona osłoną radioelektroniczną i poddana zorganizowanemu uderzeniu w cyberprzestrzeni⁵⁷, które w znacznym stopniu uniemożliwiło jakiekolwiek kierowanie administracją rządową i sektorem bezpieczeństwa wewnętrznego oraz militarnego na Półwyspie. Ponadto wcześniej dokonano rozpoznania taktycznego oraz rozpracowano wywiadowczo wszystkie poziomy kierowania państwem: od poziomu centralnego po miejski⁵⁸. W perfekcyjny sposób wykorzystano niechęć ludności rosyjskojęzycznej do władz ukraińskich i logistycznie przygotowano siły opozycyjne. Wszystko odbyło się pod czujnym okiem administracji państwowej i służb bezpieczeństwa Ukrainy⁵⁹. Jednak

Międzynarodowe” 2015, nr 2, s. 45–47.

⁵⁷ Według niektórych zachodnich ekspertów Rosja miała po raz pierwszy wykorzystać operacje w cyberprzestrzeni podczas sporu politycznego w 2007 r. w Estonii w związku z likwidacją symboli okupacji radzieckiej w przestrzeni publicznej oraz w czasie wojny z Gruzją w 2008 r. Zaznaczono jednak, że działania hakerskie wobec Estonii miały charakter nieskoordynowany i najprawdopodobniej nie były nadzorowane przez służby specjalne FR, czyli – jeśli wierzyć ekspertom – była to tzw. oddolna inicjatywa rosyjskich patriotów (hakerów). Zupełnie inaczej miała się przedstawiać sytuacja związana z atakami na systemy informatyczne Gruzji przed jej zaatakowaniem. Nie dość, że zablokowano wówczas część sieci użytkowanych przez instytucje rządowe, to jeszcze miało wprowadzić dane świadczące o przygotowaniach sił zbrojnych do ofensywy przeciwko Gruzji. Za tymi poczynaniami, według m.in. Pasi Eronena, stali rosyjscy hakerzy oraz członkowie nacjonalistycznych grup młodzieżowych. Opisany scenariusz działań przypomina modus operandi charakterystyczny dla działań aktywnych inspirowanych, prowadzonych przez radzieckie (rosyjskie) służby specjalne. Zob. *Georgia on Their Minds*, „The Wall Street Journal” 2009, October 1, http://www.wsj.com/articles/SB1000142405274870447150457444658_2129281924 [dostęp: 12 I 2018]; A. Hagen, *The Russo-Georgian War 2008*, w: J. Healey, K. Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Arlington 2013, s. 196–200; P. Eronen, *Russian Hybrid Warfare...*, s. 8.

⁵⁸ Mark Galeotti ocenił, że na wschodniej Ukrainie FSB perfekcyjnie spenetrowało ukraiński aparat bezpieczeństwa i jednocześnie prowadziło działania stymulujące do dezercji, monitorując planowanie i działania władz z Kijowa. Zob. M. Snegovaya, *Putin's Information Warfare in Ukraine...*, s. 12.

⁵⁹ Tym samym, jak zauważają polscy i zachodni eksperci, wyczerpano definicyjne podstawy wojny hybrydowej w odniesieniu do konfliktu ukraińskiego.

nie powinno to być zaskoczeniem dla większości analityków, którzy z uwagą obserwowali sytuację w tym kraju i zmiany, jakie zachodziły w systemie obronnym Federacji Rosyjskiej. Pogłębiający się chaos wewnętrzny na Ukrainie, liczne nierozwiązane konflikty społeczne, powszechna korupcja, bezrobocie, ciągłe konflikty z Rosją i brak jakichkolwiek perspektyw na poprawę życia zwykłych obywateli wraz z rozpasaniem oligarchów rujnujących państwo, przypominających kozackich watażków, którzy grasowali na Kresach Rzeczypospolitej, były swoistą wizytówką Ukrainy od zarania jej istnienia⁶⁰. Ponadto niedoinwestowane służby policyjne i specjalne oraz siły zbrojne w żaden sposób nie były w stanie przeciwstawić się przeciwnikowi. Aparat administracyjny został z jednej strony skorumpowany przez oligarchów, a z drugiej – zinfiltrowany przez służby rosyjskie⁶¹. Aby nie być gołosłownym, należy przytoczyć słowa generała lejtnanta A. Skipalskiego, twórcy kontrwywiadu wojskowego Ukrainy i byłego zastępcy szefa SBU: *Za Janukowycza niemal wszyscy szefowie ukraińskich struktur siłowych i specnazu należeli do Związku Żołnierzy Desantu FR, na czele którego stoi jeden z zastępców ministra obrony Rosji. Większość tych osób do tej pory pozostaje na swoich wysokich stanowiskach*⁶².

A oto jak generał Skipalski oceniał samo SBU: *Posiadamy strukturę z wrodzonymi elementami nieprofesjonalności i korupcji, a do tego nasyconą antyukraińskim, prorosyjskim, złodziejsko-amoralnym elementem (...). Byli funkcjonariusze KGB, którzy pozostali, aby pracować w naszym państwie, nie przeciwdziałali, ale sprzyjali antyukraińskim nastrojom w działalności rosyjskich służb specjalnych*⁶³.

Należy zauważyć, że Skipalski, oceniając kondycję ukraińskich służb specjalnych, w rzeczywistości ocenił stan państwa. Bo cóż można powiedzieć o państwie, którego szef służb specjalnych dezerteruje i znajduje schronienie u wrogiego sąsiada. Tym szefem był A.G. Jakimienko, absolwent Akademii Sił Powietrznych im. J. Gagarina, do 1998 r. kadrowy oficer Armii Rosyjskiej (tak – Rosyjskiej). Do czasów Majdanu kierował on najsilniejszą i najbardziej wpływową służbą specjalną Ukrainy, a także miał wiedzę dotyczącą funkcjonowania całego systemu

⁶⁰ Pod względem PKB na głowę mieszkańca Ukraina była i nadal pozostaje jednym z najbiedniejszych krajów Europy. Według danych MFW z 2013 r. PKB na głowę mieszkańca Ukrainy wyniosło 3,9 tysiąca USD. Dla porównania: w Estonii – 18 tysięcy USD, w Rosji – 15 tysięcy USD, w Polsce – 13 tysięcy USD, na Białorusi – 7,4 tys. USD. W 2016 r. Ukraina miała PKB na jednego obywatela w wysokości 2185 tys., a Białoruś prawie 5 tys. USD. W tym samym roku rosyjskie PKB szacowane było na ok. 8,7 tys., a Polski na ponad 12,3 tys. USD. Uczynić Ukrainę z jej czarnoziemem, zasobami naturalnymi, rzekami i morzami dwa razy biedniejszą od jałowej Białorusi – to wynik unikalny, którego ani żaden król czy hetman, ani nawet sekretarz generalny nie osiągnęli.

⁶¹ W 2010 r., po objęciu rządów przez Janukowycza, szefem SBU został Walerij Choroszkowski, który niejednokrotnie podkreślał w udzielanych wywiadach prasowych, że za dobrą współpracą z FSB kryje się *wspólna czekistowska przeszłość*. Jej wyrazem było podpisanie w maju 2010 r. umowy o współpracy z FSB i jednocześnie zerwanie kontaktów z CIA oraz zaprzestanie działań przeciwko rosyjskim służbom specjalnym na terytorium Ukrainy.

⁶² М. Солонин, *Проект «Новороссия» – утопи*, „Военно-промышленный курьер” 2014, nr 38, s. 11.

⁶³ Tamże.

bezpieczeństwa państwa ukraińskiego. Jak to się zatem stało, że decydenci polityczni na czele tak newralgicznej instytucji postawili Rosjanina? Częściowa odpowiedź widnieje we wpisie, jaki tow. Jakimienko zamieścił w internecie: *Po ukończeniu akademii zrozumiałem, że moje umiejętności są nikomu niepotrzebne. To się zwolniłem. A te pacany zauważyli (sic!), powołali ponownie, no i ciągnę ten wózek*⁶⁴.

„Te pacany” przyjęły byłego rosyjskiego oficera na służbę do zarządu SBU Doniecka, następnie wyznaczyły na stanowisko naczelnika SBU Sewastopola, aby ponownie skierować go do Donbasu, gdzie został naczelnikiem Zarządu Donieckiego. Dnia 9 stycznia 2013 r. Jakimienko został szefem SBU, co z uwagi na zajmowane przez niego stanowisko oznaczało automatyczne członkostwo w Radzie Bezpieczeństwa Narodowego i Obrony, czyli tym samym uzyskał on dostęp do wszystkich sekretów wywiadowczych i wojskowych Ukrainy. W dniu 24 lutego 2014 r., po obaleniu Janukowycza, zbiegł do Rosji, gdzie się ukrywa po dziś dzień⁶⁵. Komentarz jest raczej zbyteczny.

Nie tylko służby specjalne stanowiły piętę achillesową Ukrainy. W niewiele lepszej kondycji była ukraińska armia. Stan sił zbrojnych tego kraju (dalej: SZU) w dobie konfliktu najlepiej oddaje myśl przypisywana jednemu z chińskich filozofów: *Armia baranów pod dowództwem lwa znaczy więcej, niż armia lwów pod dowództwem barana*. Co należy na wstępie podkreślić, SZU zostały spenetrowane przez rosyjski wywiad w takim samym stopniu, jak pozostałe elementy struktur siłowych państwa ukraińskiego. Trzeba się zgodzić ze stwierdzeniem Andrzeja Wilka, znakomitego eksperta ds. problematyki polityczno-wojskowej Europy Wschodniej, że Ukraina miała blisko ćwierć wieku, aby stworzyć sprawne siły zbrojne od podstaw. Konflikt w Donbasie oraz zajęcie Krymu wykazały jednak, że to państwo wiosną 2014 r. nie dysponowało wystarczającym potencjałem bojowym (militarnym), aby zapobiec aneksji Półwyspu oraz buntowi we wschodnich prowincjach⁶⁶. Nieformalne powiązania między kadrami armii ukraińskiej a rosyjską nigdy nie zostały zerwane, czego konsekwencją było m.in. przejście znacznej części ukraińskiej kadry na stronę rosyjską po zajęciu Krymu. Niebagatelne znaczenie miały też zmiany obserwowane przez ukraińskich oficerów, jakie zachodziły w siłach zbrojnych wschodniego sąsiada, zwłaszcza w sferze ekonomicznej. Armia ukraińska, począwszy od 2010 r., była w permanentnej zapaści. Korupcja, niedofinansowanie (budżet na poziomie ok. 1 proc.⁶⁷) oraz rezygnacja z integracji z NATO tylko ten proces pogłębiły. Reformy, które zainicjowano jeszcze w latach 90. XX w., w związku z brakiem środków finansowych zostały ograniczone. Również

⁶⁴ Tamże.

⁶⁵ Tamże.

⁶⁶ A. Wilk, *Najlepsza armia, jaką miała Ukraina. Zmiany w Siłach Zbrojnych Ukrainy po agresji rosyjskiej*, Warszawa 2017, s. 8.

⁶⁷ Jeszcze w 2006 r. budżet oscylował w granicach 1,36–1,74% PKB, aby trzy lata później osiągnąć wartość 0,79%, a w następnych latach ok. 1% – przy postępującej degradacji sprzętu i zmniejszającej się liczbie poborowych, a po wprowadzeniu służby zawodowej – przy braku zainteresowania obywateli Ukrainy służbą w siłach zbrojnych. Zob. D. Sanders, „*The War We Want. The War That We Get*”: *Ukraine’s Military Reform and the Conflict in the East*, „Journal of Slavic Military Studies” 2017, t. 30, nr 1, s. 33–34.

decyzje kadrowe nie sprzyjały procesom restrukturyzacyjnym. Obraz stanu SZU w 2011 r. oddają słowa A. Gricenki, byłego szefa Komitetu Rady Najwyższej ds. Bezpieczeństwa i Obrony: *Obecnie w SZU nie ma ani jednego batalionu o zdolności bojowej, ani jednej zdolnej do walki eskadry, w armii mamy obecnie 22 tysiące wakatów, na które nikt nie chce się zaciągnąć. Brakuje oficerów niższego i średniego szczebla. Dowódca jednostki otrzymuje nieco więcej niż kasjer w supermarkecie*⁶⁸. Nie brakowało natomiast generałów – 450, w tym generałów armii (najwyższy stopień w SZU) było 14⁶⁹. Profesjonalizm kadr kierowniczych i dowódczych także nie odpowiadał realiom XXI wieku. Wystarczy wskazać dwa przykłady: pierwszy – wyznaczenie na stanowisko ministra obrony biznesmena Pawła Lebediewa, drugi – powierzenie dowództwa Marynarki Wojennej Ukrainy adm. Denisowi Bieriezowskiemu, który po mianowaniu przeszedł na stronę rosyjską⁷⁰. Nie był to zresztą jedyny oficer ukraiński, który porzucił służbę w ukraińskiej armii na rzecz Sił Zbrojnych FR.

Jak zatem rozbita wewnętrznie, zinfiltrowana oraz targana konfliktami Ukraina mogła się przeciwstawić potężnemu sąsiadowi? Odpowiedź wydaje się prosta: nie była w stanie. Co więcej, praktycznie żadne państwo, może z wyjątkiem Stanów Zjednoczonych, nie poradziłoby sobie z agresją opartą na stosowaniu narzędzi i metod hybrydowych w skali strategicznej. Być może część państw zaliczających się do tzw. starych demokracji w końcu odparłaby ewentualny atak, ale jego skutki trudno oszacować. Natomiast przypadek Ukrainy pokazuje, że słabość instytucji demokratycznych połączona z brakiem doświadczeń państwowotwórczych jest jednym z zasadniczych czynników sprzyjających dezintegracji państwa. Dlatego też nie należy doszukiwać się istnienia jakiegoś specjalnego planu (strategii) w odniesieniu do poczynań Moskwy wobec państwa ukraińskiego. I trzeba zgodzić się (przynajmniej częściowo) z niektórymi ocenami rosyjskich polityków oraz ekspertów, którzy twierdzą, że Rosja zarówno na Krymie, jak i we wschodnich obwodach Ukrainy nie stosowała i nie stosuje żadnych nowych form i metod walki, ani rozwiązań taktycznych, które Zachód definiuje jako wojnę hybrydową. Taką opinię wyraża m.in. dyrektor Centrum Analiz Strategii i Technologii w Moskwie – Rusłan Puchow⁷¹. Jego oceny są tylko częściowo prawdziwe. Rosjanie rzeczywiście nie stosowali żadnych nowych metod prowadzenia działań, które można opisać jako destabilizujące i dezintegrujące państwo. Wykorzystali doświadczenia z przeszłości, zarówno z historii własnych sił zbrojnych i służb specjalnych, jak i korzystali z doświadczeń Zachodu (przede wszystkim Stanów Zjednoczonych). W ten sposób wypracowali swój model prowadzenia wojny w warunkach epoki globalizacji.

W podsumowaniu trzeba stwierdzić, że poglądy i oceny Puchowa wpisują się w nową rosyjską doktrynę wojny przyszłości. Przy czym należy zgodzić się z opinią rosyjskiego naukowca, który właściwie ocenił kondycję wojsk ukraińskich, twierdząc,

⁶⁸ М. Солонин, *Проект «Новороссия»...*, s. 11.

⁶⁹ Tamże.

⁷⁰ A. Wilk, *Najlepsza armia, jaką miała Ukraina...*, s. 10.

⁷¹ Р. Пухов, *Миф о «гибридной войне». Никаких принципиально новых действий наша армия в Крыму и на Украине не вела*, „Независимое военное обозрение” 2015, nr 19, s. 1.

że Rosjanie nie musieli prowadzić mniej lub bardziej zaawansowanych operacji informacyjnych w związku z niewielkim stopniem z informatyzowania i dysponowania archaicznym sprzętem, w który była wyposażona armia ukraińska, a zwłaszcza jej jednostki stacjonujące na Krymie. Natomiast inne oceny i analizy Puchowa niewątpliwie należy uznać za celowe dezinformowanie opinii społecznej, wpisujące się w rosyjski model walki informacyjnej.

Przy analizie konfliktu ukraińskiego należy zwrócić uwagę na jeszcze jeden, jak się wydaje, ciekawy aspekt. Oceniając przebieg wydarzeń, począwszy od wybuchu protestów na Majdanie, przez aneksję Krymu, aż po walki we wschodnich prowincjach Ukrainy, ma się nieodparte wrażenie, że terytorium naszego wschodniego sąsiada stało się jednym wielkim poligonem, z którego najwięksi współcześni aktorzy stosunków międzynarodowych uczynili obszar (terytorium) do testowania nowych doktryn wojskowych (taktyki i strategii działań bojowych w warunkach współczesnego pola walki), technik, sprzętu (wyposażenia i systemów uzbrojenia), a także gier dyplomatycznych. Zarówno Rosjanie, jak i Zachód (oraz, rzecz jasna, Ukraina) prowadzą rozległą, bezpardonową wojnę informacyjną i psychologiczną, testują nowe systemy uzbrojenia, wsparcia, dowodzenia i doktrynę szkoleniową, jak również koncepcję przyszłych wojen (w tym zakresie prym wiedzie przede wszystkim Rosja). Straty, destabilizacja Ukrainy i jej dezorganizacja nie mają przy tym żadnego znaczenia dla Moskwy i świata tzw. starych demokracji. Liczy się tylko sprawdzenie: czy można ostatecznie wyeliminować Rosję jako konkurenta na rynku globalnym i w końcu ją okiełznać, aby się podporządkowała ogólnoświatowemu trendowi i porządkowi postzimnowojennemu. Nikt z politycznych przywódców najprawdopodobniej nie zdaje sobie sprawy z tego, jak będzie wyglądała rzeczywistość po kryzysie ukraińskim i w jakim stopniu zostaną wykorzystane doświadczenia zdobyte w wyniku wojny na Ukrainie w sferze militarnej i politycznej. Niewątpliwie oprócz strat i szkód materialnych oraz ludzkich państwo ukraińskie poniosło znacznie większy uszczerbek w sferze mentalnej i państwowotwórczej, co zresztą ma swoje odniesienie do pozamilitarnych działań hybrydowych. Pomimo wymiany rządzących i, jak się wydaje, otwarcia na Zachód, wewnętrzna sytuacja Ukrainy nadal jest skomplikowana. Pozostaje ona państwem skorumpowanym, de facto rządzone przez *familiję*, z trudem odbudowującym wiarygodność wśród obywateli i potencjał militarny. I chociaż intensywność walk znacznie osłabła, nie oznacza to, że rozwiązanie kryzysu i konfliktu niesie nadzieję na pokojowe zakończenie wojny. Wręcz przeciwnie – strony konfliktu są w poważnym impasie, a wojna hybrydowa przerozdziła się w wojnę pozycyjną.

Rekomendacje

Należy jasno zdać sobie sprawę z tego, że szeroko rozumiany Zachód wkroczył w bodaj najbardziej burzliwą erę agresywnej konfrontacji, która ma na celu obalenie fundamentalnych podstaw demokratycznych modeli i instytucji. Asymetryczno-

-hybrydowa sztuka wojenna, pomimo braku odpowiedniego potencjału militarnego, umożliwia bowiem mniej potężnym graczom przeprowadzenie wielu efektywnych uderzeń i w pewnych sprzyjających okolicznościach przejęcie inicjatywy zarówno na poziomie taktycznym, jak i strategicznym. Trzeba także pamiętać o tym, że jeszcze groźniejszym przeciwnikiem stosującym rozwinięte techniki i narzędzia hybrydowe będzie państwo, które ma wypracowaną doktrynę (koncepcję) działań i środki oraz jest zdeterminowane, aby dla osiągnięcia celów politycznych użyć ich zwłaszcza w stosunku do przeciwnika potencjalnie słabszego.

Niewątpliwie Stany Zjednoczone, UE oraz NATO dysponują odpowiednimi środkami uniemożliwiającymi Rosji prowadzenie operacji hybrydowych, ale marnotrawstwem byłoby podjęcie decyzji o przeciwdziałaniu każdemu ruchowi naszego wschodniego sąsiada, której strategia obejmuje inspirowanie działań Zachodu i wymuszanie udziału w kosztownych operacjach. Zamiast tego Zachód powinien wyraźnie zidentyfikować najważniejszą dla niego infrastrukturę strategiczną i ekonomiczną oraz podjąć efektywne działania mające na celu eliminowanie i osłabianie możliwości prowadzenia operacji hybrydowych przez Rosjan. W tym świetle należy podjąć na szeroką skalę działania wywiadowcze, m.in. takie, które będą w stanie trwale eliminować możliwości Kremla i ograniczać jego zdolność do prowadzenia działań informacyjnych oraz psychologicznych. Przez wykorzystanie własnych narzędzi asymetrycznych i hybrydowych trzeba skutecznie ograniczać potencjał i wpływy wynikające z rosyjskiej koncepcji Gierasimowa. A ponadto należy:

- budować (tworzyć) krajowe i międzynarodowe centra koordynacyjne do obrony hybrydowej;
- prowadzić badania naukowe ukierunkowane na tworzenie struktur i procedur zdolnych do przeciwstawienia się zagrożeniom hybrydowym i asymetrycznym na każdym poziomie oraz do ich użycia;
- prowadzić badania w obszarach strategicznych inwestycji Rosji, rozpoznawać je i niwelować ich wpływy;
- wprowadzić nowe, zastrzone procedury i rozwiązania prawne dotyczące szeroko rozumianego bezpieczeństwa cybernetycznego i bezpieczeństwa informacji;
- prowadzić zróżnicowaną i efektywną kampanię propagandową w odniesieniu do opinii społecznej zarówno Zachodu, jak i Rosji;
- rozwijać defensywne zdolności i sojusze w ramach wojny gospodarczej;
- rozwijać zdolności i narzędzia antykorupcyjne.

Bibliografia:

1. Blaker J., *Understanding the revolution in military affairs : A guide to America's 21st century defense military affairs*, Washington 1997, Progressive Policy Institute.

2. Darczewska J., Żochowski P., *Środki aktywne. Rosyjski towar eksportowy*, Warszawa 2017, OSW.
3. Dębczak A., Pawlak C., Kaplin J., *Analityczny model oceny hybrydowości współczesnych konfliktów*, „Zeszyty Naukowe AON” 2015, nr 2.
4. Eronen P., *Russian Hybrid Warfare: How to Confront a New Challenge to the West*, Washington 2016, FOUNDATION FOR DEFENSE OF DEMOCRACIES.
5. Freier N., *The Defense Identity Crisis: It's a Hybrid World*, „Parameters” 2009, nr 3.
6. Galeotti M., *Hybrid War or Gibrinaya Voina? Getting Russia's non-linear military challenge right*, b.m.w. 2016, Mayak Intelligence.
7. *Georgia on Their Minds*, „The Wall Street Journal” 2009, October 1, <http://www.wsj.com/articles/SB0001424052748704471504574446582129281924> [dostęp: 12 I 2018].
8. Gruszczyk A., *Hybrydowość współczesnych wojen – analiza krytyczna, w: Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapala (red. nauk.), Warszawa 2011, BBN.
9. Hagen A., *The Russo-Georgian War 2008*, w: J. Healey, K. Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Arlington 2013, Cyber Conflict Studies Association.
10. Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, nr 52.
11. Hundley R.O., *Past Revolutions, Future Transformations. What can the history of revolution in military affairs tell us about transforming the US military?*, Washington 2009, RAND.
12. Królikowski H., *Sily operacji specjalnych (Wojska Specjalne) w konfliktach hybrydowych*, „Bezpieczeństwo. Teoria i Praktyka” 2016, nr 3.
13. Lekowski M., *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*, „Bezpieczeństwo Narodowe” 2011, nr 19.
14. McCuen J.J., *Hybrid Wars*, „Military Review” 2008, t. 2.
15. Mockaitis T.R., *British Counterinsurgency in the Post-imperial Era*, London 1995, Manchester University Press.
16. Piotrowski M.A., *Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych*, „Sprawy Międzynarodowe” 2015, nr 2.
17. Reginia-Zacharski J., *Wojna w świecie współczesnym. Uczestnicy, cele, modele, teorie*, Łódź 2014, Wydawnictwo Uniwersytetu Łódzkiego.

18. Sanders D., *“The War We Want. The War That We Get”*: Ukraine’s Military Reform and the Conflict in the East, „Journal of Slavic Military Studies” 2017, t. 30, nr 1.
19. Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 14, wydanie specjalne.
20. Sloan E.C., *The Revolution in Military Affairs: Implications for Canada and NATO*, Montreal 2002, McGill-Queen’s Press.
21. Snegovaya M., *Putin’s Information Warfare in Ukraine. Soviet origins of Russia’s Hybrid Warfare*, Washington 2015, Institute for the Study of War.
22. Sołkiewicz H., *Wojna przyszłości – wojną niekontaktową (wg aktualnych poglądów rosyjskich)*, „Zeszyty Naukowe Akademii Marynarki Wojennej” 2009, nr 1.
23. *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations* General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, „Military Review” 2016, January–February.
24. Walker R.G., *SPEC FI: the United States Marine Corps and Special Operations*, Monterey 1998, Naval Postgraduate School.
25. Wąsowski K., *Istota i uniwersalność rosyjskiego modelu wojny hybrydowej wykorzystanego na Ukrainie*, „Sprawy Międzynarodowe” 2015, nr 2.
26. Vickers M, Martinage R., *The Revolution in War*, Washington 2004, The Center for Strategic and Budgetary Assessments.
27. Wilk A., *Najlepsza armia, jaką miała Ukraina. Zmiany w Siłach Zbrojnych Ukrainy po agresji rosyjskiej*, Warszawa 2017, OSW.
28. Wojnowski M., *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 13.
29. Wojnowski M., *Mit „wojny hybrydowej”. Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 14, wydanie specjalne.

Literatura rosyjska:

1. Акулинин В.Н., Епифанова Н.С, *Концепция гибридной войны в практике межгосударственного противостояния*, „Национальные интересы: приоритеты и безопасность” 2015, nr 36.

2. Бочарников И.В., Лемешев С.В., Люткене Г.В., *Современные концепции войн и практика военного строительства*, Москва 2013, ЗАО «Экон-информ».
3. Викулов С.Ф., Хрусталёв Е.Ю., *Методологические основы и специфика военно-экономического анализа*, „Экономический анализ: теория и практика” 2014, nr 7.
4. Гареев М.А., *Проблемы стратегического сдерживания в современных условиях*, „Военная мысль” 2009, nr 4.
5. Герасимов В., *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, nr 8.
6. Горбачев Ю.Е., *Кибервойна уже идет*, „Независимое военное обозрение” 2013, nr 13.
7. Горбунов В.Н., Богданов С.А., *О характере вооружённой борьбы в XXI веке*, „Военная мысль” 2009, nr 3.
8. Капитанец И., *Битва за мировой океан*, Москва 2002, Вече.
9. Пухов Р., *Миф о «гибридной войне». Никаких принципиально новых действий наша армия в Крыму и на Украине не вела*, „Независимое военное обозрение” 2015, nr 19.
10. Рогозин Д.О., *Перейти от заклинаний и воззваний к практической деятельности*, „Военно-промышленный курьер” 2013, nr 14.
11. Слипченко В.И., *Войны нового поколения: дистанционные бесконтактные*, Москва 2004, ОЛМА Медиа Групп.
12. Солонин М., *Проект «Новороссия» – итоги*, „Военно-промышленный курьер” 2014, nr 38.
13. Чекинов С.Г., Богданов С.А., *О характере и содержании войны нового поколения*, „Военная мысль” 2013, nr 10.

Abstrakt

Po zakończeniu zimnej wojny można zaobserwować gwałtowne zmiany w taktyce i prowadzeniu konfliktów oraz wojen. Zauważalne stało się narastające wzajemne przenikanie się, a także łączenie technik, wojny regularnej i nieregularnej. Współczesne konflikty militarne zarówno o charakterze regionalnym, jak i znacznie szerszym zasięgu cechuje kompleksowość zastosowania i praktycznego wykorzystania wszelkich możliwych środków walki. Ta różnorodność elementów wchodzących w taką formę

prowadzonej działalności destrukcyjnej stała się niezwykle popularnym tematem dyskursu politycznego i publicystycznego oraz została współcześnie zdefiniowana jako działania hybrydowe lub wojna hybrydowa.

Należy jasno zdać sobie sprawę z tego, że szeroko rozumiany Zachód wkroczył w bodaj najbardziej burzliwą erę agresywnej konfrontacji, która ma na celu obalenie fundamentalnych podstaw demokratycznych modeli i instytucji. Asymetryczno-hybrydowa sztuka wojenna umożliwia bowiem także mniej potężnym graczom przeprowadzenie wielu efektywnych uderzeń pomimo braku odpowiedniego potencjału militarnego i w pewnych sprzyjających okolicznościach przejęcie inicjatywy zarówno na poziomie taktycznym, jak i strategicznym.

Słowa kluczowe: wojna hybrydowa, wojny przyszłości, wojna na Ukrainie, koncepcja Gierasimowa, konflikt zbrojny, wojna asymetryczna, wojny buntownicze, wojny szóstej generacji, wojna nieregularna.

Jolanta Darczewska

Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy

Zarys zagadnienia

Presja polityczna i militarna wywierana przez Rosję na bliższe i dalsze otoczenie międzynarodowe oraz jej gotowość do eskalowania napięcia stały się w ostatnich latach jednym z głównych zagadnień dyskursu na temat bezpieczeństwa. Wysoki poziom rosyjskich zagrożeń hybrydowych¹ jest przedmiotem wielu analiz i artykułów. Nadal jednak refleksja na ten temat jest fragmentaryczna, nie obejmuje bowiem wszystkich ich aspektów i przejawów. Większość autorów skupia się na dezinformacji i propagandzie, tj. działaniach w sferze informacyjnej (przestrzeni medialnej i cybernetycznej). Tymczasem presja informacyjna stanowi wprawdzie dominujący, ale tylko jeden z instrumentów kryzysotwórczego oddziaływania Rosji. Pretekstem do jawnych i skrytych operacji medialnych stają się często celowo prowokowane incydenty wywiadowcze, graniczne, migracyjne, wydarzenia organizowane na własnym terytorium i terytoriach państw obcych (np. konferencje, festiwale, obozy pokojowe), ingerencje w wybory parlamentarne i prezydenckie, finansowe oraz polityczne wspieranie środowisk radykalnych i tendencji odśrodkowych w UE, zakłócanie procesów decyzyjnych, dyskredytacja liderów politycznych nieprzychylnych Kremlowi itp. Tego rodzaju działania w czasach zimnej wojny określano zbiorczym terminem środki aktywne². Włączenie ich do paradygmatu zagrożeń hybrydowych umożliwia poszerzenie ich postrzegania, ułatwia zdiagnozowanie i przeciwdziałanie im.

Zapobieganie zagrożeniom hybrydowym stawia kontrwywiad przed trudnym wyzwaniem. Warunkuje to złożony kompleks sił i środków wykorzystywanych przez Rosję. Zagrożenie hybrydowe to jednocześnie zagrożenie zewnętrzne i wewnętrzne, krajowe i ponadnarodowe, militarne i wywiadowcze, na które nie można odpowiedzieć symetrycznie. Operacje hybrydowe są prowadzone przez podmioty państwowe i niepaństwowe w sposób tajny i półjawny, przy wykorzystaniu metod legalnych i nielegalnych. Są realizowane zarówno w przestrzeni fizycznej, jak i informacyjno-psychologicznej. Walki z nimi nie ułatwia wojskowa terminologia („wojna informacyjna”, „wojna psychologiczna”, „wojna propagandowa”, „wojna cywilizacyjna”, „wojna polityczna”) stosowana przez rosyjskich ekspertów i dziennikarzy, sugerująca,

¹ Szczegółowo na ten temat zob. <http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html> [dostęp: 5 I 2018].

² Zob. J. Darczewska, P. Żochowski, *Środki aktywne. Rosyjski towar eksportowy*, <https://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2017-05-30/srodki-aktywne-rosyjski-towar-eksportowy> [dostęp: 5 I 2018].

że jest to wojna dwóch stron stosujących środki adekwatne. Tymczasem sytuacja jest z natury asymetryczna: operacje hybrydowe na szeroką skalę wykorzystuje agresor, podczas gdy strona atakowana – choćby ze względu na respektowanie podstawowych wolności i praw człowieka, a także wartości państwa prawa – musi znaleźć inne skuteczne metody i środki przeciwdziałania im oraz przeciwstawić narracji agresora własną, pozytywną narrację. W terminologii NATO definiuje się to jako komunikacja strategiczna. Ten termin³ ewidentnie rozszerzył swój pierwotny zakres znaczeniowy (informacyjne zabezpieczenie pola walki) i stał się swego rodzaju metodologicznym fundamentem przeciwdziałania zagrożeniom hybrydowym traktowanym według jednego, uniwersalnego wzorca. Dążąc do uspołnienia podejścia, NATO-wską terminologię przyjęła także Unia Europejska⁴.

Ponowne zainteresowanie się problematyką dotyczącą środków aktywnych⁵, obserwowane na Zachodzie, jest spowodowane nieprecyzyznością i kontrowersyjnością terminów z przydawką „hybrydowy”, a także próbą bardziej kompleksowego podejścia do hybrydowych form agresji. Wojskowa geneza tych terminów, jak się zdaje, przesłania niekiedy to, że armia nie jest jedynym (i nie głównym) uczestnikiem wojny hybrydowej: jest wykorzystywana w ograniczonym zakresie – jako argument ostateczny. W tym kontekście historyczny termin środki aktywne dobrze

³ Przywołane pojęcie komunikacja strategiczna, podobnie jak inne pojęcia stosowane w niniejszym artykule, zostało roboczo zdefiniowane w publikacji: *Mini(Słownik) BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa*, <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035...html> [dostęp: 5 I 2018]. Szerzej na temat komunikacji strategicznej zob. np. T. Kacała, *Komunikacja strategiczna*, <http://cdis.wp.mil.pl/plik/file/Publikacje/kacala.pdf> [dostęp: 5 I 2018].

⁴ Zob. np. *Komunikat UE z 6 kwietnia 2016 r. w sprawie przyjęcia wspólnych ram przeciwdziałania zagrożeniom hybrydowym i budowania odporności UE, jej państw członkowskich i krajów partnerskich, przy jednoczesnym zacieśnianiu współpracy z NATO w zakresie zwalczania tych zagrożeń*, http://europa.eu/rapid/press-release_IP-16-1227_pl.htm [dostęp: 10 XII 2017]. Ten dokument wyznaczył główne kierunki współdziałania NATO i UE: **podnoszenie świadomości społeczeństwa** przez ustanowienie specjalnych mechanizmów wymiany informacji między państwami członkowskimi i koordynację działań UE zmierzających do osiągnięcia spójnej komunikacji strategicznej; **wzmacnianie odporności** najważniejszych sektorów strategicznych, takich jak bezpieczeństwo cybernetyczne, infrastruktura krytyczna (przesyłu energii, transportu, przestrzeni kosmicznej), a także wzmocniona ochrona systemu finansowego, ochrona zdrowia publicznego oraz wspieranie wysiłków na rzecz przeciwdziałania ekstremizmowi i radykalizacji; **zapobieganie kryzysom, odpowiedź na nie i ich przezwyciężanie** (zdefiniowanie skutecznych procedur, w tym zastosowania klauzuli solidarności – art. 222 TFUE, a także klauzuli wzajemnej obrony – art. 42 ust. 7 TUE, w przypadku poważnego ataku hybrydowego o dużym zasięgu); **zacieśnienie współpracy pomiędzy UE a NATO, jak również innymi organizacjami partnerskimi** we wspólnym wysiłku ukierunkowanym na przeciwdziałanie zagrożeniom hybrydowym, przy jednoczesnym poszanowaniu zasad otwartości i niezależności procesu podejmowania decyzji każdej z organizacji.

⁵ Zob. np. С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnye-sovetskie-meropriyatiya-v-putinskoy-rossii> [dostęp: 4 I 2018]; <https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war> [dostęp: 4 I 2018]; <http://www.cyberdefence24.pl/704854.prof-andrew-wilson-rosja-jest-pewnego-rodzaju-patologicznym-panstwem-pirackim-wywiad> [dostęp: 4 I 2018].

oddaje złożoną naturę tego fenomenu i syntetyzuje różne techniki: polityczne, wojskowe, wywiadowcze, ekonomiczne, dyplomatyczne, finansowe, medialne, cybernetyczne. Podkreśla także istotną (jeśli nie najważniejszą) rolę służb wywiadowczych w przygotowaniu i budowaniu zaplecza wykonawczego operacji wpływu Rosji, a także ścisłe powiązanie tych przedsięwzięć z aktami prowokacji, dywersji, terroryzmu, międzynarodową przestępczością zorganizowaną oraz innymi przejawami działania rozkładowego. Rozpatrywany jako zagrożenia hybrydowe w retrospekcji, skłania do tezy o ich wywiadowczym charakterze. Do refleksji nad zagrożeniami ze strony Rosji termin *środkie akty wne* wnosi ponadto szerszą perspektywę polityczną, społeczną i historyczną.

Dwa modele rosyjskiego dyskursu o strategiach hybrydowych

1. Model wojskowy. W rosyjskiej myśli wojskowej terminy strategii hybrydowe, wojna hybrydowa, technologie hybrydowe itp. pojawiły się stosunkowo niedawno. Ich wprowadzenie uchwycił Michał Wojnowski⁶, który osadził je w kontekście historii rosyjskiej myśli wojskowej i kultury strategicznej. Szczegółowo przybliżając podstawowe założenia i pojęcia, umieścił je w paradygmacie geopolitycznym. Najogólniej rzecz biorąc, w Rosji zostały one wpisane w wojskowy model refleksji na temat natury współczesnej wojny jako rozwinięcie tzw. doktryny Gierasimowa, nawiązującego do amorficznych koncepcji „małych wojen”, „wojen buntowniczych” i „odpowiedzi asymetrycznych”. M. Wojnowski słusznie ocenił wystąpienie szefa Sztabu Generalnego FR podczas zgromadzenia ogólnego Akademii Nauk Wojskowych (ANW)⁷ w 2013 r., nagłościone

⁶ M. Wojnowski, *Mit „wojny hybrydowej”*, <https://www.abw.gov.pl/.../1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE..> [dostęp: 5 I 2018].

⁷ Wbrew nazwie Akademia Nauk Wojskowych (ANW) nie jest instytucją naukową, choć się pod taką podszywa. Jest finansowana przez sponsorów prywatnych, którzy otrzymują tytuł honorowych członków ANW. Skupia ok. 1500 ekspertów z zakresu bezpieczeństwa i obrony, którzy w sferze publicznej przedstawiają się jako „członkowie rzeczywistości” i „członkowie-korespondenci” ANW. Akademia została powołana dekretem Borysa Jelcyna z 1995 r. jako centrum niezależnych badań obronnych. Jej niezmiennym prezesem jest gen. armii Mahmut Gariejew. Wśród członków założycieli ANW znalazły się Rosyjski Instytut Studiów Strategicznych (znajdujący się wówczas w strukturach Służby Wywiadu Zagranicznego), Komitet Uczonych „O bezpieczeństwo globalne”, Liga Wspierania Przedsiębiorstw Obronnych, Uniwersytet Rosyjsko-Amerykański, Rosyjski Związek Przemysłowców i Przedsiębiorców, Centrum Badań Międzynarodowych i in. Akademia „zagogosporarowała” pracowników rozwiązanych instytucji naukowo-badawczych oraz kadry polityczno-wojskowe zwolnione do rezerwy. Oficjalnie pod tą prestiżową nazwą kryje się stowarzyszenie centrów analitycznych i badawczych sił zbrojnych, MSW, Służby Granicznej FSB, Ministerstwa Sytuacji Nadzwyczajnych i Obrony Cywilnej, a także niezależnych ekspertów i dziennikarzy wyspecjalizowanych w problematyce bezpieczeństwa i obronności. Akademia łączy działalność badawczą z działalnością społeczno-edukacyjną: od 2008 r. wydaje kwartalnik „Wojny Informacyjne”; jej członkowie dostarczają informacji mediom i uczestniczą w różnych projektach systemowych organizowanych przez resorty siłowe, Radę Bezpieczeństwa FR, Dumę Państwową i Radę Federacji. Doroczne konferencje Akademii stanowią ważną platformę uspołnienienia pojęć i narracji wykorzystywanych następnie w kampaniach informacyjnych

następnie w mediach rosyjskich i zagranicznych, jako operację informacyjno-psychologiczną. Jak przy tym zauważył:

Słowa generała o rzekomych zmianach, które nastąpiły w sposobach prowadzenia wojen, co miały uwidocznic „kolorowe rewolucje” w Afryce Północnej i na Bliskim Wschodzie, są na Zachodzie traktowane zbyt dosłownie. Nie chodzi tutaj o nowatorskość generowania rewolucji i przewrotów (praktykowanych od wieków), lecz o nowoczesne środki, które zostały wykorzystane do tego celu. W przypadku „arabskiej wiosny” było to m.in. zastosowanie na szeroką skalę mediów i portali społecznościowych (Facebook, Twitter), co stanowi rozwiązanie nowatorskie. Nowa nie jest więc sama idea inicjowania sztucznego przewrotu, lecz narzędzia, których użyto do realizacji tego celu⁸.

Nawiasem mówiąc, Walerij Gierasimow nie mówił wówczas o wojnie hybrydowej, ale o wojnach nowej generacji, które charakteryzował za pomocą zachodnich terminów środki niewojskowe i działania pośrednie z wykorzystaniem potencjału protestu spośród miejscowej ludności. Asymetryczne działania pośrednie miałyby polegać na izolacji politycznej kraju, sankcjach ekonomicznych, blokadzie szlaków komunikacyjnych, zastraszaniu użyciem siły, a także na wprowadzeniu kontyngentu sił międzynarodowych pod pretekstem obrony praw człowieka i prowadzenia operacji humanitarnych. Generał podkreślił przy tym szczególne znaczenie akcji informacyjnych i operacji specjalnych stanowiących istotę kolorowych rewolucji inspirowanych z zewnątrz. Notabene, koncept kolorowych rewolucji prowadzonych jakoby według reguł sztuki wojennej pojawił się także w wystąpieniach Gierasimowa w Akademii Nauk Wojskowych w latach 2014 i 2015. W roku 2016 na określenie działań hybrydowych Rosji generał użył określenia „miękka siła”/„*soft power*”, w 2017 r. mówił zaś o tzw. hybrydowych metodach prowadzenia wojny, które należy traktować jako analog metod wojny bezkontaktowej⁹, co tylko potwierdza spostrzeżenia autorów wydania specjalnego „Przeglądu Bezpieczeństwa Wewnętrznego” z 2015 r. Słowem, wojskowi badacze pojęcia wojna hybrydowa podkreślają z jednej strony jego niewielką przydatność do rosyjskiej teorii wojen, a z drugiej – zachodni rodowód *hybrid war* łączącej elementy wojny konwencjonalnej z wojną partyzancką, terroryzmem i dywersjami oraz wojną informacyjną i propagandową. Ich analizy operacji hybrydowych NATO i USA mają potencjał socjotechniczny: obrazując „powagę sytuacji”, uzasadniają mobilizacyjny model państwa budowany jakoby pod realia wojen hybrydowych (obejmujący nie tylko sferę wojskową i wojskowo-informacyjną,

prowadzonych w mediach, a także kontaktów między oficerami pozostającymi w stanie spoczynku a czynną kadram wojskowego systemu informacyjnego.

⁸ M. Wojnowski, *Mit wojny hybrydowej...*, s. 30.

⁹ Zob. np. В. Герасимов, *Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны*, <http://www.avnr.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/862-vestnik-avn-2-2016> [dostęp: 10 XII 2017]; tenże, *Мир на гранях войны*, <https://www.vpk-news.ru/articles/35591> [dostęp: 10 XII 2017].

lecz także rozległą sferę zarządzania państwem, sferę prawną, kulturową, edukacyjną czy sferę idei, w której wykuwa się przede wszystkim klarowny wizerunek wroga). Potwierdziła to konferencja ANW w marcu 2017 r. Dyskutanci zgodnie podkreślali, że hybrydową specyfikę współczesnych konfliktów wyznacza przede wszystkim przewaga środków niewojskowych nad walką zbrojną. Powoływali (i powołują) się przy tym na szacunki Sztabu Generalnego FR, w którego ocenie ta proporcja wynosi 4:1 na korzyść czynników niewojskowych¹⁰. Konkludowano przy tym, że (...) *wojnę konwencjonalną prowadzi dziś nieudacznicy*.

2. Model cywilny. Zdecydowanie bardziej dynamiczne próby adaptacji NATO-wskiej koncepcji wojen hybrydowych podjęli analitycy „cywilni”, związani z rosyjskimi służbami specjalnymi. (Tu należy zastrzec, że zaproponowany podział jest uproszczony. W Rosji jako „wojskowych” traktuje się mundurowych wszystkich rodzajów: armii, służby granicznej, Gwardii Narodowej, służb specjalnych i in. Dla ich oznaczenia w języku politycznym stosuje się zakorzenione w latach 90. XX w. pojęcie siłowiki). Analitycy powiązani ze służbami dostrzegli istotny walor praktyczny tej koncepcji. Przekładając ją na język własnej narracji i kultury strategicznej, za istotę wojny hybrydowej i jej rdzeń uznali wojnę informacyjną. Większość teoretyków nurtu rozważań, o którym mowa, ogranicza zakres definicyjny tego pojęcia, wyjmując zeń elementy związane z walką zbrojną, tj. ograniczając je do działań określanych w terminologii NATO jako działania niewojskowe (lub: niekinetyczne). Najogólniej rzecz ujmując, w modelu „niewojskowym” można wyróżnić trzy podejścia (choć najczęściej się one krzyżują i wzajemnie uzupełniają):

- 1) fenomenologiczne
- 2) technologiczne
- 3) funkcjonalne.

Głównym wyznacznikiem pierwszego podejścia są próby zdefiniowania pojęcia wojna hybrydowa oraz ustalenia jego genezy i przejawów na gruncie interdyscyplinarnym (socjologii, politologii, nauk wojskowych, nauki o bezpieczeństwie, psychologii, etnologii i in.). Z pozycji socjologa do desygnatów tego pojęcia Farhad Iļjasow¹¹ zaliczył:

- oddziaływanie propagandowe na różne audytoria celowe w kraju agresora i krajach atakowanych;
- tworzenie i inspirowanie ugrupowań separatystycznych i kolaboracjonistycznych w krajach będących celem agresji;

¹⁰ А. Бартош, *Разведка России в противостоянии гибридным угрозам*, http://nvo.ng.ru/spforces/2017-10-06/1_968_scouting.html [dostęp: 5 I 2018]. Por. tenże: *Гибридная война становится новой формой межгосударственного противоборства*, http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html [dostęp: 5 I 2018]; <https://topwar.ru/112955-gibridnaya-voyna-stanovitsya-novoy-formoy-mezhgosudarstvennogo-protivoborstva.html> [dostęp: 5 I 2018]. Zob. także niedawno wydaną monografię: А. Бартош, *Конфликты XXI века. Гибридная война и цветная революция*, Москва 2017.

¹¹ Ф.Н. Ильясов, *Словарь социальных исследований*, 2016, <http://www.jsr.su/dic/dictionary.html> [dostęp: 5 I 2018].

- inicjowanie zamieszek i masowych akcji protestu;
- operacje dywersyjne i terrorystyczne prowadzone wspólnie przez agresora i powstańców;
- niejawne wspieranie separatystów – uzbrojeniem, danymi wywiadowczymi, środkami finansowymi, a także działaniami formacji nieregularnych;
- działania ukierunkowane na destabilizację i osłabienie gospodarki atakowanego kraju;
- wsparcie dyplomatyczne i informacyjne realizowanych projektów specjalnych.

Według F. Iljasowa celami tak rozumianej wojny mają być: okupacja, aneksja terytorium oraz zmiana reżimu politycznego lub ekipy rządzącej. Aleksandr Bartosz¹², koncentrujący się na przyczynach współczesnych konfliktów hybrydowych, prezentuje koncepcję katalizatorów niestabilności na świecie. Są nimi:

- działania USA i NATO (aktywność u granic Rosji);
- jednostronne użycie siły w stosunkach międzynarodowych;
- bezprawne wykorzystanie sankcji ekonomicznych przeciwko Rosji;
- prowokowanie kryzysów finansowo-ekonomicznych;
- brak konsensusu w sprawie walki z terroryzmem międzynarodowym;
- globalna konfrontacja informacyjna i doskonalenie metod walki w cybersferze;
- tworzenie napięcia i chaosu w stosunkach międzynarodowych przez wspieranie nastrojów nacjonalistycznych, ksenofobii, separatyzmu, ekstremizmu, fundamentalizmu religijnego;
- kryzysy migracyjne oraz kryzysy związane z międzynarodowym narkobiznesem i handlem ludźmi;
- zaostrzenie walki o zasoby surowców (Bliski Wschód, Arktyka, basen Morza Kaspijskiego, Azja Centralna).

W tym kontekście A. Bartosz umieszcza pojęcie katalizatory procesów rozkładowych (noty dyplomatyczne, wrzuty informacyjne, działalność formacji paramilitarnych). Także w jego ujęciu najpotężniejszym katalizatorem są tzw. kolorowe rewolucje, organizowane w przełomowej fazie wojny hybrydowej w celu uzyskania lawinowego efektu destabilizacji zaatakowanego państwa.

Podejście technologiczne polega na wyodrębnianiu podstawowych wymiarów wojny hybrydowej oraz jej mechanizmów. Cytowany wyżej Bartosz wyróżnia front polityczny, dyplomatyczny, informacyjny, paramilitarny i historyczny. Igor Panarin poszerza je o front etniczny i twórczo rozwija front historyczny, co w tym przypadku przyjmuje charakter groteskowy. Początku operacji hybrydowych przeciwko Rosji Panarin upatruje w tajnym przymierzu Francji, Austrii i Wielkiej Brytanii (1815 r.) oraz utworzeniu rosyjskiej łoży masońskiej w celu dokonania zamachu stanu w Rosji, czego przejawem miało być powstanie dekabrystów w 1825 r. przeciwko Mikołajowi I. Nasilone operacje hybrydowe łoży masońskiej i brytyjskiej MI-6 na początku XX w. zaowocowały następnie rewolucją lutową 1917 r. i największą geopolityczną

¹² А. Бартош, *Разведка России...*, tamże.

katastrofą świata – upadkiem Imperium Rosyjskiego (drugą taką katastrofą był rozpad ZSRS). A. Bartosz sytuuje ten początek w czasach smuty (1598–1613), skutkujących (...) *hybrydową agresją Polski i Szwecji, wspieraną przez Watykan, który realizował plan stworzenia polsko-litewsko-szwedzkiego supermocarstwa, rozbioru Rosji i podporządkowania jej stolicy papieżstwa*¹³. Były analityk GRU Siergiej Diewiatow¹⁴ traktuje wojnę hybrydową przede wszystkim jako wojnę cywilizacji Wschodu z cywilizacją Zachodu. Oprócz frontu walki zbrojnej włącza do niej front finansowy (finanse światowe są według niego głównym frontem wojny hybrydowej), semantyczny (wojnę narracji), ekonomiczny (walka o zasoby i technologie) oraz front społeczny (edukacji, kultury i sportu).

Wojny finansowa, ekonomiczna i handlowa znalazły się także w centrum uwagi Jurija Bobyłowa¹⁵, o czym świadczą liczne publikacje na jego blogu i w mediach tradycyjnych. Wysiłek intelektualny tego wieloletniego pracownika sowieckiej tajnej Komisji Wojskowo-Przemysłowej, a obecnie zastępcy rektora Rosyjskiego Państwowego Uniwersytetu Geologicznego i członka Rosyjskiej Rady do Spraw Stosunków Międzynarodowych, jest skoncentrowany na przeniesieniu doświadczeń hybrydowej walki informacyjnej na inne sfery (finansową, ekonomiczną, handlową oraz innowacyjno-technologiczną). Do podjęcia hybrydowej walki informacyjnej i jej skuteczności przyczyniły się, jego zdaniem, duże zdolności organizacyjne rosyjskich służb wywiadowczych, tj. potencjał wykonawczy działający według zasady partnerstwa państwowo-prywatnego.

Ujęcie funkcjonalne, spinające podejścia zasygnalizowane powyżej, wyróżnia nie tyle treść, ile forma. Charakterystyczny jest dla niego język batalii propagandowej, nagminne operowanie pojęciami – kluczami w rodzaju agent wpływu, piąta kolumna, kolorowa rewolucja. To podejście obserwujemy także w przekazach oficjalnych przedstawicieli FR, którzy w ten sposób nadają teorii sens praktyczny. Podczas posiedzenia Rady Szefów Organów Bezpieczeństwa WNP, które odbyło się 19 grudnia 2017 r., dyrektor Służby Wywiadu Zagranicznego Siergiej Naryszkin, oskarżając Zachód o (...) *prowadzenie niewypowiedzianej wojny hybrydowej przeciwko państwu WNP*, stwierdził, że (...) *Wielka Brytania, Polska, Szwecja oraz kraje bałtyckie znalazły się w awangardzie wysiłków na rzecz przekształcenia rosyjskich środowisk emigracyjnych w tzw. rewolucyjne jaczeki*¹⁶. Takie postrzeganie rzeczywistości reprezentują na co dzień kremlowscy polittechnolodzy i tzw. liderzy opinii, interpretujący wyda-

¹³ И. Панарин, *Гибридная война против России (1816–2016 гг.)*, Москва 2016; А. Бартош, *Россия в эпоху гибридных войн*, http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html [dostęp: 10 XII 2017]; tenże: *Разведка России в противостоянии гибридным угрозам*, http://nvo.ng.ru/spforces/2017-10-06/1_968_scouting.html [dostęp: 10 XII 2017].

¹⁴ <https://devyatov.su/articles/251-nebopolitika/29572-gibridnaja-vo-na-na-finansowom-fronte> [dostęp: 5 I 2018].

¹⁵ <http://www.park.futurrussia.ru/extranet/blogs/Bobylov> [dostęp: 5 I 2018].

¹⁶ <http://www.interfax.ru/world/592442> [dostęp: 20 XII 2017]; <http://www.mk.ru/politics/2017/12/19/naryshkin-na-zapade-iz-rossiyskikh-emigrantov-gotovyat-revolucionerov.html> [dostęp: 20 XII 2017].

czenia w sposób zgodny z „linią Kremla”. Aleksiej Puszkow, przewodniczący komisji Rady Federacji ds. polityki informacyjnej i współpracy z mediami, komentując w rządowej gazecie poprawki do ustawy *O informacji, technologiach informacyjnych i ochronie informacji*, w myśl których zagraniczne media mogą być uznane za zagranicznych agentów (symetryczna odpowiedź Rosji za zmuszenie rosyjskich mediów Russia Today i Sputnik do zarejestrowania się w Stanach Zjednoczonych w charakterze agentów zagranicznych), skomentował amerykańskie posunięcie jako (...) *informacyjny komponent wojny hybrydowej Stanów Zjednoczonych przeciwko Rosji, mającej na celu ograniczenie rosyjskiego wpływu na bieg wydarzeń na świecie, nadzarpnięcie prestiżu oraz wizerunku FR*¹⁷.

Funkcjonalny wymiar rosyjskich rozważań unaoczniają zwłaszcza ostatnie publikacje wspomnianego już Igora Panarina¹⁸, profesora Akademii Dyplomatycznej przy MSZ FR, w przeszłości analityka KGB i Federalnej Agencji Informacji i Łączności Rządowej (FAPSI). Ten znany teoretyk i praktyk wojen informacyjnych (orędownik i czołowy przedstawiciel geopolityki informacyjnej) przełożył stosowane przez siebie wcześniej pojęcia i założenia badawcze ujmowane w matrycy wojny informacyjnej na język teorii wojny hybrydowej Zachodu przeciwko Rosji. Mają one w gruncie rzeczy ten sam szeroki zakres desygnatów. Opisany przez niego model obrony suwerenności kraju (wymagającej w jego opinii wzmocnienia informacyjnej obecności Rosji we wszystkich strategicznie ważnych regionach świata) okazał się przydatny w jego rozważaniach na temat przeciwdziałania zachodnim technologiom wojny hybrydowej. W autorskiej definicji wojny hybrydowej Panarin uwzględnił aktualne trendy w dyskusji na ten temat:

Wojna hybrydowa – to zespół metod nacisku wojskowo-siłowego, polityczno-dyplomatycznego, informacyjno-psychologicznego i informacyjno-technicznego, a także technologii kolorowych rewolucji, terroryzmu i ekstremizmu, przedsięwzięć służb specjalnych i struktur dyplomacji publicznej realizowanych według jednego planu przez organy państwa, blok wojskowo-polityczny lub korporacje ponadnarodowe¹⁹.

¹⁷ <https://rg.ru/interviews/3070.html> [dostęp: 5 I 2018].

¹⁸ И. Панарин, *Гибридная война против России...*; także: *Гибридная война. Теория и практика*, Москва 2017 oraz także: *Гладиаторы гибридной войны*, <http://ruspravda.info/Gladiatori-gibridnoy-voyni-23791.html> [dostęp: 5 I 2018]; *Гибридная война: прошлое, настоящее и будущее*, <http://новости.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B3%D0%B8%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0%D1%8F-%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D1%88%D0%BB%D0%BE%D0%B5-%D0%BD%D0%B0%D1%81%D1%82%D0%BE%D1%8F%D1%89%D0%B5%D0%B5-%D0%B8-%D0%B1%D1%83%D0%B4%D1%83%D1%89%D0%B5%D0%B5-%D0%B8%D0%B3%D0%BE%D1%80%D1%8C-%D0%BF%D0%B0%D0%BD%D0%B0%D1%80%D0%B8%D0%BD/> [dostęp: 5 I 2018].

¹⁹ И. Панарин, *Гладиаторы гибридной войны...* [dostęp: 5 I 2018].

Ważnymi instrumentami wojny hybrydowej według tego autora są: operacje informacyjne, operacje psychologiczne, ataki cybernetyczne, sankcje ekonomiczne, broń etniczna, broń organizacyjna, informacyjne i finansowe wsparcie ugrupowań opozycyjnych oraz destrukcyjna działalność agentury wpływu ulokowanej w strukturach władzy państwowej. Także I. Panarin podkreśla, że najważniejszymi „żołnierzami” („gladiatorami”) tej wojny są służby specjalne, do czego predestynują je posiadane narzędzia.

Działalność naukowa i publicystyczna autorów związanych ze służbami wywiadowczymi argumentuje tezę o ich aktywnym uczestnictwie w wojnie politycznej Rosji z Zachodem²⁰. Jest to wojna permanentna. Hybrydowe narzędzia niewojskowe to te same narzędzia, które w czasach zimnej wojny opisywano jako środki aktywne. Również te narzędzia umieszcza się w kontekście wojen informacyjnych, psychologicznych, ekonomicznych itp. Dziś na ich określenie, jak to pokazuje przybliżony wyżej dyskurs, rosyjscy teoretycy upowszechniają pojęcie technologie hybrydowe, zastępując nim wcześniejsze pojęcia: technologie informacyjno-psychologiczne i technologie niesiłowego rozwiązywania konfliktów²¹. Taka rekontekstualizacja terminów nie zmienia ich istoty: podobnie jak pojęcia stosowane wcześniej, dają Rosjanom możliwość podwójnego zastosowania – jako konstruktywnego narzędzia mobilizacji i optymalizacji własnej działalności oraz jako destrukcyjnej „broni” (konceptyjnej, informacyjnej). Te tzw. wojny, obliczone na długie trwanie, wymagają stałego odnawiania koncepcji, dostosowywania ich do aktualnych realiów, mobilizowania „żołnierzy” i szkolenia ich nowych pokoleń. Podejście „hybrydowe” wzbudziło m.in. nową falę zainteresowania zimną wojną: coraz głośniej rozlegają się głosy, że nigdy nie została ona zakończona. Prowadzi to do nowej ideologizacji rosyjskiej agresji przeciwko Ukrainie czy w Syrii – jako „sprawiedliwej” wojny Rosji przeciwko Stanom Zjednoczonym i NATO. Z tego względu ważnym elementem współczesnej rosyjskiej narracji jest podkreślanie roli resortów siłowych, w tym wywiadu, które mają mandat, siły i środki do zwalczania kolorowych rewolucji – najważniejszej technologii konfrontacji Zachodu z Rosją. Taka „hybrydowa” narracja nie stała się symbolem nowoczesnego myślenia i funkcjonowania, przeciwnie – kieruje w stronę wypróbowanych metod i doświadczeń z przeszłości.

²⁰ M. Galeotti, *Służby wywiadowcze Rosji są w stanie politycznej wojny*, <https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/PL/index.htm> [dostęp: 5 I 2018].

²¹ Zob. na przykład: A.B., Манойло, *Технологии несилового разрешения конфликтов*, Москва 2014. Współcześnie zresztą używa się wielu synonimicznych terminów, takich jak np. środki wsparcia czy specjalne środki wpływu. Pojawiły się one już w *Doktrynie wojennej* i *Doktrynie bezpieczeństwa informacyjnego* z 2000 r.; w tekstach późniejszych zastąpiono je terminami: środki niewojskowe, działania pośrednie (tj. dywersja, sabotaż, organizowanie nieregularnych formacji zbrojnych), oddziaływanie informacyjne, oddziaływanie informacyjno-psychologiczne, oddziaływanie informacyjno-techniczne. W ostatniej wersji *Doktryny wojennej* z grudnia 2014 r. wprowadzono dodatkowo pojęcie technologie informacyjne. Zostało ono przeniesione także do nowej redakcji *Doktryny bezpieczeństwa informacyjnego* z grudnia 2016 r.

Perspektywa historyczna: środki aktywne jako strategia hybrydowa

Środki aktywne to pojęcie równie wielowymiarowe jak pojęcie technologie hybrydowe. Ten historyczny termin jest fasadą, za którą kryją się różne formy oddziaływania, wśród których zawsze dominowały dezinformacja i specpropaganda. Były one realizowane przez różnych aktorów, najczęściej pod kontrolą służb specjalnych. Termin pojawił się w latach 60. XX w. (na fali natężenia walki ideologicznej ZSRS przeciwko Zachodowi) jako pojęcie zbiorcze zawierające w sobie takie pojęcia, jak dezinformacja, sabotaż, dywersja itp., które maskowały ofensywny charakter działań przedstawianych jako obronne. Środki aktywne znajdowały się w arsenale zarówno wywiadu, jak i kontrwywiadu. Najobszerniejsza jest ich definicja zawarta w *Słowniku kontrwywiadowczym* (Moskwa, 1972)²² wydanym przez Wyższą Szkołę KGB im. Feliksa Dzierżyńskiego (pod red. W.F. Nikitczenki). Pojęcie środki aktywne (ros. *активные мероприятия*) zdefiniowano tu jako:

(...) działania kontrwywiadu umożliwiające przejrzanie zamiarów przeciwnika, pozwalające uprzedzić jego niepożądane kroki, wprowadzić przeciwnika w błąd, przechwycić jego inicjatywę, udaremnić jego akcje dywersyjne. Środki aktywne, w odróżnieniu od środków ochronnych, np. dotyczących zabezpieczenia reżimu tajności oraz ochrony tajemnicy państwowej i wojskowej, mają charakter ofensywny, umożliwiają wykrycie i przerwanie wrogiej działalności we wczesnym jej stadium, zmuszają przeciwnika do zdemaskowania się, pozwalają narzucić mu swą wolę, zmuszają do działań w niesprzyjających warunkach oraz kierunkach pożądanym dla organów kontrwywiadu. W praktyce działalności kontrwywiadowczej organów bezpieczeństwa państwowego do środków aktywnych zalicza się przedsięwzięcia mające na celu zbudowanie pozycji agenturalnych w obozie przeciwnika i jego otoczeniu, prowadzenie gier operacyjnych z przeciwnikiem, jego dezinformację, kompromitację i demoralizację, przerzut na terytorium ZSRR osób mających szczególną wartość operacyjną, zdobywanie informacji wywiadowczej itp.

Wywiadowczą definicję środków aktywnych przytoczył były funkcjonariusz I Zarządu Głównego i archiwista wywiadu KGB Wasilij Mitrochin, który zwrócił uwagę na ich wymiar polityczny, ekonomiczny, wojskowy oraz ideologiczny. Według niego w wywiadzie KGB określano je jako:

(...) działania agenturalno-operacyjne, ukierunkowane na wywieranie wpływu na politykę zagraniczną i wewnętrzną sytuację polityczną krajów będących obiektem tych działań prowadzonych w interesie Związku Sowieckiego i innych krajów socjalistycznych, światowego komunizmu i ruchów narodowowyzwoleńczych; osłabianie

²² *Контрразведывательный словарь*, Москва 1972, s. 161–162, <http://www.kgbdocuments.eu/index.php?1442843474>; <https://docviewer.yandex.com/?url=ya-disk-public%3A%2F%2FfA1-GUq9IcULWRmqEoOAPcEXoJ1HxKPkixIzBR4mngdg%3D&arc> [dostęp: 15 VI 2017].

politycznej, wojskowej, gospodarczej i ideologicznej pozycji kapitalizmu; torpedowanie jego agresywnych planów w celu stworzenia sprzyjających warunków pomyślnej realizacji polityki zagranicznej Związku Sowieckiego oraz zapewnienia pokoju i postępu społecznego²³.

Obie definicje łączy identyczne postrzeganie celu wykorzystywania środków aktywnych, tj.: wywieranie wpływu na przeciwnika, dezinformowanie go, kompromitowanie i demoralizowanie z zamiarem stworzenia sprzyjających warunków do pomyślnej realizacji celów polityki zagranicznej Związku Sowieckiego. Dezinformację rozumiano przy tym szeroko: jako wpływ za pomocą słowa i jako działanie.

Najważniejszą rolę w realizacji tych technik odgrywały służby specjalne, głównie w związku z posiadaniem narzędzi niezbędnych do formułowania strategicznych celów i zadań polityki Kremla, typowania ich zewnętrznych operatorów i niejawnego finansowania. Pierwsze sowieckie dezinformbiuro powstało w 1923 r. w ramach OGPU/NKWD. Odrębną komórką nastawioną na prowadzenie takich działań był wydział „D” (od ros. *dieza* – ‘dezinformacja’) powołany w 1959 r. w ramach I Zarządu Głównego KGB (wywiad), przekształcony z czasem w Służbę „A” (od ros. *aktiwka* – ‘działania aktywne’). Analogiczne struktury powołał wywiad wojskowy (GRU), gdzie do 1991 r. działał VII Zarząd (specpropaganda). Główny Zarząd Polityczny Armii i Marynarki, jak pisze Oleg Diemidow²⁴, miał także inne rozgałęzione struktury do prowadzenia walki informacyjnej. Przedstawiona instytucjonalizacja środków aktywnych świadczyła o próbie połączenia różnych form oddziaływania w skoordynowany, planowy proces. Praktyka unaocznia też znamiennej ewolucję podejścia Kremla do strategii dezinformacji: od słowa do działania i od form miękkich do twardych (od dywersji informacyjnej, ideologicznej do dywersji twardej).

Środki aktywne były przedmiotem szczegółowych badań zachodnich analityków zajmujących się wojną psychologiczną, które były prowadzone przez ZSRS w czasach zimnej wojny²⁵. Zawężając to pojęcie, opisywano je niekiedy jako dezinformację²⁶. Sam Władimir Volkoff, francuski literat, który opracował antologię tekstów na ten temat, we wstępie do niej określił dezinformację jako „doktrynę” (system myślenia i postępowania), traktując wprowadzanie w błąd jako jedną z technik²⁷. Jego komentarze do tekstów precyzyjnie ukazują cele, metody i środki sowieckich operacji wpływu na opinię publiczną i politykę państw obcych. Źródłem wiedzy na ten temat jest też szeroka, tłumaczona na język polski, literatura słynnych dezerterów z KGB – Jurija Biezmenowa, Olega Kaługina, Olega Gordijewskiego, Anatolija Golicyna i in.

²³ W. Mitrochin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002, s. 13.

²⁴ О. Демидов, *Инфовойска России: к структуре нового тина?*, <http://vpoanalytics.com/2017/03/08/infovojska-rossii-k-strukture-novogo-tipa/> [dostęp: 5 I 2018].

²⁵ С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnye-sovetskie-meropriyat-ya-v-putinskoy-rossii> [dostęp: 10 XI 2017].

²⁶ *Psychosocjotechnika. Dezinformacja. Oręż wojny*, V. Volkoff (oprac.), Komorów 1999.

²⁷ Tamże, s. 11.

Pojawiające się z rzadka publikacje rosyjskie mają z natury rzeczy bardziej lub mniej zakamuflowany charakter mitotwórczy. Służą motywacji bądź autokreacji rosyjskich służb: problematyka sowieckich środków aktywnych jest bowiem w Rosji do dziś objęta klauzulą tajności.

W identyfikowaniu i diagnozowaniu niejawnych mechanizmów współczesnych operacji służb rosyjskich pomocna może się okazać perspektywa historyczna. Jak pisze Marek Świerczek:

Podczas analizy działań współczesnych rosyjskich służb specjalnych należy zdać sobie sprawę, że ich modus operandi został wypracowany na początku lat 20. XX wieku. To właśnie wtedy rewolucyjne pomysły twórców kontrwywiadu ofensywnego i szeroko rozumianych operacji dezinformacyjnych zetknęły się z osiągnięciami carskiej Ochrazy, której funkcjonariusze zasilili nie tylko kształtujący się wywiad Armii Czerwonej, lecz także WCzeKa oraz późniejsze GPU i OGPU. Z tego powodu wszelkie próby zrozumienia działalności współczesnego wywiadu rosyjskiego, zarówno na płaszczyźnie operacyjnej, jak i rozumianej jako jeden z elementów polityki zagranicznej Rosji wymagają perspektywy historycznej. Tylko takie spojrzenie pozwala poznać stosowane w przeszłości operacyjne instrumentarium i wyciągnąć wnioski na podstawie celów osiąganych za jego pomocą²⁸.

Sam cytowany tekst jest przykładem znakomitej analizy historycznej zróżnicowanego instrumentarium służb sowieckich stosowanego przeciwko II RP. Realizując plan destabilizacji państwa polskiego, służby te wykorzystywały wszelkie dostępne narzędzia: od środków dywersyjno-terrorystycznych i quasi-militarnych, przez zmasowaną propagandę antypolską w RP i na zachodzie Europy, po zakulisowe działania polityczne. Opisane przez M. Świerczka techniki destabilizacji II RP prowadzą do wniosku, że Rosjanie nie stosują jakiegoś jednego modus operandi, tylko dostosowują metody do zamierzonych celów. Na tej podstawie można zidentyfikować pewne uniwersalne zasady, którymi się kierują rosyjskie służby wywiadowcze. Taką niezmienną zasadą jest np. poszukiwanie słabości przeciwnika czy drażliwych tematów, a następnie ich wykorzystanie w celu pogłębienia podziałów w społeczeństwie i zaognienia sytuacji. Uniwersalna jest zasada długotrwałego

²⁸ M. Świerczek, *Wojna hybrydowa jako strategia polityczna. Próba analizy historycznej na przykładzie działań ZSRS wobec II RP*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-8/1323,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-16-9-2017.html> [dostęp: 5 I 2018]; tenże: *Działania wobec Attachatu Wojskowego przy Poselstwie RP w Moskwie w początkach jego funkcjonowania jako egzemplifikacja kontrwywiadowczego modus operandi stosowanego przez służby rosyjskie*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-9/1384,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-17-9-2017.html> [dostęp: 5 I 2018]; tenże: *Udział Wiktora Tomira Drymmera w aferze MOCR-Trust w świetle jego artykułu z 1965 r. pod tytułem „Trust”. Wstęp do analizy*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-1/1008,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-10-6-2014.html> [dostęp: 5 I 2018]; tenże: *Modus operandi GPU na przykładzie operacji „Trust” opisanej w „Trioch stolicach” W.W. Szulgina*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-3/1180,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-12-7-2015.html> [dostęp: 5 I 2018].

oddziaływania (proces rozkładu II RP trwał przez cały okres jej istnienia). Niezmienne jest odwracanie wektorów w akcji propagandowej towarzyszącej działaniom aktywnym: mimo że to sowiecka Rosja była agresorem, Polska w jej ówczesnej agitacji i propagandzie była przedstawiana jako (...) *drapieżnik, pokraczny bękart z syndromem imperialnym, pies łańcuchowy, koń trojański Zachodu* itp. Oprócz zasygnalizowanych uniwersalnych zasad stosowanych przez służby sowieckie, omawiana analiza pozwala na wyodrębnienie kolejnych zasad – organizacyjnych, które przedstawiono w tabeli poniżej.

Tab. 1. Zasady stosowane przez służby sowieckie podczas operacji tajnych (wywiadowczo-organizacyjne).

| Przedsięwzięcia operacyjne | Zasady organizacyjne |
|--|--|
| Zmasowana akcja propagandowa kierowana zarówno do Polaków, jak i mniejszości zamieszkujących ówczesne Kresy Wschodnie, a także na Zachód | Transgraniczny charakter (eksterytorialność) akcji informacyjnej i propagandowej |
| Przerzut prowokatorów, dywersantów, agitatorów, szpiegów | Tajność oraz inspiracja przeciwnika |
| Zainspirowanie wybuchu powstania na Kresach | Zaskoczenie i dezorientacja przeciwnika |
| Seria zamachów bombowych w centralnej Polsce, np. na prochownię w Cytadeli Warszawskiej | Oddziaływanie na emocje społeczeństwa przeciwnika |
| Wpływanie na polską scenę polityczną przez KPRP, Białoruską Hromadę, partie i frakcje sejmowe II RP | Wykorzystanie zasobów własnych i zasobów przeciwnika |
| Organizowanie zamieszek na tle żądań ekonomicznych | Kompleksowość metod wpływu (politycznych, ekonomicznych, społecznych i in.) |
| Kampania zastraszania polskich organów ścigania (zamachy na policyjnych prowokatorów) | Oslabianie morale przeciwnika |
| Skrytobójstwa, plan zamordowania marszałka Józefa Piłsudskiego | Zasada „cel uświęca środki” |

Źródło: Opracowanie własne na podstawie: M. Świerczek, *Wojna hybrydowa jako strategia polityczna. Próba analizy historycznej na przykładzie działań ZSRS wobec II RP*, „Przeгляд Bezpieczeństwa Wewnętrznego” 2017, nr 16, s. 81–97.

Perspektywa historyczna prowadzi także do wniosku, że rosyjskie służby nie porzuciły metod stosowanych w przeszłości. Pierwszym zadaniem wspomnianego Wydziału D KGB było np. skompromitowanie RFN jako kraju neonazizmu. Do RFN przetrzucono wschodnioniemieckich agentów, aby bezcześcili żydowskie nagrobki, malowali antysemickie hasła na synagogach, sklepach i siedzibach organizacji żydowskich oraz prowokowali do analogicznych działań ludność miejscową. W 1959 r., jak pisał John Barron²⁹, władze RFN odnotowały 833 antysemickie akty, co spotkało się z potępieniem RFN na arenie międzynarodowej i nadszarpięło wizerunek tego kraju w oczach opinii publicznej. Trudno o bardziej czytelną analogię z szeroko prowadzonymi dziś „wojnami pomnikowymi”, które błyskawicznie przekształcają się w demonstracje antypolskie, antyukraińskie, antylitewskie, antyłotewskie, antyestońskie itd.

Tego typu przykłady można mnożyć. Należy jednak odnotować, że mechanizmy sprawdzone w przeszłości są doskonałe, urozmaicane oraz dostosowywane do bieżących realiów i potrzeb. Przykładem może tu być ewolucja grup pozorowanych (legendowanych grup agentury i funkcjonariuszy służb). Po raz pierwszy tego typu grupa została wykorzystana, jak pisze prof. Igor Hałagida³⁰, w 1918 r. w operacji znanej jako tzw. spis Lockharta (domniemanymi spiskowcami byli agenci CzeKi, którzy zgłosili się do brytyjskiego dyplomaty). Ta prowokacja posłużyła następnie Feliksowi Dzierżyńskiemu jako argument przeciwko dyplomacji zachodniej, która podjęła próbę przeprowadzenia zamachu stanu w ZSRS, co szeroko nagłośniono w kraju i za granicą. Organizowanie grup pozorowanych (w formie fikcyjnych struktur niepodległościowych i antyreżimowych) doprowadzono do perfekcji podczas drugiej wojny światowej, kiedy to wykorzystywano je do likwidacji środowisk antykomunistycznych na zajmowanych terytoriach (Ukraina, Białoruś, Litwa, Łotwa, Estonia i in.), a także po wojnie – do likwidacji podziemia antykomunistycznego w krajach bloku wschodniego. Współcześnie grupy pozorowane pojawiają się w miejscach różnych konfliktów (np. na wschodniej Ukrainie czy podczas próby nieudanego zamachu stanu w Czarnogórze w 2016 r.) w rozmaitej postaci: prywatnych spółek wojskowych, organizacji kozackich, oddziałów samoobrony, młodzieżowych bojówek organizacji ekstremistycznych, zaciągów ochotniczych, sił specjalnych pozbawionych dystynkcji itp.

Tajne technologie hybrydowe jako zagrożenie wywiadowcze

Operacje wywiadowcze określane jako technologie hybrydowe czy środki aktywne nie mieszczą się w formule typowych działań wywiadu, nie mają bowiem nic wspólnego ze zbieraniem informacji i analizą – służą realizacji celów polityki zagranicznej, gospodarczej i obronnej Rosji. Najogólniej rzecz ujmując, spośród „klasycznych” działań wywiadu wyróżnia je charakter sprawczy³¹. O ile te pierwsze dotyczą

²⁹ Cyt. za: *Psychosocjotechnika. Dezinformacja...*, s. 130.

³⁰ <http://polska1918-89.pl/pdf/miedzy-dezinformacja-a-rzeczywistoscia.-prowokacyjne-dzialania-sluzb-k,5366.pdf> [dostęp: 5 I 2018].

³¹ W terminologii anglosaskiej tego typu przedsięwzięcia definiuje się jako *covert action*.

podejmowania decyzji, gdy coś się wydarzy, o tyle te drugie są stosowane po to, żeby coś się wydarzyło. Chodzi o to – wyjaśnia A. Bartosz³² – aby zaprojektować i wykreować przyszłość wroga.

Nowe realia, przede wszystkim porzucenie sztywnej komunistycznej ideologii po upadku ZSRS, a także gwałtowne przemiany społeczne i ekonomiczne, poszerzyły możliwości rosyjskich służb zarówno w kraju, jak i za granicą. Wywiad, podporządkowany bezpośrednio prezydentowi, od samego początku działał w aurze celowości, co zapewniała przygotowana w SWZ ustawa *O organach wywiadowczych FR* przyjęta w sierpniu 1992 r. Stanowiła ona, że (...) *etatowi pracownicy wywiadu mogą zajmować stanowiska w ministerstwach, departamentach, przedsiębiorstwach i organizacjach bez ujawniania swych powiązań z organami wywiadu zagranicznego*. Jeśli w czasach KGB wywiad był ześrodkowany w rezydenturach zagranicznych pod przykrywką dyplomatyczną oraz w placówkach rozpoznanych na Zachodzie (przedstawicielstwa Aeroflotu, przedstawicielstwa handlowe, biura korespondentów zagranicznych), to odtąd mógł działać pod przykrywką dowolnej organizacji politycznej, gospodarczej czy społecznej. Okno możliwości poszerzyła rosyjskojęzyczna diaspora rozrzucona po wszystkich krajach powstałych wskutek rozpadu ZSRS.

Rosyjskim służbom sprzyjały także nowe realia technologiczne: rozwój technik informacyjno-komunikacyjnych, powszechne wykorzystanie techniki komputerowej, rosnące uzależnienie państw od infrastruktury informatycznej itp. Ułatwia to nie tylko zdobywanie informacji, lecz także manipulowanie nimi.

Zgodnie z tradycją w walce o informacje (wiedzę) rosyjski wywiad strategiczny wykazuje tendencję do szerokiego działania w różnych sferach: politycznej, ekonomicznej, społecznej, naukowo-technicznej, socjologicznej, kulturalnej i wojskowej. Walkę o informacje w rosyjskiej doktrynie wywiadowczej i założeniach strategicznych szybko przekształcono w walkę informacyjną (mówiąc ściślej – dezinformacyjną) na frontach odpowiadających komponentom wywiadu. Wystarczy przypomnieć, że sam termin *walka informacyjna* pojawił się na Zachodzie dopiero w połowie lat 90. XX w. i niemal natychmiast został wprowadzony do rosyjskich dokumentów oficjalnych (występował już w *Doktrynie bezpieczeństwa informacyjnego* i *Doktrynie wojennej* z 2000 r.). Sprzyjały temu długa tradycja stosowania środków walki informacyjno-psychologicznej oraz bieżące doświadczenia związane z dwiema wojnami czeczeńskimi i wyzwaniem, jakim było dla Rosji rozszerzenie NATO i UE, czemu towarzyszyły niezwykle dynamiczne kampanie informacyjne. Nie powinno zatem dziwić, że większość rosyjskich teoretyków podkreśla szczególną rolę instrumentarium informacyjnego na wszystkich etapach operacji hybrydowych (jako środka pasywnego – od monitorowania sytuacji w poszukiwaniu pęknięć i niespójności w krajach atakowanych, przez planowanie operacji i typowanie wykonawców, po jej wykonanie i tzw. oprawę medialną).

Zob. M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 61–62. Mirosław Minkina określa je mianem operacji pozainformacyjnych wywiadu. Zob. M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 209–245.

³² А. Бартош, *Гибридная война...*, tamże.

W tym kontekście, jak twierdzi J. Bobyłow, posunięciem trudnym do przecenienia było stworzenie mobilizacyjnych sieci informacyjnych (u ich podstaw legły mechanizmy wywiadowcze, a także partnerstwo państwowo-prywatne oraz budowanie kompetencji, tj. przygotowanie kadr analitycznych i wykonawczych zdolnych do prowadzenia samodzielnych działań), które powinny stać się modelem dla „działań hybrydowych” w innych obszarach: ekonomicznym, finansowym, handlowym, a także innowacji przemysłowych³³. Przy akcentowaniu pomocniczej roli wywiadu³⁴ Bobyłow rozróżnia operacje specjalne (realizowane przez wywiad) i projekty specjalne (w których wywiad uczestniczy). Charakteryzując operacje specjalne, przytacza następujące ich wyróżniki:

- destrukcyjny charakter (celem jest likwidacja bądź osłabienie przeciwnika);
- tajność i inspirację (działania tajne mogą mieć charakter zarówno legalny, jak i nielegalny);
- brak ograniczeń przestrzennych;
- wykorzystanie własnych obywateli i obywateli państw obcych;
- kompleksowość (działanie zgodnie z zasadą „cel uświęca środki);
- szerokie spektrum metod wykorzystywanych na różnych poziomach rozwiązywania problemu;
- specjalną strukturę wykonawczą (wykorzystanie zasobów stałych, a także organizacji jednorazowych tworzonych w celu realizacji zadania);
- specjalne zabezpieczenie materialne (w tym finansowe);
- szczególny tryb zarządzania przebiegiem operacji: ich autonomiczność i anonimowość wymaga delegowania odpowiedzialności z centrum decyzyjnego do struktur wykonawczych;

³³ Ю. Бобылов, *Экспортно-ориентированные инновационные промышленные прорывы России по стратегиям гибридных войн*, «Информационные войны» 2015, nr 1, s. 55–61. Szczególnie interesujące z punktu widzenia omawianej problematyki są artykuły: tegoż, *Спецслужбы и стратегия гибридных войн*, www.rusnor.org/pubs/articles/12200.htm [dostęp: 5 I 2018]; tegoż, *Проблема внешней ведомственной конкурентной разведки России. Информационные, правовые и организационные аспекты*, «Информационные войны» 2016, nr 4, s. 67–79; tegoż, *Новые наукоемкие гибридные войны*, <http://www.proatom.ru/modules.php?name=News&file=print&sid=7397> [dostęp: 5 I 2018]. Zdaniem autora współczesne realia ekonomiczne na świecie stawiają Rosję przed nowym mobilizacyjnym wyzwaniem: zbudowania adekwatnych struktur zarządzania państwem oraz mobilizacyjnej sieci ekonomicznej, przy wykorzystaniu tajnych technologii służb specjalnych i z ich udziałem, a także z udziałem zróżnicowanych podmiotów prywatnych, ze światem kryminalnym włącznie. W tym kontekście autor postuluje m.in. utworzenie w urzędach państwowych, przedsiębiorstwach i spółkach strategicznych oraz w koncernach prywatnych odrębnych struktur tzw. trójki (zajmujących się bezpieczeństwem ekonomicznym) na wzór jedyńki (komórki do ochrony tajemnicy państwowej i szeroko rozumianego bezpieczeństwa informacyjnego) oraz dwójki (ds. przygotowań mobilizacyjnych i zarządzania kryzysowego). Świadczy to m.in. o przywiązaniu rosyjskich conceptualistów do starych sowieckich rozwiązań biurokratycznych.

³⁴ Swoją pomocniczą rolę podkreśla także rosyjski wywiad. Według świadectwa dezertera ze Służby Wywiadu Zagranicznego FR Siergieja Trietjakowa po rozwiązaniu KGB Służba „A” została przekształcona w Służbę „MS” (od ros. *mieroprijatija sodiejstwija* – ‘środki, przedsięwzięcia wsparcia’, czyt. wsparcia Kremla). Zob. P. Earley, *Towarzysz J. Tajemnice szefa rosyjskiej siatki szpiegowskiej w Stanach Zjednoczonych po zimnej wojnie*, Poznań 2008, s. 184–185.

- stosowanie zróżnicowanych metod w zależności od celu;
- koncentrowanie wysiłku na słabych (wrażliwych) miejscach przeciwnika;
- zaskoczenie i dezorientację przeciwnika;
- charakter planowy;
- nieograniczone wykorzystanie zasobów przy rozwiązywaniu zadań priorytetowych;
- prowadzenie walki informacyjno-psychologicznej towarzyszącej operacjom specjalnym.

W rosyjskiej literaturze trudno znaleźć informacje na temat zasobów wykonawczych niezbędnych do realizacji operacji i projektów specjalnych, co nie dziwi: ani wywiad, ani Kreml nie ujawniają swojego udziału w tego typu operacjach i projektach. Z badań historycznych dotyczących środków aktywnych, a także z badań współczesnych mechanizmów szerzenia dezinformacji wynika jednak, że są one realizowane przez wiele różnych podmiotów. Można je z grubsza podzielić na podmioty państwowe oraz podmioty niepaństwowe – instrumentalizowane, pośredniczące („proxy”, jak się je dziś określa). Przedstawiono je w tabeli 2.

Tab. 2. Podmioty operacji i projektów specjalnych.

| Podmioty państwowe | Podmioty instrumentalizowane (Proxy) |
|--|---|
| Służby wywiadowcze FR | Stowarzyszenia utworzone przez b. wojskowych i funkcjonariuszy |
| Funkcjonariusze pozostałych resortów siłowych i MSZ | Quasi-militarne bojówki (kozacy, kluby sportów walki, Nocne Wilki) |
| Pracownicy administracji państwowej różnych szczebli | Cerkiew prawosławna |
| Personel dyplomatyczny na placówkach zagranicznych FR | Rosyjskie organizacje trzeciego sektora (np. CIS EMO – dyplomacja publiczna) |
| Personel rządowej Agencji Współpracy z Rodakami (Rossodrużestwo) | Rosyjskojęzyczna diaspora |
| Państwowe fundacje typu Russkij Mir | Fundacje międzynarodowe (finansowane przez oligarchów, np. Władimira Jakunina, Konstantina Małofiejewa) |
| Służby bezpieczeństwa koncernów państwowych (Gazprom, Rosnieft, Rosatom) | Służby bezpieczeństwa i ochrony koncernów prywatnych |

| | |
|---|---|
| Państwowe ośrodki analityczne | „Niezależne” ośrodki analityczne skupiające teoretyków i praktyków |
| Stowarzyszenia finansowane przez państwo (Rosyjskie Towarzystwo Geograficzne, Wojskowe Towarzystwo Historyczne) | Członkowie grup przestępczych, skorumpowani biznesmeni |
| Stowarzyszenia kulturalne, przyjaźni, współpracy | Oddziały dywersji działające na zasadzie komercyjnej (np. prywatna spółka wojskowa Wagnera) czy działające w sieciach społecznościowych (fabryki trolli i trolling) |
| Systemowe partie polityczne (np. Liberalno-Demokratyczna Partia Rosji Władimira Żyrinowskiego) | Organizacje nacjonalistyczne i ekstremistyczne oraz ich młodzieżowe przybudówki |
| Państwowe media (w tym multimedialny koncern Rossija Siegodnia) | Media oligarchów (np. Katehon Małofiejewa czy brytyjskie gazety „The Independent” i „The Evening Standard”, kontrolowane przez Aleksandra i Jewgienija Lebiediewów) |

Źródło: Opracowanie własne.

Podmioty wymienione w tabeli są traktowane przez rosyjskich teoretyków jako tzw. zasoby własne. Podmioty niepaństwowe miałyby wchodzić w organizacyjne „sieci mobilizacyjne” jako ich samodzielne elementy, zarządzane w sposób szczególny. Za odrębną grupę podmiotów można uznać te należące do aktywów wywiadowczych Rosji za granicą: tzw. nielegalów, agenturę w krajach zainteresowania operacyjnego, nieświadomych agentów, zwanych „pożytecznymi idiotami”, tzw. przyjaciół Rosji na Zachodzie (skorumpowani politycy i biznesmeni, partie, ekolodzy, antyglobaliści, pacyfiści) i innych wymagających jeszcze szczegółowych badań. Oczywiście, podkreślanie przez samych Rosjan zdolności operacyjnych oraz roli niepaństwowych podmiotów krajowych i zagranicznych jako „rosyjskiej miękkiej siły” skłania do postawienia pytania, czy nie jest to część ich operacji dezinformacyjnych. Tym ważniejsze w takim kontekście wydaje się dokładne zmapowanie różnorodnych ośrodków wpływu Rosji, pełniących także rolę swoistych centrów werbunkowych³⁵. Umożliwia to ponadto doprecyzowanie celów i dokładniejsze zidentyfikowanie obszarów zagrożonych rosyjskimi działaniami³⁶.

³⁵ Taki werbunek pod obcą flagą prowadzą także obywatele innych krajów, co potwierdził przykład Białorusina Aleksandra Usowskiego. Zob. np. P. Reszka, M. Tomaszewicz, *Jak Kreml finansował skrajną prawicę w Polsce?*, <http://www.newsweek.pl/polska/polityka/jak-kreml-finansowal-skrajna-prawice-w-polsce-artykuly,408023,1.html> [dostęp: 8 I 2018].

³⁶ Zob. J. Darczewska, P. Żochowski, *Środki aktywne...*, tamże, s. 63–68.

Współczesne technologie hybrydowe: podstawy koncepcyjne i organizacyjne

Środki aktywne, których nazwa jest obecnie zastępowana nazwą (terminem) technologie hybrydowe, były przedmiotem wnikliwych badań na Zachodzie w czasie zimnej wojny. Duże zasługi na tym polu miała międzyresortowa komisja do ich zwalczania przy Departamencie Stanu USA, działająca w latach 1981–1992 pod kierunkiem wicesekretarza stanu Dennisa Kuxa. Jej eksperci i członkowie przygotowywali cykliczne raporty na temat sowieckich działań. Sam Kux podjął próbę stypologizowania tych zróżnicowanych instrumentów i podzielił je na wzór typologii źródeł wywiadowczych na białe, szare i czarne. Sprawstwo i odpowiedzialność za działania w strefie białej (działania jawne, z pozycji legalnych) i szarej (z wykorzystaniem metod na w pół legalnych, pod różnego rodzaju przykryciem) przypisał Kremlowi, w czarnej, z wykorzystaniem wywiadowczych metod technicznych i osobowych – KGB.

Ten podział, jak się wydaje, jest aktualny do dziś, mimo że Rosja zrezygnowała z próby zmiany świata według preferencji ideologicznych, które legły u podstaw koncepcyjnych zimnowojennych środków aktywnych. Model doktrynalny uzasadniający obecne działania jest równie sztywny: opiera się na przeciwstawieniu świata rosyjskiego światu zachodniemu, czego podstawę ma stanowić odmienność cywilizacyjna „świata rosyjskiego”, poszerzanego do „świata eurazjatyckiego”. Narracja oparta na tzw. geopolitycznym światopoglądzie naukowym jest równie uproszczona, co w spektakularny sposób ilustruje pseudointelektualna podbudowa projektów i operacji hybrydowych przedstawiona na początku niniejszego opracowania. Jest to ponadto narracja wolna od krępującego działania systemu wartości, którego Rosja nie sformułowała do dziś, a który w praktyce sprowadza się do podważania wartości cudzych. Geopolityka warunkuje też ton tej narracji: Stany Zjednoczone i NATO stały się niejako „wrogiem absolutnym”, który kwestionuje rolę Rosji jako liczącego się bieguna siły na świecie, nadużywa jej zaufania i nieustannie ją upokarza, modelując sytuację światową za pomocą kolorowych rewolucji. Rywalizacja z USA i NATO stała się zarazem uniwersalnym „argumentem” polityki i wewnętrznej (kreowanie iluzji zagrożenia oraz wszechobecnej antyrosyjskiej histerii czy rusofobii), i zagranicznej Rosji. Kwestionując cudze wartości (jak np. suwerenne prawo Gruzji i Ukrainy do określania własnej drogi rozwoju i wyboru sojuszy) oraz walcząc o poszerzenie strefy wpływów, Rosja przedstawia to jako akt obrony jej suwerenności i lustrzaną odpowiedź na cyniczną grę Zachodu. Taki światopogląd stał się podstawą myślenia i działania władz FR i rosyjskich resortów siłowych. Jest on traktowany jako skuteczna „broń koncepcyjna”.

Jeśli chodzi o podstawy organizacyjne, „broń organizacyjną”, to jej istotą jest zarządzanie systemami społecznymi, w tym mechanizmami ich samoorganizacji, i realizacją projektów specjalnych przy wykorzystaniu różnorodnych, sygnalizowanych wyżej podmiotów. W teorii ujmuje się ją w paradygmat „zarządzania

refleksyjnego”³⁷. Jest oczywiste, że modelowanie zachowań społeczeństwa przeciwnika wymaga szczegółowej wiedzy, której dostarcza wywiad. Służby wywiadowcze są wprawdzie najważniejszym, ale tylko jednym z wielu podmiotów wykonawczych i centrów werbunkowych – pisze socjolog Igor Ejdman³⁸. Rozbudowany system organizacyjny ten autor przedstawia w postaci piramidy, na której wierzchołku znajduje się prezydent Putin podejmujący decyzje strategiczne. Jego instrukcje realizuje Administracja Prezydenta (np. jej wiceszef Aleksiej Gromow nadzoruje koncern medialny – tj. kwestie związane z propagandą – w którego skład wchodzi stacja telewizyjna RT i agencja Sputnik; ich agendy zagraniczne także zajmują się „organizowaniem przyjaciół Rosji”), a poszczególni doradcy prezydenta nadzorują MSZ i resorty siłowe. Znajdujące się w Administracji Prezydenta swoiste „punkty dowodzenia” działają z kolei za pośrednictwem wielkich koncernów, stowarzyszeń społecznych, fundacji międzynarodowych, poszczególnych oligarchów itp. Stąd wniosek, że w ostatecznym rozrachunku to Kreml mobilizuje wykonawców, daje sygnał do rozpoczęcia i zakończenia wojen hybrydowych.

Novum polega głównie na wykorzystaniu nowych technologii i kanałów komunikacyjnych, które poszerzyły możliwości Rosji w tym zakresie. Internet zniósł wcześniejsze bariery komunikacyjne, zapewnił dostęp do informacji w czasie rzeczywistym i umożliwił służbom szybkie spenetrowanie informacyjne obiektu działań. Rozwój tzw. nowych mediów (media tradycyjne online i media społecznościowe) stworzył możliwości błyskawicznego upowszechniania spreparowanych treści (ich emitowania na cały świat, powielania, wycinania informacji niepożądanych, narzucania własnej interpretacji), gwarantując przy tym anonimowość nadawcy i dostęp do odbiorcy bez pośredników. Zapewnił też możliwości „wybielania” dezinformacji: odbiorca, szukając potwierdzenia podsunętej mu informacji, uzyskuje ją z kilku innych dezinformujących źródeł. Dziś zresztą zdeinformować można nie tylko człowieka, ale i maszyny: tzw. złe (szkodliwe) boty np. zarządzają ruchem w sieci i kierują go na strony agresora informacyjnego przez zmianę ich pozycji w rankingu wyszukiwarek (tzw. dobrych botów). W rezultacie globalna sieć dostarczyła skrzynki z nowymi narzędziami, co sprawia, że współczesne problemy z agresywną polityką zagraniczną Rosji są tylko wzmocnioną wersją starych.

Posiłkując się badaniami prowadzonymi w czasie zimnej wojny oraz uwzględniając nowe elementy, uwspółcześniony aparat środków aktywnych, czyli technologii hybrydowych – według dzisiejszej terminologii – można przedstawić w sposób zaprezentowany w tabeli 3.

³⁷ Szerzej na ten temat zob. M. Wojnowski, „Zarządzanie refleksyjne” jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w., „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 12, s. 11–36; tenże: *Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 17, s. 11–55.

³⁸ И. Эйджман, *Первая мировая гибридная война*, <http://www.kasparov.ru/material.php?id=59D27ACA13CFD> [dostęp: 5 I 2018]; <http://www.aravot-ru.am/2017/10/05/252828> [dostęp: 5 I 2018].

Tab. 3. Współczesny aparat technologii hybrydowych.

| Rodzaj technologii hybrydowych | Przedsięwzięcia organizacyjne |
|--|---|
| CZARNE (koordynowane przez służby wywiadowcze) | <ul style="list-style-type: none"> – pozyskiwanie agentury wpływu oraz instrumentalizowanie do realizacji celów Rosji osób tego nieświadomych – skrytobójstwa i terroryzm – fabrykowanie dowodów (fałszywe dokumenty, fejki) – grupy pozorowane do przeprowadzania aktów prowokacji, np. dewastacja pomników i miejsc pamięci – akcje quasi-militarne: dywersja i niejawne ograniczone stosowanie przemocy – inspirowanie demonstracji i zamieszek – przekupywanie, korumpowanie i szantażowanie polityków – tworzenie fałszywych kont i sieci botów do prowadzenia ataków cybernetycznych, propagandy 2.0 i organizowania cyberprotestów |
| SZARE (koordynowane przez Kreml) | <ul style="list-style-type: none"> – instrumentalizowanie oraz inspirowanie różnych grup społecznych, w tym partii i organizacji skrajnych – działania za pośrednictwem rosyjskiego sektora pozarządowego i kontrolowanych organizacji międzynarodowych – instrumentalizowanie rosyjskich fundacji i stowarzyszeń, np. Russkij Mir, Rosyjskie Towarzystwo Historyczne – zakładanie prorosyjskich portali oraz ich wspieranie finansowe – zakładanie fabryk trolli i organizowanie prokremlowskich sieci – dokonywanie ataków społecznościowych, trolling |
| BIAŁE (koordynowane przez Kreml) | <ul style="list-style-type: none"> – akcje propagandowe prowadzone za pośrednictwem multimedialnych państwowych agencji informacyjnych (TV RT, Radio Sputnik, RIA Novosti) – przedsięwzięcia realizowane za pośrednictwem oddziałów Rosodrużestwa, RONIÓK-ów (rosyjskie ośrodki nauki i kultury) przy ambasadach Federacji Rosyjskiej, innych organów władzy wykonawczej i ustawodawczej (np. Komisji do Spraw Obrony Suwerenności FR przy Radzie Federacji) – organizowanie wydarzeń o charakterze naukowym i kulturalnym (konferencje, wystawy, rajdy pamięci, stypendia i kursy językowe) |

Źródło: Opracowanie własne na podstawie: D. Kux, *Soviet Active Measures and Disinformation: Overview and Assessment*, "Parameters, Journal of the US Army War College" (Winter 1985).
 Za: С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnyye-sovetskie-meropriyatija-v-putinskoy-rossii> [dostęp: 29 XII 2017].

Na zakończenie warto jeszcze raz zaakcentować, że technologie hybrydowe, zwane niegdyś środkami aktywnymi, ukorzenione w tradycji oraz kulturze politycznej i strategicznej Rosji, stanowiły instrumentarium zróżnicowane: od zwykłej propagandy i dezinformacji opartych na fałszerstwach, do skrytobójstw politycznych i terroryzmu państwowego. Między nimi rozciąga się rozbudowana szara strefa. Ta właśnie strefa to główny obszar konfrontacji Rosji z Zachodem, zorientowanej na destrukcję podstaw zaatakowanych państw (administracyjno-politycznych, społeczno-ekonomicznych oraz kulturowo-światopoglądowych). Jest to jednocześnie obszar najmniej zbadany i wymykający się z pola analizy – ze względu na tajny i na wpół legalny charakter prowadzonych tu działań (a co za tym idzie – brak twardych faktów), brak narzędzi do pomiaru ich skali i dokonanych spustoszeń, a także ze względu na mnogość i różnorodność działających w niej podmiotów pośredniczących.

Podsumowanie: złożona natura rosyjskiego zagrożenia

Działania Rosji wpisują się we współczesną rzeczywistość bezpieczeństwa, którą charakteryzuje rosnące znaczenie zagrożeń niewojskowych (sytuowanych pod progiem wojen konwencjonalnych), zmienność i nieprzewidywalność. W strategii NATO zyskały one miano zagrożeń hybrydowych, lokowanych w obszarze obronności, co nie ułatwia ich zrozumienia i zwalczania. Opisane wyżej działania prowadzone z udziałem służb wywiadowczych FR i różnych „cywilnych” podmiotów agresji hybrydowej są dalekie od jednoznacznie militarnego wymiaru, w związku z czym przeciwdziałanie im metodami wojskowymi jest niewystarczające. Z racji zakulisowego charakteru należy je traktować jako zagrożenia wywiadowcze i lokować w obszarze bezpieczeństwa.

Historyczny termin *środki aktywne* dobrze oddaje transsektorową naturę rosyjskiego zagrożenia. Większość technik konfrontacji FR z otoczeniem zewnętrznym ma charakter pośredni, trudny do uchwycenia. Ich celem jest realizacja interesów strategicznych i wzmocnienie pozycji międzynarodowej Rosji oraz „rozbrojenie” przeciwnika, tj. doprowadzenie do sytuacji, w której aktorzy wewnętrzni będą realizować cele polityki zagranicznej FR. Wykorzystując słaby opór i trudności w identyfikacji zagrożenia, Rosja destabilizuje sytuację w atakowanych państwach, wywiera destrukcyjny wpływ na ich struktury administracyjne i decyzyjne, podważa podstawy społeczne i ekonomiczne, a także podłoże kulturowe (ideologia, system wartości, kultura polityczna, rządy prawa). Jest to zagrożenie jednocześnie zewnętrzne i wewnętrzne, krajowe i ponadnarodowe, na które nie można odpowiedzieć symetrycznie. Działania rozkładowe są prowadzone przez podmioty państwowe i niepaństwowe, w sposób tajny i jawny, legalny i nielegalny. Stanowią proces ciągły, polegający na zintegrowanej aktywności państwa na wielu frontach i z wykorzystaniem różnych kanałów (dyplomatycznych, politycznych, ekonomicznych, militarnych, społecznych, medialnych), podporządkowanej długofalowej strategii wsparcia polityki Kremla.

Narracja strategiczna narzucona przez Rosję zaciera granice między wojną a pokojem, między działaniami ofensywnymi a defensywnymi. Jej najważniejszym elementem jest kształtowanie obrazu Rosji jako ofiary cynicznej gry Zachodu oraz narzucanie opinii, że jest to wojna dwóch stron stosujących środki adekwatne. Tymczasem sytuacja jest z natury asymetryczna: strona zaatakowana może ocenić skalę zniszczeń dopiero po ich skutkach.

Ze względu na to, że długofalowe cele rosyjskiej polityki zagranicznej uwzględniają rewizję obecnego systemu bezpieczeństwa międzynarodowego, w perspektywie średnioterminowej należy oczekiwać, że intensywność i zakres działań przeciwko państwom NATO i UE nie ulegną zmniejszeniu. Świadczą o tym systematyczne poszerzanie zaplecza koncepcyjnego i wykonawczego, jak również włączenie sił i środków militarnych do tzw. arsenału wpływu. Oznacza to, że kryzysotwórcza rola rosyjskiego zagrożenia będzie wzrastać, a jego skuteczne odparcie będzie wymagało zwiększonej uwagi podmiotów odpowiedzialnych za bezpieczeństwo i obronność państw oraz dalszych intensywnych badań dotyczących rosyjskich systemowych projektów organizacyjnych, ich założeń koncepcyjnych, nowych technik wpływu, korupcyjnych mechanizmów finansowania, a także wypracowania procedur pozwalających na jego szybkie i skuteczne zneutralizowanie. Pozwoli to uniknąć myślenia, że agresor jest schematyczny: należy być przygotowanym na nowe, nieznane jeszcze metody konfrontacji politycznej.

Bibliografia:

1. Andrew Ch., Mitrochin W., *Archiwum Mitrochina II. KGB i świat*, Poznań 2006, Rebis.
2. *Biuro Bezpieczeństwa Narodowego. (Mini)słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*, <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035>, MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 5 I 2018].
3. Darczewska J., Żochowski P., *Środki aktywne. Rosyjski towar eksportowy*, <https://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2017-05-30/srodki-aktywne-rosyjski-towar-eksportowy> [dostęp: 5 I 2018].
4. Galeotti M., *Shūzby wywiadowcze Rosji są w stanie politycznej wojny*, <https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/PL/index.htm> [dostęp: 5 I 2018].
5. Earley P., *Towarzysz J. Tajemnice szefa rosyjskiej siatki szpiegowskiej w Stanach Zjednoczonych po zimnej wojnie*, Poznań 2008, Rebis.
6. Grabowski W.T., *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego 2013–2016*, <https://horyzonty.ignatianum.edu.pl/index.php/HP/article/view/756> [dostęp: 5 I 2018].

7. Hałagida I., *Między dezinformacją a rzeczywistością. Prowokacyjne działania służb komunistycznych*, <http://polska1918-89.pl/pdf/miedzy-dezinformacja-a-rzeczywistoscia.-prowokacyjne-dzialania-sluzb-k,5366.pdf> [dostęp: 5 I 2018].
8. Herman M., *Potęga wywiadu*, Warszawa 2002, Bellona.
9. *Internet trolling as a tool of hybrid warfare: the case of Latvia*, NATO StratCom Centre of Excellence, Riga 2016, StratCom.
10. Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego” 2015, nr 2, 49–65. DOI 10.15804/ppk.2015.02.03, <http://www.marszalek.com.pl/przegladprawakonstytucyjnego/ppk24/03.pdf> [dostęp: 5 I 2018].
11. Kacała T., *Komunikacja strategiczna*, <http://cdis.wp.mil.pl/plik/file/Publikacje/kacala.pdf> [dostęp: 5 I 2018].
12. *Komunikat UE z 6 kwietnia 2016 r. w sprawie przyjęcia wspólnych ram przeciwdziałania zagrożeniom hybrydowym i budowania odporności UE, jej państw członkowskich i krajów partnerskich, przy jednoczesnym zacieśnianiu współpracy z NATO w zakresie zwalczania tych zagrożeń*, http://europa.eu/rapid/press-release_IP-16-1227_pl.htm [dostęp: 10 XII 2017].
13. LeVine S., *Labirynt Putina*, Warszawa 2010, AMF.
14. Lukas E., Pomerantsew P., *Winning the Information War. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe*, <https://lif.blob.core.windows.net/lif/docs/default-source/publications/winning-the-information-war-full-report-pdf.pdf?sfvrsn> [dostęp: 15 X 2017].
15. Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, Rytm.
16. Minkina M., *Zagrożenia wywiadowcze dla Unii Europejskiej i Sojuszu Północnoatlantyckiego*, „Doctrina. Studia Społeczno-Polityczne” 2009, nr 6, s. 155–174.
17. Minkina M., Gałek B., *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015, Rytm.
18. Pacepa I.M., Rychlak R.J., *Dezinformacja*, Gliwice 2015, Editio.
19. *Psychosocjotechnika. Dezinformacja. Oręż wojny*, V. Volkoff (oprac.), Komorów 1999, Antyk.
20. Reszka P., Tomaszewicz M., *Jak Kreml finansował skrajną prawicę w Polsce?*, <http://www.newsweek.pl/polska/polityka/jak-kreml-finansowal-skrajna-prawice-w-polsce-,artykuly,408023,1.html> [dostęp: 8 I 2018].
21. Świerczek M., *Działania wobec Attachatu Wojskowego przy Poselstwie RP w Moskwie w początkach jego funkcjonowania jako egzemplifikacja kontr-*

- wywiadowczego *modus operandi* stosowanego przez służby rosyjskie, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-9/1384>, *Przegląd-Bezpieczeństwa-Wewnętrzne-go-nr-17-9-2017.html* [dostęp: 5 I 2018].
22. Świerczek M., *Modus operandi GPU na przykładzie operacji „Trust” opisanej w „Trioach stolicach” W.W. Szulgina*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-3/1180>, *Przegląd-Bezpieczeństwa-Wewnętrzne-go-nr-12-7-2015.html* [dostęp: 5 I 2018].
 23. Świerczek M., *Udział Wiktora Tomira Drymmera w aferze MOCR-Trust w świetle jego artykułu z 1965 r. pod tytułem „Trust”. Wstęp do analizy*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-1/1008>, *Przegląd-Bezpieczeństwa-Wewnętrzne-go-nr-10-6-2014.html* [dostęp: 5 I 2018].
 24. Świerczek M., *Wojna hybrydowa jako strategia polityczna. Próba analizy historycznej na przykładzie działań ZSRS wobec II RP*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-8/1323>, *Przegląd-Bezpieczeństwa-Wewnętrzne-go-nr-16-9-2017.html* [dostęp: 5 I 2018].
 25. Weiss M., *Revealed: The Secret KGB Manual for Recruiting Spies*, <https://www.thedailybeast.com/the-kgb-papers-how-putin-learned-his-spycraft-part-1> [dostęp: 5 I 2018].
 26. *Wojna hybrydowa*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, wydanie specjalne.
 27. Wojnowski M., *Mit „wojny hybrydowej”*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, wydanie specjalne, s. 7–39.
 28. Wojnowski M., *Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 17, s. 11–55.
 29. Wojnowski M., *„Zarządzanie refleksyjne” jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 12, s. 11–36.
 30. Zygar M., *Wszyscy ludzie Kremla. Tajne życie dworu Władimira Putina*, Warszawa 2017, Agora.
 31. Żebrowski A., *Zagrożenia wywiadowcze na progu XXI wieku*, http://cejsh.icm.edu.pl/cejsh/element/...5e6a.../Zagrozenia_wywiadowcze_453-466.PDF [dostęp: 15 I 2018].

Literatura rosyjska:

1. Абрамс С., *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnye-sovetskie-meropriyatiya-v-putinskoj-rossii> [dostęp: 4 I 2018].
2. Бартош А., *Гибридные войны как проявление глобальной критичности современного мира*, „Геополитика и безопасность” 2015, nr 1, s. 71–73.
3. Бартош А., *Гибридные войны как проявление глобальной критичности современного мира*, http://isc.mslu.ru/index.php?option=com_content&task=view&id=366&Itemid=36 [dostęp: 1 IX 2015].
4. Бартош А., *Модель управляемого хаоса в сфере военной безопасности*, „Вестник Академии военных наук” 2014, nr 1, s. 69–78.
5. Бартош А., *Разведка России в противостоянии гибридным угрозам*, http://nvo.ng.ru/spforces/2017-10-06/1_968_scouting.html [dostęp: 5 I 2018].
6. Бобылов Ю.А., *Новые наукоемкие гибридные войны*, <http://www.proatom.ru/modules.php?name=News&file=print&sid=7397> [dostęp: 5 I 2018].
7. Бобылов Ю.А., *Проблема внешней ведомственной конкурентной разведки России. Информационные, правовые и организационные аспекты*, „Информационные войны” 2016, nr 4, s. 67–79.
8. Бобылов Ю.А., *Спецслужбы и стратегия гибридных войн*, www.rusnor.org/pubs/articles/12200.htm.
9. Бобылов Ю.А., *Экспортно-ориентированные инновационные промышленные прорывы России по стратегиям гибридных войн*, „Информационные войны” 2015, nr 1, s. 55–61.
10. Герасимов В., *Мир на гранях войны*, <https://www.vpk-news.ru/articles/35591> [dostęp: 11 XII 2017].
11. Герасимов В., *Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны*, <http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/862-vestnik-avn-2-2016> [dostęp: 10 XII 2017].
12. Горбунов Е., *Фактор стабильности – стратегическая дезинформация*, <http://ricolor.org/history/rsv/good/2/> [dostęp: 11 XII 2017].
13. Демидов О., *Инфовойска России: к структуре нового типа?*, <http://vpoanalytics.com/2017/03/08/infovojska-rossii-k-strukture-novogo-tipa/> [dostęp: 5 I 2018].
14. Ильясов Ф.Н., *Словарь социальных исследований*, 2016, <http://www.jsr.su/dic/dictionary.html> [dostęp: 5 I 2018].

15. Карякин В., *Стратегии непрямых действий, «мягкой силы» и технологии «управляемого хаоса» как инструменты переформатирования политических пространств*, „Информационные войны” 2014, nr 3, s. 29–30.
16. Колобов А.О., *Власть силы и сила власти. (О значении специальных операций в глобальной дипломатии США и других великих держав)*, <https://cyberleninka.ru/article/n/vlast-sily-i-sila-vlasti-o-znachenii-spetsialnyh-operatsiy-v-global-noy-diplomatii-ssha-i-drugih-velikih-derzhav> [dostęp: 5 I 2018].
17. *Контрразведывательный словарь*, Москва 1972, <http://www.kgbdocuments.eu/index.php?1442843474> [dostęp: 15 VI 2017].
18. Манойло А.В., *Гибридные войны и цветные революции в мировой политике*, „Право и политика” 2015, nr 7, s. 918–920.
19. Манойло А.В., *Парадигмы управления международными конфликтами: конкуренция или конфронтация*, „Национальная безопасность” 2011, nr 5, s. 135–142.
20. Манойло А.В., *Технологии несилового разрешения современных конфликтов*, Москва 2014, Горячая линия – Телеком.
21. Панарин И.Н., *Гибридная война против России, 1816–2016 гг.*, Москва 2016, Горячая линия – Телеком.
22. Панарин И.Н., *Гибридная война. Теория и практика*, Москва 2017, Горячая линия – Телеком.
23. Панарин И., *Гибридная война: прошлое, настоящее и будущее*, <http://новости.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B3%D0%B8%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0%D1%8F-%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D1%88%D0%BB%D0%BE%D0%B5-%D0%BD%D0%B0%D1%81%D1%82%D0%BE%D1%8F%D1%89%D0%B5%D0%B5-%D0%B8-%D0%B1%D1%83%D0%B4%D1%83%D1%89%D0%B5%D0%B5-%D0%B8%D0%B3%D0%BE%D1%80%D1%8C-%D0%BF%D0%B0%D0%BD%D0%B0%D1%80%D0%B8%D0%BD/> [dostęp: 5 I 2018].
24. Панарин И., *Гладиаторы гибридной войны*, <http://ruspravda.info/Gladiatorigibridnoy-voyni-23791.html> [dostęp: 5 I 2018].
25. Радченко В., *Главная профессия – разведка*, Москва 2011, <http://litbook.net/book/39527/glavnaya-professiya-razvedka/> [dostęp: 5 I 2018].
26. Эйдман И., *Первая мировая гибридная война*, <http://www.kasparov.ru/material.php?id=59D27ACA13CFD>; <http://www.aravot-ru.am/2017/10/05/252828> [dostęp: 5 I 2018].

Abstrakt

W artykule podjęto próbę przedstawienia środków aktywnych jako elementów strategii działań hybrydowych. Autorka wychodzi z założenia, że w wykrywaniu i diagnozowaniu współczesnych operacji rosyjskich służb wywiadowczych jest pomocna perspektywa historyczna. Takie analityczne ramy pojęciowe umożliwiają pokazanie pewnych uogólnień; prowadzą także do wniosku o ciągłości i złożoności działań będących treścią przywołanych terminów.

Środki aktywne i technologie hybrydowe rozpatrywane w artykule mają ten sam zakres desygnatów i stanowią zbiorcze pojęcia zróżnicowanego instrumentarium oddziaływania politycznego, wojskowego, wywiadowczego, biznesowego, dyplomatycznego, medialnego, ekonomicznego, społecznego, cybernetycznego i in., służącego realizacji długoterminowych celów polityki Kremla. Jest oczywiste, że przeciwdziałanie rosyjskiemu zagrożeniu wymaga równie kompleksowego podejścia.

Słowa kluczowe: środki aktywne, wojna hybrydowa, zagrożenia, wywiad, operacje dezinformacyjno-wywrotowe, tajna operacja.

Danuta Gibas-Krzak

Rosyjska koncepcja Eurazjatyckiego Systemu Obrony Powietrzno-Kosmicznej. Analiza problemu

Celem niniejszego artykułu jest zaprezentowanie możliwości utworzenia Eurazjatyckiego Systemu Obrony Powietrzno-Kosmicznej jako głównego elementu w rozwoju eurazjatyckiej integracji pod przewodnictwem Federacji Rosyjskiej oraz ukazanie ważnej roli geopolitycznej Eurazji we współczesnych stosunkach międzynarodowych. Punktem wyjścia do przeprowadzenia analizy są wnioski i interpretacje przedstawione w opracowaniach prof. Aleksieja Podbieriezkin – naukowca z Moskiewskiego Państwowego Instytutu Stosunków Międzynarodowych Ministerstwa Spraw Zagranicznych Federacji Rosyjskiej. Jest on cenionym analitykiem, doradcą prezydenta FR oraz autorem kilku monografii dotyczących bezpieczeństwa i stosunków międzynarodowych (m.in.: Алексей Иванович Подберезкин, *Евразийская воздушно-космическая оборона*, Moskwa 2013). W 2017 r. A. Podbieriezkin wydał dwutomowe opracowanie na temat współczesnej polityki wojskowej Federacji Rosyjskiej: *Современная военная политика России: учебно-методический комплекс* (Moskwa 2017).

Geopolityczne znaczenie Eurazji

Na znaczenie Eurazji wskazywał w 1990 r. Zbigniew Brzeziński w swoim opracowaniu *Wielka szachownica*. Podkreślał w nim fenomen wojskowo-polityczny tego obszaru, przedstawionego jako gigantyczna szachownica, na której rozgrywa się walka o światową hegemonię. Niemniej jednak już w 1904 r. istotne znaczenie kontynentu dostrzegł angielski geograf Halford John Mackinder. Uważał on, że ten, kto rządzi tzw. Wyspą Świata¹, panuje nad światem, ponieważ na tym właśnie obszarze rozgrywają się najważniejsze wydarzenia mające wpływ na dzieje ludzkości. Innymi słowy – to tutaj toczy się historia. Centralnym punktem „Wyspy Świata” jest zaś Eurazja oraz położony w niej „Heartland” (leżący w jej północnej i środkowej części). Zgodnie z tą teorią kontrola nad Heartlandem gwarantuje władzę nad światem. H.J. Mackinder przyznawał, że jego granic nie da się jednoznacznie określić. Sam niejednokrotnie zmieniał jego zasięg, raz ograniczając go do terytorium Rosji, innym razem rozciągając aż do obszaru Mongolii².

Powyższe założenia miały istotny wpływ na rosyjskie środowisko polityczne, czego rezultatem w czasach ZSRR była konceptualizacja jednej z najbardziej istotnych

¹ „Wyspa Świata” (*World Island*) obejmuje masę kontynentalną, na którą składają się: Europa, Azja oraz Afryka. Pozostałe obszary: Ameryka Południowa i Północna, Australia oraz Archipelag Malajski – są satelitami „Wyspy Świata” i odgrywają mniejszą rolę. Zob. A. Cianciara, *Klasyczne koncepcje geopolityczne*, w: *Geopolityka*, A. Dybczyński (red. nauk.), Warszawa 2013, s. 59–61.

² Tamże.

rosyjskich koncepcji geopolitycznych – eurazjatyizmu. Odnosi się ona nie tylko do spraw ideowych, lecz także jest pojmowana jako oryginalny ruch umysłowy, w którym podkreślono wyjątkowość rosyjskiej historii i kultury, rozumianych jako odrębna cywilizacja. To stało się podstawą twierdzenia, że eurazjatyzm jest kluczem do tajemnicy duszy rosyjskiej³. W opinii eurazjatów Rosja nie jest ani Azją, ani Europą; należy ją traktować jako odrębną jednostkę geograficzną, stanowi bowiem region, na którego rozwój zasadniczy wpływ miała specyfika etniczna Wielkorusów. Przyjmowano, że obszar Eurazji pokrywa się z granicami Rosji. Eurazjatów charakteryzowała niechęć do Zachodu, a ich zadaniem było udowodnienie, że Rosja ma prawo do odrębności cywilizacyjno-kulturowej. Piotr Sawicki podkreślał, że cywilizacja rosyjska jest powołana do odgrywania wyjątkowej roli w ramach Starego Świata (Azja i Europa), polegającej na utrzymaniu jego jedności⁴. W tym sensie Rosja powinna być kontynuatorką geopolitycznych tradycji imperium mongolskiego, co tłumaczono w ten sposób, że rosyjska presja na Skandynawię, Polskę, Persję i Turcję zastąpiła najazdy koczowniców na strefę kontynentalno-oceaniczną⁵.

Wielu badaczy przywołuje fakt, że po rozpadzie ZSRR eurazjatyzm stał się najbardziej wpływową orientacją w rosyjskiej geopolityce. Odrodził się on w doktrynalnej postaci neoeurazjatyizmu, za którego głównego reprezentanta uważa się Aleksandra Dugina. W tym podejściu Zachód (głównie USA) jest uznawany za wroga, podobnie jak ideologia atlantyizmu⁶. A. Dugin dostrzegał odrębność kulturową i geograficzną Eurazji, jednak w jego teoriach imperium euroazjatyckie rozrasta się i sięga aż do Afryki Środkowej. Zgodnie z tą ideologią Rosja miałaby tworzyć alians z Chinami, Indiami oraz Iranem (wymienia się nawet Irak i Tybet), skierowany przeciwko światu anglosaskiemu. Razem występowałyby przeciwko śmiertelnemu wrogowi, za którego został uznany Zachód na czele z USA, ze względu na przekonanie, że amerykańska wersja liberalizmu stanowi zagrożenie dla Rosji i całej planety. Europa i prozachodnie państwa Azji Wschodniej, z Japonią w pierwszym rzędzie, docelowo miałyby zostać dołączone do sojuszu eurazjatyckiego⁷.

Warto także wspomnieć, że w 1997 r. ciekawą koncepcję geopolityczną przedstawił Władimir Chaczaturow, który zwrócił uwagę na cztery następujące determinanty światowego porządku:

- 1) przestrzeń geograficzna zajmowana przez Indie i Chiny stanowi geopolityczne centrum świata;

³ R. Paradowski, *Eurazjatyckie imperium Rosji. Studium idei*, Toruń 2001, s. 38–39.

⁴ J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, s. 113 i nast.

⁵ Tamże.

⁶ I. Massaka, *Eurazjatyzm. Z dziejów rosyjskiego misjonizmu*, Wrocław 2001, s. 175–194. *A t l a n t y z m* to jeden z nurtów we współczesnej geopolityce rosyjskiej odwołujący się do tradycji rosyjskiego okcydentalizmu, którego zasadniczym założeniem było wiązanie pomyślności Rosji z jej współpracą z Zachodem. Zob. J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej...*, s. 38.

⁷ T. Klin, *Geopolityka pozimnowojenna*, w: *Geopolityka...*, s. 253.

- 2) globalne procesy geopolityczne są inicjowane przez geopolityczne centrum świata;
- 3) w przebiegu globalnych procesów geopolitycznych tworzą się dwa bieguny: stabilny, który obejmuje geopolityczne centrum świata, i niestabilny;
- 4) wraz ze zmianą przebiegającą na obszarze choćby jednego bieguna świat wchodzi w okres geopolitycznej niestabilności (globalne wojny i rewolucje).

Jak widać, zgodnie z tymi założeniami Rosja jest postrzegana jako część bieguna zarówno stabilnego, jak i niestabilnego, w związku z czym odgrywa rolę „geopolitycznej osi świata”. Zdaniem W. Chaczaturowa celem rosyjskiej polityki powinno być umocnienie znaczenia tej osi przez reintegrację państwa oraz zbudowanie silnych relacji z Chinami oraz Indiami⁸.

Renesans programów geopolitycznych sprawił, że w istotny sposób oddziałują one na całe środowisko międzynarodowe w drugiej dekadzie XXI w., co jest związane przede wszystkim z przeorientowaniem sił w istniejącym układzie jako następstwem zmian w polityce zagranicznej USA. Sprawa dotyczy przede wszystkim sytuacji politycznej w Azji Środkowej oraz Azji Południowo-Wschodniej. Nie można zaprzeczyć, że obecnie odnotowuje się wzrost niestabilności w wielu państwach i regionach świata, a zwłaszcza na obszarze Eurazji, na który przypada w ostatnich dziesięcioleciach 90 proc. wszystkich konfliktów wojskowych. Dlatego też jest ważne, aby podjąć kompleksowe działania służące obronie zbiorowej w tym regionie, zgodnie z paradygmatem Heartlandu, który wydaje się niezwykle wpływowy w bieżących relacjach strategicznych, zwłaszcza w odniesieniu do aktualnej polityki Federacji Rosyjskiej. Zdaniem rosyjskich analityków:

Poradziecka Azja Środkowa w polityce zagranicznej Waszyngtonu przeszła drogę od obiektu trzeciorzędnego zainteresowania w Rosji do jednego z głównych obiektów interesów amerykańskich w świecie. Prognozowane skomplikowanie problemów afgańskich pociągnie za sobą także wzrost zainteresowania USA, Rosji i Chin tym regionem. W związku z tym możliwy jest wzrost konfliktu interesów tych państw w regionie⁹.

Warto przy tym zauważyć, że to wojskowo-polityczne właściwości Eurazji stały się pierwotną przyczyną, która w XXI w. spowodowała nasilenie się konfrontacyjności na jej obszarze. Te cechy charakterystyczne wyrażają się zwłaszcza w:

- specjalnej roli geopolitycznej, gospodarczej i historycznej Eurazji w świecie, która w najbliższym dziesięcioleciu będzie gwałtownie rosła. I to nie tylko z powodu szybkiego tempa rozwoju Chin, Indii oraz innych państw, lecz także z powodu wielu sprzeczności cywilizacyjnych i geopolitycznych kumulujących się w ostatnich dziesięcioleciach;

⁸ Z. Lach, J. Skrzyp, *Geopolityka i geostrategia*, Warszawa 2007, s. 56–57.

⁹ А.А. Казанцев, *Политика США в постсоветской Центральной Азии: характер и перспективы*, <http://ehd.mgimo.ru/IORManagerMgimo/file?id=E3DAB956-8956-310D-0D-4C-2235B2392202> [dostęp: 3 I 2018].

- wzrastającej roli Rosji w Eurazji, która może być głównym graczem na kontynencie, ale której wpływy nie są w adekwatne do roli, jaką chciałaby na tym obszarze odgrywać, zwłaszcza w regionach na wschód od Uralu, gdzie jest skoncentrowany olbrzymi potencjał surowcowy i gdzie znajdują się arterie transportowe o znaczeniu światowym;
- koncentracji zasobów, (...) *przy czym, nie tylko energetycznych, ale też rolniczych, wodnych, leśnych. Ogromny potencjał ludzki Eurazji, którego wskaźnik jakościowy szybko rośnie (w samych tylko Chinach w okresie reform ponad 300 mln osób uzyskało wyższe wykształcenie), zacznie w sposób nieunikniony odgrywać kluczową rolę w rozwoju światowym*¹⁰;
- stosunkowej niezależności od „państw morskich” – poprzednich liderów¹¹.

Programowe podstawy Eurazjatyckiego Systemu Obrony Powietrzno-Kosmicznej

Badania podejmowane przez A. Podbieriezkiną w czasie, gdy wciąż aktualny pozostaje konflikt na liniach Moskwa–Waszyngton i Moskwa–Unia Europejska, pozwalają dostrzec inną perspektywę działań w zakresie bezpieczeństwa międzynarodowego, a także zdefiniować rolę Rosji na „euroazjatyckiej szachownicy”. Rzeczywiście, proces rozszerzenia NATO na wschód, do którego doszło po zakończeniu zimnej wojny, przekształcił ten sojusz z organizacji regionalnej w ogólnoswiatową, włączając w jej sferę odpowiedzialności całą Eurazję. Wydarzenia w Iraku, Afganistanie, stanowisko wobec Syrii oraz Iranu świadczą o tym, że NATO jako koalicja wojskowo-polityczna jest jedyną rzeczywistą siłą międzynarodową zapewniającą bezpieczeństwo w Eurazji. Niemniej jednak za alternatywę dla jej potencjału można uważać Szanghajską Organizację Współpracy (SzOW)¹² oraz utworzoną w ramach Wspólnoty Niepodległych Państw Organizację Układu o Bezpieczeństwie Zbiorowym (OUBZ), która jest narzędziem integracji przestrzeni poradzieckiej w zakresie obronnym i militarnym.

W Szanghajskiej Organizacji Współpracy Rosja i Chiny odgrywają dominującą rolę, przy czym Chiny są liderem w dziedzinie ekonomii, natomiast Rosja oferuje pozostałym członkom przede wszystkim współpracę polityczno-militarną¹³. Co więcej, Rosjanie i Chińczycy są gotowi do finansowania niezależności pozostałych członków

¹⁰ А.И. Подберезкин, *Евразийская воздушно-космическая оборона*, Москва 2013, s. 25.

¹¹ Tamże. Ten problem dotyczy teorii geopolitycznej, zgodnie z którą najważniejsze znaczenie dla dziejów świata ma nie Heartland, tylko szeroki pas półwyspów (tzw. Rimland) otaczających Heartland. Rimland ma istotne znaczenie w teoriach geopolitycznych Nicholasa Johna Spykmana, według którego stanowi on centrum światowej potęgi. W obrębie Rimlandu znajdują się: kontynentalna Europa, Bliski Wschód, Indie, Chiny oraz półwyspy: Indochiński, Malajski i Koreański. Zob. N.J. Spykman, *The geography of the peace*, New York 1944, s. 36–40.

¹² L. Firmanty, *Szanghajska Organizacja Współpracy jako element polityki bezpieczeństwa Chińskiej Republiki Ludowej*, w: *Badania wschodnie. Polityka wewnętrzna i międzynarodowa*, W. Baluk, Z.J. Winnicki (red.), Wrocław 2008, s. 236–237.

¹³ M. de Haas, *Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization*, „The Journal of Slavic Military Studies” 2017, nr 1, s. 1–2.

organizacji od Zachodu. Rosja jest zainteresowana wzmocnieniem tej organizacji jako narzędzia w globalnej rywalizacji z USA w taki sposób, aby z SzOW uczynić polityczną przeciwwagę dla państw zachodnich¹⁴.

Tym działaniom służą badania naukowców z Moskiewskiego Państwowego Instytutu Spraw Międzynarodowych (Московский государственный институт международных отношений, MGIMO), w tym A. Podbieriezki, który jest jednym z wielu zwolenników prowadzenia bardziej aktywnej polityki opartej na ideach eurazjatyckich, z przewodnią rolą Rosji. Podjęte działania mają charakter strategiczny, czego wyrazem było powołanie w grudniu 2011 r. Wojsk Obrony Powietrzno-Kosmicznej – W(OPK), tj. nowego rodzaju wojsk, który jest przeznaczony do zapewnienia bezpieczeństwa Rosji w sferze powietrzno-kosmicznej¹⁵. Nie przypadkiem właśnie dlatego na szczycie szefów państw WNP w Aszhabadzie, który odbył się w grudniu 2012 r., rozważano kwestię nie tyle projektów ekonomicznych, ile stworzenia Połączonego Systemu Obrony Przeciwrakietowej państw WNP. W tym celu powołano specjalny komitet koordynacyjny. Poparcie uzyskała propozycja Rosji, aby w ramach wspomnianej inicjatywy zostały zintegrowane jednostki rosyjskie i pododdziały utworzonych w 2011 r. Wojsk Obrony Powietrzno-Kosmicznej (obecnie Siły Powietrzno-Kosmiczne Federacji Rosyjskiej). Można to nazwać pierwszym krokiem do utworzenia Eurazjatyckiej Obrony Powietrzno-Kosmicznej.

Formowanie kilku ośrodków siły militarnej w Eurazji jest skierowane na uzyskanie potencjałów strategicznego uzbrojenia ofensywnego, a przede wszystkim – powietrzno-kosmicznego komponentu precyzyjnego rażenia o różnym przeznaczeniu¹⁶. Prace nad Eurazjatycką Obroną Powietrzno-Kosmiczną są asertywnym krokiem Rosji, która zmierza do przejścia odpowiedzialności za bezpieczeństwo Eurazji w obawie przed dominacją NATO i USA na jej obszarze. Główne tezy opracowania A. Podbieriezki tworzą paradygmat wspólnego bezpieczeństwa, co ma szczególne znaczenie w obliczu wzrastających zagrożeń współczesnego świata, który ma być jednocześnie odpowiedzią na antyrosyjskie (zdaniem rosyjskich analityków) dążenia i plany NATO.

Wyjątkowo niebezpieczny charakter przybiera obecnie problem Korei Północnej, w związku z próbami jądrowymi przeprowadzonymi przez ten kraj, co rodzi zagrożenie wciągnięcia Półwyspu w wojnę. To z kolei z pewnością doprowadziłoby do interwencji Stanów Zjednoczonych. Skutki ewentualnego konfliktu z udziałem supermocarstwa są nie do przewidzenia. Z badań przeprowadzonych przez rosyjskich naukowców można wywnioskować, że Rosja obawia się dominacji amerykańskiej w Eurazji. Zdaniem A. Podbieriezki jest oczywiste, że USA dążą do zablokowania odrodzenia się strategicznej obecności Rosji na tym obszarze, a także utworzenia sojuszu politycznego pomiędzy Moskwą, Pekinem i Teheranem. Nie bez znaczenia

¹⁴ Ł. Firmanty, *Szanghajaska Organizacja Współpracy...*, s. 236–237.

¹⁵ W dniu 5 II 2006 r. została zatwierdzona koncepcja Formowania Zintegrowanego Systemu Obrony Powietrzno-Kosmicznej do 2016 r. Zob. M. Depczyński, *Rosyjskie Siły Zbrojne. Od Milutina do Putina*, Warszawa 2015, s. 240.

¹⁶ А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 50–51 i nast.

pozostaje także i to, że dla USA Azja Środkowa jest geopolitycznie ważnym przyczółkiem w regionie na wypadek ewentualnej konfrontacji z Rosją i Chinami. W te idee wpisują się założenia doktryny morskiej Federacji Rosyjskiej z 2015 r. Podstawowe sformułowanie dla nowej doktryny zostało zawarte w punkcie 52 dokumentu: *Głównym nie do przyjęcia elementem dla Federacji Rosyjskiej w relacjach z NATO są plany przesuwania infrastruktury wojskowych sojuszu ku jej granicom oraz próby przyznawania sojuszowi globalnych funkcji*¹⁷. Doktryna ma dwa wymiary: globalny – adresowany głównie do Stanów Zjednoczonych, i europejski – skierowany do NATO. Ten zapis, wyrażony w pkt 52, może być odczytany jako przesłanie dla decydentów wojskowych w NATO i USA, że Federacja Rosyjska nie dopuści do przewagi Stanów Zjednoczonych w skali globalnej¹⁸. Warto zauważyć, że taki sam wydźwięk mają inne dokumenty strategiczne FR, np. zawarte w znowelizowanej *Strategii Bezpieczeństwa* oraz *Doktrynie Obrony*, opracowanych w 2000 r. Podstawowe priorytety bezpieczeństwa, czyli polityczne i ekonomiczne zagrożenie wewnętrzne, zastąpiono zagrożeniem zewnętrznym, tj. ingerowaniem w strefę wpływów przez inny podmiot.

Jako istotne niebezpieczeństwo wymieniono także konflikty militarne o dużej skali. Jednocześnie uwypuklono rolę Rosji jako mocarstwa, które zamierza zagwarantować sobie własne wpływy w wymiarze regionalnym i globalnym. Podkreślono również, że NATO i USA w sposób nieusankcjonowany prawem próbują ingerować w rosyjską strefę interesów i że utrzymywanie ładu jednobiegunowego z hegemonią amerykańską prowadzi do zaburzeń oraz konfliktów na skalę światową¹⁹. W tym kontekście nie budzą zdziwienia wywody A. Podbieriezki, że Rosja pretenduje do bycia głównym aktorem eurazjatyckiej integracji i promuje własny system wartości nie tylko w kulturze i ekonomii, lecz także w dziedzinie bezpieczeństwa międzynarodowego. Aby osiągnąć ten cel, będzie musiała w jeszcze większym stopniu, niż w ostatnich latach, akcentować swoją politykę zagraniczną i wojskową na kierunkach południowym i wschodnim. Tym bardziej, że regiony „na wschód od Uralu” stają się jej najważniejszym interesem politycznym. Jednocześnie państwo rosyjskie obawia się dążeń Zachodu, co najlepiej wyraża się w słowach A. Podbieriezki:

Licząc na to, że uda się zachować jedność terytorialną, suwerenność i bezpieczeństwo Eurazji tylko przy pomocy prawa międzynarodowego i międzynarodowych instytucji – to naiwność. Podobnie jak naiwnie było liczyć M. Gorbaczowowi na wartości ogólnoludzkie. Znanych jest немало wypowiedzi, że Rosja nie może rządzić się bogactwami ukrytymi w czeluściach Syberii, czy też nieustannie dysponować takimi ogromnymi przestrzeniami, z takimi zapasami surowców naturalnych (M. Albright, M. Thatcher, Z. Brzeziński), które jawnie kolidują z normami międzynarodowymi. Jak też i otwarte próby wykorzystania presji siłowej i miękkiej siły wobec Rosji.

¹⁷ J. Symonides, *Nowa doktryna morska Federacji Rosyjskiej*, „Kwartalnik Bellona” 2016, nr 1, s. 13.

¹⁸ Tamże.

¹⁹ M. Depczyński, *Rosyjskie Siły Zbrojne...*, s. 29–30.

Naprawić tę niesprawiedliwość można w opinii wielu polityków tylko w drodze rewizji granic państwowych Rosyjskiej Federacji, co w oczach zachodnich polityków wcale nie wydaje się aż tak niemożliwe. W tych celach może być realizowane całe mnóstwo scenariuszy, wśród których najbardziej bezpiecznym i właściwym pod względem politycznym jest zmuszenie Rosji pod groźbą użycia siły militarnej, aby sama zrezygnowała z kontroli nad korytarzami transportowymi, zasobami, a następnie jednością terytorialną. Obecnie takie kalkulacje rzeczywiście istnieją. Co więcej, historia dowodzi, że podobny rozwój wydarzeń częściej jest normą, niż wyjątkiem. I to nie tylko w przeszłości, ale i w najnowszej historii, gdzie ostatnimi przykładami były ZSRR i Jugosławia²⁰ (tłum. aut.).

Z tych wywodów wynika, że Rosja powinna podjąć działania zapobiegawcze przeciwko ewentualnym działaniom rewizjonistycznym skierowanym przeciwko niej.

Kontynuacja doktryny Władimira Putina

Zdaniem A. Podbieriezkińa nie ma podstaw do tego, aby uważać, że nastąpi osłabienie napięcia w Eurazji lub rezygnacja USA z przeciwdziałania procesom integracyjnym na tym kontynencie. Strategiczne interesy USA w Azji Środkowej po raz pierwszy zostały wyraźnie zdefiniowane w kwietniu 1997 r. w specjalnym raporcie skierowanym przez Departament Stanu do Kongresu. W dokumencie wskazywano, że USA, będące jednym z największych na świecie konsumentów energii, są zainteresowane „rozszerzeniem i dywersyfikacją” światowych zasobów energetycznych. Co więcej, konstatowano, że z uwagi na swoje właściwości interesy amerykańskie w tym regionie noszą charakter nie tylko ekonomiczny, lecz także strategiczny, gdyż (...) *problem bezpośrednio dotyczy zapewnienia bezpieczeństwa Zachodu*. Z kolei w doktrynalnym ujęciu Rosjan pojawiają się tezy, że zadaniem rosyjskiej polityki w regionie Eurazji jest sformowanie wspólnej pokojowej przestrzeni bezpieczeństwa i stabilizacji opartej na zasadzie niepodzielności bezpieczeństwa wspólnego, współpracy i wzajemnego zaufania²¹.

Nie dziwi to, że te sprawy, odnoszące się do strategicznych priorytetów funkcjonowania w środowisku międzynarodowym, pozostają niezmiennym wykładnikiem polityki zagranicznej prowadzonej przez prezydenta Władimira Putina od roku 2000. Warto wspomnieć, że zostały one mocno zaakcentowane w czasie jego wystąpienia 10 lutego 2007 r. na monachijskiej konferencji bezpieczeństwa, podczas której wygłosił on tzw. mowę monachijską, nazwaną następnie *Doktryną Putina*. Stanowi ona wykładnię zasad nowoczesnej polityki zagranicznej Rosji opartej na całkowitej krytyce jednobiegunowości, czyli ładu światowego, w którym władzę sprawuje jeden hegemon (USA). W ocenie Putina, jednobiegunowość jest przyczyną nowych wojen

²⁰ А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 49–50.

²¹ А.И. Подберезкин, *Современная военная политика России: учебно-методический комплекс*, t. 2, Москва 2017, s. 910.

i napięć w stosunkach międzynarodowych, prowadzi do niepowstrzymanego hiperużycia siły militarnej w relacjach międzynarodowych, co z kolei sprawia, że świat staje w obliczu permanentnego konfliktu, kolejnego wyścigu zbrojeń i braku bezpieczeństwa w sytuacji nowych zagrożeń, takich jak terroryzm²². Co więcej, Putin przedstawił rosyjską kontrpropozycję wobec strategii amerykańskiej, jaką jest zbudowanie nowej architektury globalnego bezpieczeństwa (*the architecture of global security*)²³, mającej na celu ustanowienie świata wielobiegunowego, w którym wpływy jednego mocarstwa byłyby równoważone przez oddziaływanie regionalnych ośrodków władzy: Unii Europejskiej, Japonii, Rosji, Chin, Indii i Brazylii²⁴.

Putinowska doktryna została oceniona jako krytyka stanowiska Zachodu wobec Rosji, który dążąc do zapewnienia sobie przewagi geopolitycznej w Europie i Azji Centralnej, nie docenił aspiracji Federacji Rosyjskiej po zakończeniu zimnej wojny. Rosja tymczasem poczuła się zagrożona ze strony unilateralizmu amerykańskiego, którego egzemplifikacją stało się okrażanie jej przez siły NATO, począwszy od republik nadbałtyckich, a skończywszy na bazach amerykańskich w Azji Centralnej. W ocenie wielu komentatorów Rosja przedstawiła siebie jako „obleżoną twierdzę”, oskarżyła USA o nowy wyścig zbrojeń, nieprzestrzeganie prawa międzynarodowego, jak również o ingerencję w politykę państw WNP²⁵. A co najważniejsze – nie godziła się na istniejący ład jednobiegunowy i dążyła do poprawy swojej pozycji politycznej na arenie międzynarodowej²⁶.

Innym postulatem obecnym w polityce Federacji Rosyjskiej po zakończeniu zimnej wojny jest propozycja przyjęcia nowego układu bezpieczeństwa zbiorowego, która została przedstawiona przez Dmitrija Miedwiediewa w 2008 r. Pierwszym etapem nowego planu miałyby być zwołanie szczytu Organizacji Bezpieczeństwa i Współpracy (OBWE) z udziałem wszystkich struktur bezpieczeństwa, łącznie z NATO, UE, WNP oraz Organizacją Układu o Bezpieczeństwie Zbiorowym²⁷. Ta propozycja stanowiła kontynuację idei i programów, które wyznaczyły kierunek w rosyjskiej polityce zagranicznej po zimnej wojnie, gdyż już w 1994 r. Rosja proponowała, aby przekształcić Konferencję Bezpieczeństwa i Współpracy w Europie (KBWE) w rodzaj regionalnej ONZ, z Radą Bezpieczeństwa (Komitet Wykonawczy). KBWE-OBWE miała bowiem stanowić polityczną nadbudowę europejskiego systemu bezpieczeństwa i zapewniać Rosji równoprawny z Zachodem wpływ na zarządzanie przestrzenią euroatlantycką (chodziło głównie o możliwość współdecydowania

²² D. Gibas-Krzak, *Świat w polityce zagranicznej Federacji Rosyjskiej*, „Kwartalnik Bellona” 2010, nr 4, s. 32–42.

²³ V. Putin, *Speech and the Following Discussion at the Munich Conference on Security Policy*, <http://en.kremlin.ru/events/president/transcripts/24034> [dostęp: 3 I 2018].

²⁴ Tamże.

²⁵ S. Blank, *Threats to and from Russia: an Assessment*, „Journal of Slavic Military Studies” 2008, nr 3, s. 515.

²⁶ M. Stuermer, *Putin i odrodzenie Rosji*, Wrocław 2008, s. 15.

²⁷ A. Krzymowski: *Plan Miedwiediewa – nowa architektura bezpieczeństwa?*, „Sprawy Międzynarodowe” 2009, nr 2, s. 23–24.

w sprawach dotyczących wstępowania do NATO nowych państw)²⁸. W dniu 8 października 2008 r. podczas konferencji w Evian we Francji prezydent Miedwiediew, postulując wzmocnienie ONZ, przedstawił kilka zasad (nazwanych później *Planem Miedwiediewa*), na których miałyby się oprzeć nowa architektura bezpieczeństwa europejskiego. Należy do nich zaliczyć:

- poszanowanie integralności terytorialnej, suwerenności i politycznej niezależności;
- niedopuszczenie do użycia siły oraz groźby jej użycia;
- sprzeciw wobec prób zapewnienia własnego bezpieczeństwa kosztem bezpieczeństwa innych;
- brak zgody na działania osłabiające jedność wspólnej przestrzeni bezpieczeństwa;
- brak zgody na rozwój sojuszy wojskowych na niekorzyść bezpieczeństwa innych uczestników traktatu.

Najistotniejsze znaczenie dla wzrostu pozycji mocarstwowej Rosji miała jednak idea niepodzielności bezpieczeństwa dla wszystkich, dzięki której Moskwa zyskałaby wpływ na rozszerzenie NATO oraz na decyzje w sprawach rozmieszczenia w Europie Środkowej elementów tarczy antyrakietowej²⁹. Warto podkreślić, że te idee stały się zasadnicze dla elit politycznych Federacji Rosyjskiej, a wypracowane strategiczne programy działania w zakresie obronności nadal opierają się na tych samych założeniach, sformułowanych po zakończeniu międzyblokowej konfrontacji. W ocenie wielu analityków celem Rosji nie jest jednak dążenie do ustanowienia ładu wielobiegunowego, tylko przejęcie roli hegemonu, co stanowi powrót do zimnowojennej rywalizacji między ZSRR a USA.

Przyszłość koncepcji Aleksieja Podbieriezkina

Należy przyjąć, że pomysł Eurazjatyckiego Systemu Obrony Powietrzno-Kosmicznej stanowi rozszerzenie dotychczasowych koncepcji ideowo-programowych Rosji, związanych z przekształceniem ładu międzynarodowego. Tym razem jednak jest on wzorowany na komponencie wojskowym i odnosi się do obszaru Eurazji. Pod pojęciem Obrony Powietrzno-Kosmicznej (OPK) należy rozumieć rozwinięte siły i środki zapewniające obronę Federacji Rosyjskiej i jej sojuszników przed napaścią z powietrza i kosmosu, na ziemi i morzu, w przestrzeni powietrznej i okołoziemskiej, połączone kontaktami funkcjonalnymi. Do jej zadań zaliczamy:

- uprzedzanie o napaści rakietowej i kosmicznej oraz rozpoznawanie przestrzeni kosmicznej i informowanie o niej wojsk;
- niszczenie bloków bojowych międzykontynentalnych rakiet balistycznych i rakiet balistycznych okrętów podwodnych, niszczenie lub funkcjonalne obездwładnienie aparatów kosmicznych przeciwnika;
- uprzedzanie o napaści powietrznej, rozpoznawanie sytuacji w powietrzu i kontrola wykorzystania przestrzeni powietrznej; obrona najważniejszych obiektów

²⁸ A. Брыс, *Rosja w XXI wieku. Gracj światowy czy koniec gry?*, Warszawa 2008, s. 120.

²⁹ Д. Медведев, *Выступление на Конференции по вопросам мировой политики*, Evian, <http://kremlin.ru/events/president/transcripts/1659> [dostęp: 3 I 2018].

zarządzania państwowego i wojskowego przed uderzeniami środków napadu powietrzno-kosmicznego, obrona gospodarki i infrastruktury, a także dużych zgrupowań wojsk i obiektów sił zbrojnych;

- określenie sytuacji radioelektronicznej, zapewnienie obrony radioelektronicznej obiektów OPK³⁰.

Do sprawnego działania tego systemu jest wymagana rozbudowa i integracja systemów wojskowych. Chodzi o to, aby wyposażać Siły Zbrojne Federacji Rosyjskiej we współczesne środki i systemy Obrony Powietrzno-Kosmicznej, a także konkurować na równych prawach z głównymi producentami systemów Obrony Powietrznej (OP) i OPK. Obecnie najsilniejszy potencjał wojskowo-polityczny mają państwa NATO, które są głównym dostawcą zarówno środków napadu powietrzno-kosmicznego, jak i środków OP i OPK w świecie. Co więcej, intensyfikuje się kompleks wojskowo-przemysłowy i rynek zbrojeń Chińskiej Republiki Ludowej. Kraje NATO oraz ich sojusznicy, a także Chiny, są zainteresowane rozwojem własnych środków OP i OPK³¹.

Ważność programu OPK polega na tym, że obecnie nie ma żadnego połączanego systemu bezpieczeństwa eurazjatyckiego; do tej roli pretenduje tylko NATO, które rozszerza swoje wpływy na cały kontynent.

W ujęciu A. Podbieriezkiha istnieje kilka możliwych scenariuszy kształtowania nowego systemu, które sprowadzają się do:

- 1) stworzenia systemu bezpieczeństwa eurazjatyckiego (na wzór OBWE), w którego skład wchodziłyby wszystkie kraje od Irlandii do Filipin i który miałby nie tylko zobowiązania polityczne, lecz także mechanizmy ich realizacji;
- 2) formowania koalicyjnych systemów bezpieczeństwa międzynarodowego, w których skład wchodziłyby najważniejsze państwa i sojusze kontynentu:
 - USA
 - UE
 - Chiny
 - Indie
 - Rosja;
- 3) rozwoju istniejących sojuszy wojskowo-politycznych (koalicji) i tworzenia nowych: OUBZ, SzOW itp.³²

Rosyjscy analitycy, obawiając się dominacji NATO, stawiają tezę, że inicjatywy integracyjne w Eurazji pod przewodnictwem Rosji będą uznane przez USA za niepotrzebne, gdyż stanowią niebezpieczeństwo dla hegemonii amerykańskiej³³. Dlatego Sojusz będzie wszelkimi sposobami przeciwdziałal próbom powołania do życia jakiegokolwiek koalicji, ma bowiem wiele instrumentów, aby nie dopuścić do sytuacji, w której dwustronna lub wielostronna współpraca w poszczególnych dziedzinach mogłaby

³⁰ S. Kleszcz, M. Kloske, *Rosyjska strategia*, „Kwartalnik Bellona” 2010, nr 4, s. 47; А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 448–449.

³¹ Tamże.

³² Tamże, s. 32–33.

³³ Tamże, s. 33.

przekształcić się w koalicję wojskowo-polityczną w Eurazji, w tym także z udziałem krajów UE. Z kolei na Zachodzie analitycy krytykują politykę Putina i wskazują, że w związku z obecnymi działaniami Rosjan na arenie międzynarodowej jest możliwe tylko podjęcie „strategii siły”, co powinno zostać dokonane wspólnie przez USA i UE³⁴.

Indie i Chiny wobec Euroazjatyckiej Obrony Powietrzno-Kosmicznej

W rosyjskiej koncepcji połączona Eurazjatycka Obrona Powietrzno-Kosmiczna powinna stać się częścią szerszego porozumienia politycznego, analogicznego do Karty Helsińskiej OBWE z 1975 r., w którym byłoby zagwarantowane suwerenne prawo do zapewnienia bezpieczeństwa wojskowego terytoriów narodowych. Tym bardziej, że wiele krajów eurazjatyckich, przede wszystkim Indie i Chiny, szybko posuwają się w tym kierunku samodzielnie, a ich strategiczne dokumenty i działania na arenie międzynarodowej wyraźnie wskazują na to, że pragną być istotnymi, a może nawet najważniejszymi graczami na „eurazjatyckiej szachownicy”³⁵. Wzrastający potencjał Indii czy Chin jest bezdyskusyjny i na pewno będzie wywierał znaczny wpływ na układ sił w regionie.

Zgodnie z koncepcjami indyjskiej polityki zagranicznej po zimnej wojnie celem państwa stało się dążenie do osiągnięcia statusu mocarstwa w XXI wieku³⁶. Chodzi przede wszystkim o uznanie globalnych aspiracji Indii przez inne mocarstwa. Zdaniem hinduskich analityków, w świecie opartym na hierarchii Indie mają stać w jednym rzędzie z takimi mocarstwami, jak UE, USA, Chiny, Japonia i Rosja, jak również należeć wraz z nimi do światowych potęg. Co prawda Indie u progu XXI w. wybrały strategię bandwagoningu, czyli przyłączania się do silniejszego (w tym wypadku – do USA), to jednak nie jest to dowód, że chcą się podporządkować temu hegemonowi. Bardziej aspirują do roli równorzędnego gracza w stosunkach międzynarodowych, zwłaszcza że symbolami siły państwa są wciąż: broń nuklearna i armia. O statusie mocarstwa decyduje przecież głównie posiadanie dużego potencjału militarnego, m.in. dysponowanie bronią jądrową. W tym kontekście warto zwrócić uwagę, że Shakti – hinduska bogini siły – coraz częściej charakteryzuje indyjską percepcję

³⁴ Przykładem takiej retoryki są wypowiedzi Theresy May, premier Wielkiej Brytanii, która wskazywała na to, że Putin musi wybrać inną strategię od tej, która polegała na aneksji Krymu, wywołaniu konfliktu na Ukrainie oraz przeprowadzeniu cyberataków na europejskie rządy i parlamenty. Jednocześnie brytyjska premier nie odniosła się negatywnie do partnerstwa z Rosją, ale pod warunkiem przestrzegania przez ten kraj zasad obowiązujących w świecie demokratycznym. Zob. *May do Rosjan: Wiemy co robicie. Nie odniesiecie sukcesu*, TVN24 z 14 XI 2017 r., <https://www.tvn24.pl/wiadomosci-ze-swiatea,2/theresa-may-krytykuje-rosje-putina,789946.html> [dostęp: 3 I 2018]; *Die Welt: Reset z Rosją niemożliwy. Jedyną opcją strategia siły*, Defence24 z 27 XII 2017 r., <http://www.defence24.pl/719274,die-welt-reset-z-rosja-niemozliwy-jedyna-opcja-strategia-sily> [dostęp: 3 I 2018].

³⁵ А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 459–460.

³⁶ J. Zajączkowski, *Polityka zagraniczna Indii po zakończeniu zimnej wojny*, w: *Polityka zagraniczna. Aktorzy. Potencjały. Strategie*, T. Łoś-Nowak (red. nauk.), Warszawa 2011, s. 178.

porządku międzynarodowego³⁷. Ponadto trzeba nadmienić, że indyjska doktryna nuklearna opiera się na pojęciu minimalnego wiarygodnego odstraszenia oraz na zasadzie „*no first use*”, również w stosunku do państw, które dysponują bronią jądrową. Oznacza to, że sprawą zasadniczą pozostaje zdolność do przetrwania nieprzyjacielskiego ataku (odnosi się to zarówno do samych środków przenoszenia, jak i struktur dowodzenia) oraz przeprowadzenia efektywnego uderzenia odwetowego. Siła tego uderzenia powinna być na tyle znaczna, aby zniechęcić potencjalnego agresora do zastosowania własnych sił nuklearnych. W tym kontekście jest zrozumiałe, że wszystkie używane i rozwijane systemy balistyczne są systemami mobilnymi (kołowymi lub kolejowymi)³⁸. Warto też zaznaczyć, że zarys indyjskiej doktryny nuklearnej ujawniony w 1999 r. zawierał pojęcie *atomowa triada* (pociski z głowicami jądrowymi umieszczone na lądzie, okrętach podwodnych i na bombowcach).

Zgodnie z przyjętymi założeniami strategicznymi Indie zanotowały postęp w opracowaniu narodowego dwupoziomowego systemu OP, którego komponentami są antyrakiety AAD mające zdolność przechwytywania w strefie atmosfery ziemskiej rakiet balistycznych przenoszących głowice jądrowe. Indyjskie wojska raketowe dysponują aktualnie trzema typami rakiet balistycznych, a dwa kolejne są w trakcie doskonalenia. Obecnie, jak się ocenia, ich system OA jest zdolny do przechwytywania rakiet przeciwnika wystrzelonych z dystansu do 2000 km. Już w 2016 r. nowa indyjska rakietą była w stanie niszczyć rakiet balistyczne o zasięgu 5000 km. Dziesięć lat wcześniej rozpoczęto budowę pierwszego hinduskiego strategicznego nuklearnego okrętu podwodnego (tzw. boomera). Pojawiające się informacje mówią o budowie od trzech do pięciu boomerów; wydaje się jednak mało prawdopodobne, aby docelowym systemem dla nich miała być rakiet krótkiego zasięgu, w wysokim stopniu ograniczająca ich rolę strategiczną³⁹. Niewątpliwie na deskach kreślarskich znalazły się nowe modyfikacje indyjskich antyrakiet i zakończenie prac nad planem rozmieszczenia systemu OA. Sprawą otwartą pozostaje, czy w tych planach przewidziano współpracę z Amerykanami. Tym bardziej, że Hindusi w zasadzie nie odrzucają współdziałania z zagranicą w sferze budowy OA – udział w ich programie bierze Izrael, który udziela im pomocy przy budowie stacji radiolokacyjnej wczesnego ostrzeżenia o napadzie raketowym.

Chiny, ukierunkowane na zachowanie stabilności politycznej, zwracają uwagę przede wszystkim na ekspansję ekonomiczną. Przy czym trzeba pamiętać, że bez Państwa Środka współczesny świat nie mógłby funkcjonować – wpływ na to ma intensywny rozwój chińskiej gospodarki. Rozwiązywanie ważnych problemów globalnych następuje więc przez prowadzenie polityki pragmatycznej, co sprawia, że Chińczycy nie tracą żadnej okazji, aby rozszerzyć swoją obecność na rynkach zagranicznych,

³⁷ Tamże, s. 178–179.

³⁸ R. Ciastoń, *Indie vs. Pakistan – nuklearna rywalizacja*, portal geopolityka.org z 13 IX 2011 r., <http://www.psz.pl/116-bezpieczenstwo/indie-vs-pakistan-nuklearna-rywalizacja> [dostęp: 5 I 2018].

³⁹ *Indie testują nową antyrakiety*, Defence24 z 11 II 2017 r., <http://www.defence24.pl/545788,indie-testuja-nowa-antyrakiety> [dostęp: 3 I 2018].

także za pośrednictwem mniejszości chińskiej osiadłej w wielu państwach. Można zatem mówić nie tylko o ekspansjonizmie, lecz także o sinocentryzmie. Chiny bowiem przez swoją siłę dośrodkową stają się centrum przyciągającym i tworzą odrębną cywilizację, której atrakcyjność decyduje o skali oddziaływania⁴⁰. Ważnym aspektem narodowej strategii jest to, że w Chinach za najważniejsze zagrożenie bezpieczeństwa narodowego jest uznawana przewaga w dziedzinie informacyjno-komunikacyjnej. W zasadzie nie jest możliwa sytuacja, aby sieci socjalne były wykorzystywane do koordynowania działalności grup antyrządowych i demonstracji noszących charakter zdecydowanie wywrotowy, czego rezultatem jest zakaz funkcjonowania Facebooka i Twittera. Natomiast chińskie portale społecznościowe są pod kontrolą chińskiego rządu. Za tego typu działaniami kryją się dążenia do przeciwstawienia się dominacji amerykańskiej, zwłaszcza w zakresie wpływania na politykę informacyjną Chin i wykorzystywania zasobów chińskiego Internetu do stymulowania różnego rodzaju działalności dysydenckiej⁴¹. Przy czym nową rzeczywistością geopolityczną staje się formowanie dwóch ośrodków wojskowo-politycznych siły militarnej – Chin i USA – które w najbliższym dziesięcioleciu mogą ze sobą rywalizować, chociaż współpraca także nie jest wykluczona. Analitycy często wskazują na to, że powstanie chińskiego supermocarstwa mogłoby oznaczać powrót do dwubiegunowości, w której dwa ośrodki władzy: pierwszy – w Waszyngtonie, drugi – w Pekinie, mogłyby reprezentować odmienne wzorce globalizacji i systemów politycznych, co przypominałoby ład zimnowojenny⁴². Skala współpracy i rywalizacji są trudne do przewidzenia, ale istnieje zagrożenie, że te procesy mogą się odbywać kosztem innych krajów.

Jaką rolę mogłaby zyskać Rosja w nowym układzie sił? W ocenie komentatorów rosyjskich ewentualne hamowanie rozwoju OPK Rosji nieuchronnie doprowadzi do tego, że w USA w perspektywie średnioterminowej zostanie stworzony nie tylko potencjał do wykonania uderzenia obezwładniającego, lecz także zdolny do zneutralizowania ocalałych sił planowanych do wykorzystania w uderzeniu odwetowym. Takie działanie może doprowadzić do destabilizacji sytuacji na świecie i ponownie uczynić potencjał militarny globalnym instrumentem polityki zagranicznej USA i Sojuszu Północnoatlantyckiego⁴³. Z uwagi na to pojawia się postulat A. Podbieriezkina, aby Rosja i Europa zjednoczyły się w celu kontrolowania przestrzeni eurazjatyckiej⁴⁴. Warto też zauważyć, że w Chinach w ostatnich latach postrzega się Rosję jako główny podmiot stabilizujący w Eurazji, zdolny do osłabienia polityki amerykańskiej. W związku z tym strona chińska dąży do coraz ściślejszej współpracy z Rosjanami na płaszczyźnie militarnej, począwszy od wspólnych ćwiczebnych lotów taktycznych do kooperacji w zakresie obrony przeciwlotniczej i zadań logistycznych. Lejtmotywem tych

⁴⁰ C. Jean, *Geopolityka*, Wrocław–Warszawa–Kraków 2007, s. 320–321.

⁴¹ А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 373.

⁴² J. Marszałek-Kawa, *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy. Potencjały. Strategie...*, s. 123.

⁴³ А.И. Подберезкин, *Евразийская воздушно-космическая...*, s. 452.

⁴⁴ Tamże.

działań jest budowanie potencjału militarnego, który może odgrywać ważną rolę w skali globalnej. Niewątpliwie Pentagon spogląda na te działania z dużym zaniepokojeniem. W USA ukazują się wiele artykułów na ten temat, zwłaszcza dotyczących komponentu obrony przeciwrakietowej i współpracy sił powietrznych obydwu państw, która zmierza do budowy wspólnej obrony powietrznej w przestrzeni Eurazjatyckiej. Rozwój tego potencjału może bowiem zmniejszyć dotychczasowe, wyjątkowe zdolności USA do prowadzenia operacji powietrznych w rejonie Azji i Pacyfiku oraz na obszarze Europejskiego Teatru Działań Wojennych, co w znacznym stopniu wpływa na osłabienie amerykańskiej ekspansji i wskazuje na zmieniający się ład międzynarodowy⁴⁵.

Konkluzje

W drugim dziesięcioleciu XXI w. trwa dążenie do przekształcenia przestrzeni powietrznej, kosmicznej oraz informacyjnej w jedno pole walki, na którym nie będzie wyraźnych granic ani „pod względem wysokości”, ani „pod względem przestrzeni”, ani też „pod względem oddziaływania informacyjnego”. Jest to nowy globalny teatr działań bojowych, który staje się rozstrzygający i spycha na drugi plan tradycyjne przestrzenie stosowania potencjału militarnego – tj. przestrzeń lądową i morską. Rosjanie oczekują, że w perspektywie średnioterminowej w latach 2018–2020 dojdzie do zakończenia etapu przygotowawczego, podczas którego powstaną zasadniczo nowe systemy uzbrojenia oraz zostaną opracowane i przetestowane nowe koncepcje ich użycia. Wraz z dewaluacją idei „odstraszania jądrowego” i wzrostem sprzeczności między nowymi ośrodkami siły oznacza to, że kraje dysponujące znacznym potencjałem militarnym mogą przejść do aktywnej fazy jego użycia. W konsekwencji środki prowadzenia działań wojennych w takiej jednej przestrzeni powietrzno-kosmiczno-informacyjnej stają się rozstrzygające dla zwycięstwa. Tego typu integracja nieuchronnie spowoduje ujednoczenie zarządzania państwowego i dowodzenia wojskowego strategiczną bronią ofensywną (jądrową i konwencjonalną) oraz uzbrojeniem obronnym (strategiczną bronią ofensywną i OPK), a także środkami oddziaływania informacyjnego. Słuszne wydaje się postawienie hipotezy, że będzie to swoista „bitwa o Eurazję”, a rozwiązanie tego zadania stanie się wyzwaniem dla współpracy międzynarodowej, wspartej wysiłkami politycznymi. Rezultat ostateczny będzie zależał od potencjału wojskowo-technicznego, strategicznego uzbrojenia ofensywnego i obronnego oraz rozwoju przemysłu w zakresie produkcji jego komponentów⁴⁶.

Trzeba też podkreślić, że zdaniem Rosjan batalia o Eurazję może stanowić starcie z hegemonią amerykańską, co stawia pod znakiem zapytania rosyjskie umacnianie się na obrzeżach dawnego ZSRR i budowanie przeciwwagi dla USA. Warto zwrócić uwagę, że w najnowszej amerykańskiej Strategii Bezpieczeństwa Narodowego

⁴⁵ *Sky's the limit for joint Russian-Chinese Eurasian Air Defense Zone*, 1 VIII 2017, <https://sputniknews.com/military/201708011056086886-russian-chinese-common-airspace-defense/> [dostęp: 18 I 2018].

⁴⁶ Tamże, s. 78.

z 19 grudnia 2017 r. (National Security Strategy) wymienia się Chiny i Rosję jako państwa, które aktywnie wpływają na osłabienie bezpieczeństwa i znaczenia Stanów Zjednoczonych. Co więcej, te państwa dysponują potencjałami: propagandowym, asymetrycznym, konwencjonalnym i nuklearnym, które mogą posłużyć do rewizji istniejącego porządku międzynarodowego⁴⁷. Stanowi to niejako przyznanie się Amerykanów, że Chiny i Rosja są ich rywalami w skali globalnej. W tym kontekście „wojnę o Eurazję” można więc uznać za starcie zmierzające do panowania nad Heartlandem, czyli za zmagania o zdobycie rządów nad światem, które przywracają dwublokową rywalizację z okresu zimnej wojny. Po przeciwnych stronach stają USA (NATO) i Federacja Rosyjska, a niewiadomą pozostaje, jaką strategię działania przyjmą Indie i Chiny. Z dużym prawdopodobieństwem można przewidywać, że ład międzynarodowy ulegnie całkowitemu przemodelowaniu. Nie wiadomo, czy jednocześnie nie wzmocnią się tendencje o charakterze ekspansjonistycznym ze strony najważniejszych graczy na arenie międzynarodowej.

Bibliografia:

1. *Badania wschodnie. Polityka wewnętrzna i międzynarodowa*, W. Baluk, Z.J. Winnicki (red.), Wrocław 2008, Oficyna Wydawnicza Arboretum.
2. Blank S., *Threats to and from Russia: an Assessment*. „Journal of Slavic Military Studies” 2008, t. 21, nr 3.
3. Bryc A., *Rosja w XXI wieku. Gracz światowy czy koniec gry?* Warszawa 2008, Wydawnictwa Akademickie i Profesjonalne.
4. Cianciara A., *Klasyczne koncepcje geopolityczne*, w: *Geopolityka*, A. Dybczyński (red. nauk.), Warszawa 2013, Poltext.
5. Ciastoń R., *Indie vs. Pakistan – nuklearna rywalizacja*, 12 XI 2011, <http://www.psz.pl/116-bezpieczenstwo/indie-vs-pakistan-nuklearna-rywalizacja> [dostęp: 5 I 2018].
6. Depczyński M., *Rosyjskie siły zbrojne. Od Milutina do Putina*, Warszawa 2015, Bellona.
7. *Die Welt: Reset z Rosją niemożliwy. Jedyną opcją strategia siły*, 27 XII 2017, <http://www.defence24.pl/719274,die-welt-reset-z-rosja-niemozliwy-jedyna-opcja-strategia-sily> [dostęp: 3 I 2018].

⁴⁷ Amerykański dokument wymienia także Iran oraz Koreę Północną i oskarża te państwa o działalność destabilizującą państwa sąsiednie. Jednocześnie podkreśla, że KRLD w związku z zaawansowanym programem nuklearnym staje się zagrożeniem globalnym. Zob. M.A. Piotrowski, B. Wiśniewski, *Strategia bezpieczeństwa narodowego USA: podejście administracji Trumpa*, „Biuletyn PISM” z 21 XII 2017 r., <http://www.pism.pl/publikacje/biuletyn/nr-128-1570> [dostęp: 3 I 2018].

8. Firmanty Ł., *Szanghajska Organizacja Współpracy jako element polityki bezpieczeństwa Chińskiej Republiki Ludowej*, w: *Badania wschodnie. Polityka wewnętrzna i międzynarodowa*, W. Baluk, Z.J. Winnicki (red. nauk.), Wrocław 2008, Oficyna Wydawnicza Arboretum.
9. *Geopolityka*, A. Dybczyński (red. nauk.), Warszawa 2013, Poltext.
10. Gibas-Krzak D., *Świat w polityce zagranicznej Federacji Rosyjskiej*, „Kwartalnik Bellona” 2010, nr 4.
11. Haas M. de, *Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization*, „The Journal of Slavic Military Studies” 2017, t. 30, nr 1.
12. *Indie testują nową antyrakietę*, 11 II 2017, <http://www.defence24.pl/545788,indie-testuja-nowa-antyrakiete> [dostęp: 3 I 2018].
13. Jean C., *Geopolityka*, Wrocław–Warszawa–Kraków 2007, Zakład Narodowy im. Ossolińskich.
14. Kleszcz S., Kloske M., *Rosyjska strategia*, „Kwartalnik Bellona” 2010, nr 4.
15. Krzymowski A., *Plan Miedwiediewa – nowa architektura bezpieczeństwa?*, „Sprawy Międzynarodowe” 2009, nr 2.
16. Lach Z., Skrzyp J., *Geopolityka i geostrategia*, Warszawa 2007, Wydawnictwo AON.
17. Marszałek-Kawa J., *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy. Potencjały. Strategie*, T. Łoś-Nowak (red. nauk.), Warszawa 2011, Poltext.
18. Massaka I., *Eurazjatyzm. Z dziejów rosyjskiego misjonizmu*, Wrocław 2001, Funna.
19. *May do Rosjan: Wiemy co robicie. Nie odniesiecie sukcesu*, 14 XI 2017, <https://www.tvn24.pl/wiadomosci-ze-swiata,2/theresa-may-krytykuje-rosje-putina,789946.html> [dostęp: 3 I 2018].
20. Paradowski R., *Eurazjatyckie imperium Rosji. Studium idei*, Toruń 2001, Uniwersytet Mikołaja Kopernika.
21. Piotrowski M.A., Wiśniewski B., *Strategia bezpieczeństwa narodowego USA: podejście administracji Trumpa*, 21 XII 2017, „Biuletyn PISM” 2017, nr 128, <http://www.pism.pl/publikacje/biuletyn/nr-128-1570> [dostęp: 3 I 2018].
22. Potulski J., *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, Wydawnictwo Uniwersytetu Gdańskiego.

23. Putin V., *Speech and the Following Discussion at the Munich Conference on Security Policy*, 10 II 2007, <http://en.kremlin.ru/events/president/transcripts/24034> [dostęp: 3 I 2018].
24. Spykman N.J., *The Geography of the Peace*, New York 1944, Harcourt, Brace and Company.
25. Stuermer M., *Putin i odrodzenie Rosji*, Wrocław 2008, Wydawnictwo Dolnośląskie.
26. Symonides J., *Nowa doktryna morska Federacji Rosyjskiej*, „Kwartalnik Bellona” 2016, nr 1.
27. Zajączkowski J., *Polityka zagraniczna Indii po zakończeniu zimnej wojny*, w: *Polityka zagraniczna. Aktorzy. Potencjały. Strategie*, T. Łoś-Nowak (red. nauk.), Warszawa 2011, Poltext.

Literatura rosyjska:

1. Казанцев А.А., *Политика США в постсоветской Центральной Азии: характер и перспективы*, 5 II 2013, <http://ehd.mgimo.ru/IORManagerMgimo/file?id=E3DAB956-8956-310D-0D4C-2235B2392202> [dostęp: 3 I 2018].
2. Медведев Д., *Выступление на Конференции по вопросам мировой политики*, Evian, 8 X 2008, <http://kremlin.ru/events/president/transcripts/1659> [dostęp: 3 I 2018].
3. Подберезкин А.И., *Евразийская воздушно-космическая оборона*, Москва 2013, Издательство „МГИМО – Университет”.
4. Подберезкин А.И., *Современная военная политика России: учебно-методический комплекс*, t. 1 i 2, Москва 2017, Издательство „МГИМО – Университет”.

Abstrakt

Autorka artykułu omawia na tle uwarunkowań geopolitycznych Rosji najważniejsze tezy planu A. Podbieriezkina, które tworzą paradygmat wspólnego bezpieczeństwa w ujęciu rosyjskim na strategicznym obszarze Eurazji. Ma to szczególne znaczenie w obliczu wzrastających zagrożeń współczesnego świata. Szczególnie niebezpieczny charakter, w związku z przeprowadzaniem prób jądrowych i nieobliczalnym reżimem Kim Dzong Una, przybiera obecnie problem Korei Północnej, co rodzi zagrożenie, że nagły

konflikt może wciągnąć Półwysep w wojnę. To z kolei z pewnością doprowadziłoby do interwencji Stanów Zjednoczonych. Skutki ewentualnego konfliktu z udziałem supermocarstwa są nie do przewidzenia. Innym problemem pozostaje wciąż aktualny konflikt na linii Moskwa–Waszyngton i Moskwa–Unia Europejska. Rzeczywiście, rozszerzenie NATO na wschód przekształciło ten blok z regionalnego w globalny i włączyło w strefę jego odpowiedzialności całą Eurazję. Tymczasem Rosja, stojąca w opozycji do takiej strategii, próbuje budować przeciwwagę dla polityki amerykańskiej. Służą temu m.in. badania naukowców z MGIMO, w tym A. Podbieriezki, który jest jednym z wielu zwolenników prowadzenia bardziej aktywnej polityki opartej na ideach eurazjatyckich, z przewodnią rolą Rosji. Na szczycie OUBZ w Aszchabadzie poparcie uzyskała propozycja Rosji dotycząca zintegrowania jednostek rosyjskich i pododdziałów utworzonych w 2011 r. Wojsk Obrony Powietrzno-Kosmicznej (obecnie: Siły Powietrzno-Kosmiczne Federacji Rosyjskiej). W ten sposób zainicjowano powołanie do życia Eurazjatyckiej Obrony Powietrzno-Kosmicznej. Formowanie kilku ośrodków siły militarnej w Eurazji, połączone z rosnącym znaczeniem Indii i Chin oraz ich możliwościami ekonomicznymi i militarnymi, jest skierowane na uzyskanie potencjałów strategicznego uzbrojenia ofensywnego, a przede wszystkim – powietrzno-kosmicznego komponentu precyzyjnego rażenia o różnym przeznaczeniu. Na lata 2018–2020 Rosjanie przewidują zakończenie etapu przygotowawczego, podczas którego powstaną zasadniczo nowe systemy uzbrojenia oraz zostaną opracowane i przetestowane nowe koncepcje ich użycia. W artykule podkreślono, że będzie to swoista „bitwa o Eurazję”, która stanie się wyzwaniem dla współpracy międzynarodowej, wspartej wysiłkami politycznymi. Rezultat ostateczny będzie zależał od potencjału wojskowo-technicznego strategicznego uzbrojenia ofensywnego i obronnego oraz rozwoju przemysłu w zakresie produkcji jego komponentów.

Słowa kluczowe: Eurazja, Rosja, Chiny, Indie, USA, Obrona Powietrzno-Kosmiczna, Doktryna Putina, postzimnowojenna rywalizacja, zmiana ładu międzynarodowego, geopolityka.

II

STUDIA I ANALIZY

Anna Łasińska

Wybrane techniki obrazowania stosowane w kryminalistyce

Kryminalistyka to szeroka, wielodyscyplinarna nauka wykorzystująca różne techniki i metody badań uznawane i rozwijane od dawna w naukach przyrodniczych. Przez wiele tysięcy człowiek gromadził wiedzę o obiektach ożywionych na podstawie tego, co mógł zobaczyć gołym okiem. Dopiero na przełomie wieków XVI i XVII pojawiły się pierwsze mikroskopy. Za twórców mikroskopu uważa się Holendrów, Hansa i Zachariasza Janssensów, którzy pierwsze konstrukcje wykonali ok. 1590 r. Ze względu na słabe powiększenie (ok. 10 razy) mikroskopy nie zdobyły wtedy uznania jako narzędzia badawcze. Przełomu dokonał wynalazca i przedsiębiorca Antonie van Leeuwenhoek, który w XVII w. udoskonał konstrukcję mikroskopu, a następnie rozwinął produkcję tych urządzeń. A. Leeuwenhoek jako pierwszy obserwował żywe komórki – plemniki, pierwotniaki, erytrocyty itp. Odkrycie przez Wilhelma Roentgena tzw. promieni X przyczyniło się m.in. do rozwoju metod obrazowania pozwalających na nieinwazyjne badanie wnętrza żywych organizmów.

Postęp technologii obserwowany we współczesnym świecie pociąga za sobą zmiany we wszystkich dziedzinach życia, usprawnia je, przyspiesza ich rozwój oraz otwiera na nowe możliwości badawcze. Współczesna kryminalistyka adaptuje na swoje potrzeby nowe metody badawcze, technologie i urządzenia w celu optymalizowania uzyskiwanych wyników i dostarczania ich wymiarowi sprawiedliwości w jak najpełniejszej i najpewniejszej formie. Zadaniem ekspertów pracujących w laboratoriach kryminalistycznych jest dostarczanie dogłębnej informacji na temat zabezpieczonego materiału dzięki stosowaniu zarówno niszczących, jak i nieniszczących rodzajów badań. W chemii sądowej istotne są badania śladowych ilości różnorodnych substancji chemicznych tworzących ślad na miejscu przestępstwa i stanowiących materiał dowodowy. Mikroślad jako dowód materialny w sprawie sądowej nie powinien ulec zniszczeniu bądź zużyciu podczas przeprowadzania badań. Stawia to wysokie wymagania biegłym oraz w badaniach wykorzystywanym przez nich technikom. W badaniach strukturalnych oraz właściwości fizycznych i chemicznych mikrośladów stosuje się wiele różnorodnych metod i technik obrazowania. Głównym celem tych metod – niezależnie od zastosowanego rozwiązania technicznego i narzędzia (od najprostszego szkła powiększającego do zaawansowanych mikroskopów elektronowych) jest uzyskanie powiększonego obrazu niewielkich obiektów.

Obecnie na świecie używa się wielu rodzajów mikroskopów oraz sprzężonych z nimi innych urządzeń wielozadaniowych w celu uzyskania informacji dotyczących kształtu analizowanych próbek i obiektów, ich rozmiarów, składu chemicznego, struktury krystalicznej, właściwości mechanicznych, elektrycznych bądź magnetycznych. Najczęściej stosuje się techniki mikroskopii optycznej i elektronowej, techniki

spektrometryczne, m.in. podczerwieni i Ramana, oraz techniki wykorzystujące promieniowanie rentgenowskie.

W artykule zostaną zaprezentowane niektóre techniki obrazowania, takie jak mikroskopia konfokalna¹, elektronowa i sił atomowych oraz spektrometria mikro-Ramana, które mają zastosowanie w wielu dziedzinach kryminalistyki. W tabeli 1 porównano podstawowe właściwości mikroskopów: optycznego (światłnego), skaninowego elektronowego (ang. *scanning electron microscope*, SEM) oraz mikroskopu sił atomowych (ang. *atomic force microscope*, AFM).

Tab. 1. Podstawowe właściwości mikroskopów: optycznego, elektronowego i sił atomowych².

| Cecha mikroskopu | Mikroskop optyczny | SEM | AFM |
|----------------------------------|--|----------------------|---------------------------|
| Rozdzielczość względem osi x,y | 1000 nm | 5 nm | 0,1 nm |
| Rozdzielczość względem osi z | – | – | 0,01 nm |
| Powiększenie | do 2000 | do 10^6 | do 10^8 |
| Głębka ostrości | średnia | duża | mała |
| Środowisko prowadzenia badań | powietrze, ciecz, próżnia | próżnia | powietrze, ciecz, próżnia |
| Rodzaj ograniczenia | dyfrakcja światła (CLSM – mikroskop konfokalny – dyfrakcja lasera) | dyfrakcja elektronów | rozmiar igły |

Niezależnie od typu narzędzia zastosowanego do obrazowania jednym z jego istotnych parametrów jest tzw. zdolność rozdzielcza, czyli najmniejsza odległość między dwoma punktami, które na uzyskanym obrazie mogą być uznawane jako odrębne. Przyczyną ograniczonej zdolności rozdzielczej **mikroskopu optycznego** jest dyfrakcja światła, która powoduje, że obrazy szczegółów sąsiadujących ze sobą na próbce stają się nierozróżnialne, gdy odległość między nimi była bliska długości fali świetlnej. Idea budowy mikroskopu optycznego stała się podstawą **mikroskopii**

¹ Odmiana mikroskopii świetlnej charakteryzująca się powiększonym kontrastem i rozdzielczością. Używana do uzyskania wysokiej jakości obrazów oraz rekonstrukcji obrazów w trzech wymiarach, za: https://pl.wikipedia.org/wiki/Mikroskopia_konfokalna [dostęp: 29 XII 2017] (przyj. red.).

² Wszystkie tabele i materiały ilustracyjne zostały opracowane przez autorkę tekstu (przyj. red.).

elektronowej, w której wiązka światła została zastąpiona wiązką elektronową zapewniającą uzyskanie obrazu o parametrach (powiększenie, rozdzielczość) niedostępnych dla klasycznej mikroskopii świetlnej. Techniki mikroskopii elektronowej umożliwiają uzyskanie obrazów z rozdzielczością rzędu 0,1–0,05 nm, czyli ponad 4000 razy lepszą niż typowy mikroskop optyczny. Jest to jednocześnie zdolność rozdzielcza około 4 000 000 razy lepsza niż zdolność, jaką ma ludzkie oko. Mikroskopia optyczna ma wiele zalet, cech i funkcjonalności niedostępnych dla innych typów mikroskopii. Ostatnie rozwiązania koncepcyjne i techniczne wykorzystywane w konfokalnej skaningowej mikroskopii optycznej rozszerzają możliwości tej metody.

Mikroskop optyczny jest niezbędnym narzędziem w laboratoriach biologicznych, medycznych i kryminalistycznych. Z powodu swojej prostej budowy i niewysokiej ceny jest on nadal mikroskopem używanym najczęściej. Budowa standardowego mikroskopu optycznego pozostaje niezmienna od ponad wieku. Klasyczny mikroskop świetlny jest zbudowany z dwóch soczewek: obiektywu i okularu, których łączne powiększenia dają końcowe powiększenie obrazu.

W badaniach jakości materiałów nieodzowne są **mikroskopy stereoskopowe** (zdj. 1). Są to mikroskopy optyczne umożliwiające przestrzenne widzenie obserwowanego obiektu.

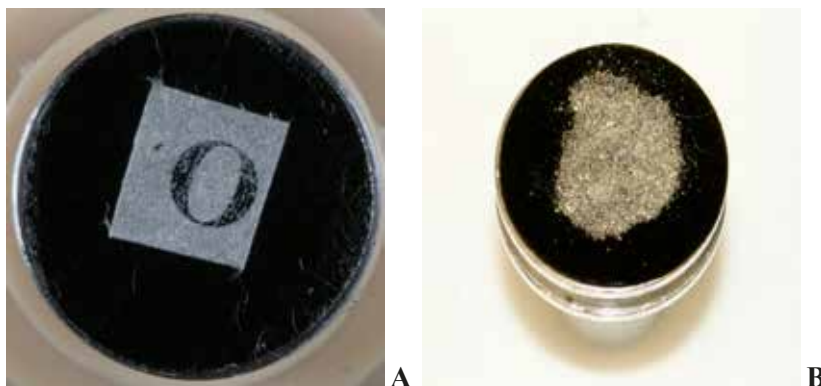


Zdj. 1. Mikroskop stereoskopowy zintegrowany z mikroskopową kamerą cyfrową i ciekłokrystalicznym ekranem.

Światło biegnące w torach optycznych mikroskopu stereoskopowego oddzielnie dla każdego oka wytwarza obraz postrzegany przez umysł człowieka jako

trójwymiarowy. Tego rodzaju mikroskopy charakteryzują się niewielkim, powyżej 300-krotnym powiększeniem. Obserwacja odbywa się w świetle przechodzącym lub odbitym.

Mikroskopy stereoskopowe są zalecane do prac związanych z badaniem pisma ręcznego, archeologią, gemmologią, botaniką, badaniami jakości elektronicznych płytek drukowanych, badaniami jakościowymi próbek do analizy SEM/EDX, do obserwacji struktur krystalicznych na poziomie mikrometrycznym, wstępnych oględzin materiału dowodowego (zdj. 2) oraz wszelkich prac precyzyjnych.



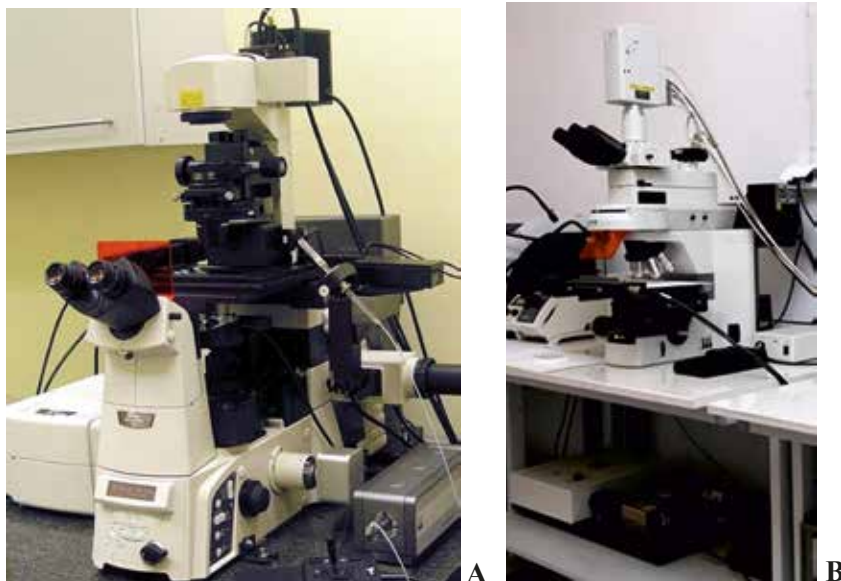
Zdj. 2. Stoliki do mikroskopu SEM z próbkami wydruku na papierze (A) i mieszaniny pirotechnicznej (B) widziane w mikroskopie stereoskopowym³.

Jednym z istotnych ograniczeń klasycznej mikroskopii optycznej jest światło pochodzące spoza płaszczyzny ogniskowania. Obiektyw mikroskopu zbiera obrazy nie tylko z płaszczyzny ogniskowania, lecz także z całego przekroju próbki. Obrazy obiektów leżących w płaszczyźnie ogniskowania jest ostry i wyraźny. Obrazy obiektów leżących przed i za tą płaszczyzną są nieostre (rozmyte) i to tym bardziej, im dalej leżą od tej płaszczyzny. W rezultacie obraz obiektu widoczny w klasycznym mikroskopie charakteryzuje się wysokim tłem zmniejszającym ostrość konturów.

Najdoskonalszym typem mikroskopu świetlnego pod względem optycznym jest **mikroskop konfokalny**. Jego wynalazca, Marvin Minsky, twierdził, że idealny mikroskop świetlny powinien odcinać światło nie pochodzące z płaszczyzny ostrości obiektywu oraz skanować punkt po punkcie badany preparat. W dzisiejszych czasach parametry laserowo skanującego mikroskopu konfokalnego (ang. *Laser Scanning Confocal Microscope*, LSCM) zbliżyły się do teoretycznych granic powiększenia i rozdzielczości obrazu, które obowiązują dla mikroskopii świetlnej od XIX w. (ich autorem jest niemiecki fizyk Ernst Abbe). Mikroskop

³ A. Łasińska, K. Barszcz, *Ilościowa i jakościowa analiza mieszanin pirotechnicznych SEM/EDS*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, nr 11, s. 181.

konfokalny (zdj. 3) jest zbudowany na bazie mikroskopu fluorescencyjnego⁴, przy czym źródłem światła jest laser lub kilka laserów, które zapewniają skupioną wiązkę światła o dużej intensywności.



Zdj. 3. Odwrócony mikroskop konfokalny Nikon TiE Eclipse A1 z mikroselectorem oraz mikrodysekcją laserową (A) oraz mikroskop optyczny Nikon Eclipse 80i z wyposażeniem konfokalnym C1 (B).

Wiązka światła jest ogniskowana na oglądanym obiekcie. Założeniem mikroskopii konfokalnej jest wyeliminowanie obrazów pochodzących spoza płaszczyzny ogniskowania. Światło jest skupiane w jednym punkcie preparatu na określonej głębokości. Fluorescencja jest wzbudzana w punkcie ogniskowania, ale także powyżej i poniżej płaszczyzny tego punktu. Dzięki konfokalnej przysłonie otworowej (pinholi), sprzężonej wielkością i położeniem z przysłoną otworową toru oświetlenia, w detektorze jest rejestrowany tylko obraz punktu z płaszczyzny ogniskowej preparatu. Głębokość wzbudzenia fluorescencji promieniem lasera i odbierania światła emitowanego wynosi ok. 50 μm . W mikroskopach konfokalnych dwufotonowych zakres jest poszerzony do 400–500 μm . Automatyczne powtórzenie skanowania i kolejnych przesunięć wzdłuż

⁴ Mikroskopia fluorescencyjna – rodzaj mikroskopii świetlnej, która jest wykorzystywana do badania próbek fluoryzujących (absorbujących jedną długość światła i emitujących inną). Światło o jednej długości fali jest używane do wzbudzania cząsteczek fluorescencyjnych, a światło o innej długości fali, które jest emitowane przez cząsteczki, jest gromadzone i używane do wytworzenia obrazu. W przypadkach, gdy obiekty, np. części komórki lub tkanki, które mają być obserwowane, nie wykazują fluorescencji, muszą być znakowane przed obserwacją barwnikiem fluorescencyjnym lub znacznikiem.

osi współrzędnej z umożliwia zebranie stosu obrazów (tzw. skrawków optycznych) z kolejnych warstw preparatu. Uzyskany obraz warstwowy charakteryzuje się słabszym tłem i ostrzejszymi konturami. Ta metoda pozwala uzyskać większe powiększenie oglądanych materiałów i ułatwia ich interpretację. Dzięki zestawowi obrazów warstwowych można odtworzyć trójwymiarowy obraz obiektu wraz z jego budową wewnętrzną. W mikroskopach konfokalnych najczęściej wykorzystuje się lasery: argonowy, argonowo-kryptonowy, helowo-neonowy, półprzewodnikowe (diodowe), na ciele stałym (femto-, nano-, pikosekundowe – tytan-szafir). Zależnie od typu lasera linie spektralne⁵ emitowanego światła są różne. Na przykład laser Ar, który jest rodzajem jonowego lasera gazowego, emituje światło w zakresie widzialnym i UV o różnych długościach fal (351, 454, 528 nm).

We współczesnych mikroskopach konfokalnych stosuje się dwa odmienne rozwiązania konstrukcyjne. W obydwu otrzymuje się obraz przekroju obiektu na określonej głębokości, jednak te obrazy są otrzymywane w odmienny sposób.

W skanującym laserowo mikroskopie konfokalnym skupiona wiązka światła laserowego przemieszcza się skokowo po obiekcie. Na swojej drodze wzbudza do emisji cząsteczki fluorochromów. Aby uzyskać możliwie silne skupienie wiązki w płaszczyźnie ogniskowania, na drodze optycznej jest umieszczona pinhola. Wiązka po przejściu przez pinholę trafia na lustro dichromatyczne. Odbija ono światło wiązki wzbudzającej, a przepuszcza światło emitowane przez fluorochrom (o większej długości fali). Wiązka wzbudzająca przechodzi następnie przez obiekt, który ostatecznie skupia ją w postaci mikroskopijnej plamki na płaszczyźnie ogniskowania. Światło emitowane przez cząsteczki fluorochromu przechodzi przez obiekt, lustro dichromatyczne (bez odbicia) i trafia na drugą przesłonę z otworkiem. Promienie, które pochodzą z płaszczyzny ogniskowania, przechodzą także przez otworek i trafiają do detektora, pozostałe są zatrzymywane na przesłonie. Zmiana położenia lustra dichromatycznego pozwala na zmianę położenia punktu skupienia wiązki na płaszczyźnie ogniskowania. Położenie lustra jest kontrolowane przez system komputerowy zapisujący jednocześnie położenie plamki świetlnej i natężenie światła, które są rejestrowane przez detektor. Systematyczne przemiatanie (skanowanie) płaszczyzny ogniskowania pozwala uzyskać informację o analizowanym obiekcie.

W dwufotonowych mikroskopach konfokalnych (ang. *Two-photon Confocal Microscope*, TPCM) do wzbudzenia fluorochromu stosuje się promieniowanie z zakresu bliskiej podczerwieni o energii kwantu równej połowie energii wzbudzenia. W takich warunkach wzbudzenie cząsteczki fluorochromu nastąpi tylko wtedy, gdy cząsteczka zaabsorbuje prawie jednocześnie dwa kwanty promieniowania. W praktyce takie zjawisko zachodzi tylko w miejscu silnego zogniskowania wiązki. Dlatego w mikroskopach dwufotonowych nie jest potrzebna pinhola przed detektorem, gdyż emitowane światło pochodzi wyłącznie z płaszczyzny ogniskowania. Laser wytwarza

⁵ Linia spektralna – ciemna lub jasna linia w jednolitym, ciągłym widmie, powstająca wskutek nadmiaru lub deficytu fotonów (w porównaniu z pobliskimi częstotliwościami) w wąskim zakresie częstotliwości.

krótkie impulsy promieniowania o dużej gęstości fotonów (dziesiątki kilowatów w maksimum impulsu), jednak o niskiej energii impulsu (nanodżul na impuls). Zasada skanowania obiektu jest w tej konstrukcji analogiczna do działania mikroskopu ze skanowaniem laserowym. Mikroskopy dwu- lub wielofotonowe mają wiele zalet wynikających ze stosowania wiązki wzbudzenia z zakresu bliskiej podczerwieni, do których należy zaliczyć m.in.:

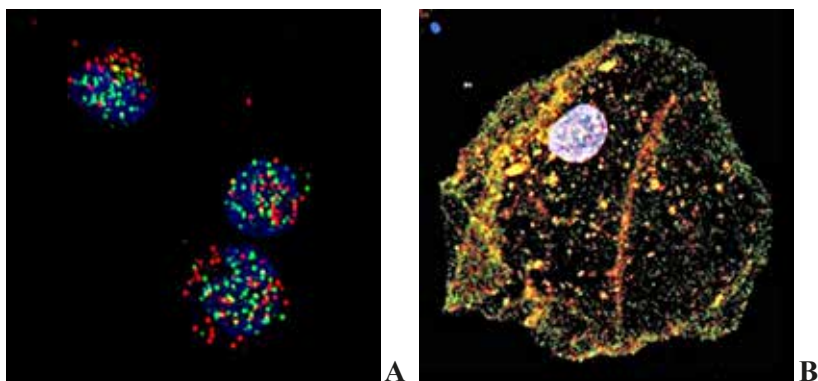
- niską energię niesioną przez wiązkę, która powoduje znacznie mniejsze uszkodzenie fotochemiczne i termiczne obiektu,
- lepszą penetrację preparatów biologicznych niż przy stosowaniu krótkofalowego światła widzialnego lub promieniowania UV. Umożliwia to pracę z obiektami o większej grubości,
- większą czułość niż LSCM, co pozwala pracować z niższymi stężeniami fluorochromów.

Dane o analizowanym obiekcie są zbierane w formie intensywności świecenia punktu i ze swej natury są monochromatyczne. Po zebraniu kompletu danych obraz jest przetwarzany w format typowy dla zdjęć cyfrowych. Może być wówczas łatwo kolorowany. Jeżeli obiekt jest barwiony więcej niż jednym fluorochromem, to muszą się one różnić długością fali światła wzbudzającego. Dla każdej długości fali są zbierane niezależne dane o obiekcie. Emisji pochodzącej od poszczególnych fluorochromów przypisuje się zwykle kontrastowe barwy. Te dane kompiluje się w jeden obraz na etapie tworzenia zdjęcia cyfrowego. Obecnie w handlu są dostępne mikroskopy konfokalne pozwalające na wzbudzenie światła przy trzech lub więcej zakresach fal. Wraz z rozwojem oferty dostępnych fluorochromów i wzrostem ich specyficzności mikroskopia konfokalna staje się coraz bardziej dostępną techniką badawczą dostarczającą ogromnych ilości szczegółowych informacji. Możliwe jest uzyskanie pojedynczego skanu w czasie mniejszym niż 0,05 s. Pozwala to rejestrować przebieg szybko zmieniających się procesów zachodzących w żywej komórce lub tkance i obserwować je potem w formie filmu wideo.

Przewagą mikroskopii konfokalnej, która nie występuje w innych rozwiązaniach technicznych, jest możliwość uzyskania serii przekrojów badanego obiektu na różnych głębokościach. Taka seria przekrojów może być wykorzystana do odtworzenia przestrzennej struktury obiektu.

Technika mikroskopii konfokalnej znalazła szerokie zastosowanie w naukach biologicznych, medycynie, inżynierii genetycznej⁶, a także w kryminalistyce. W medycynie sądowej pozwala wykryć i zobrazować zmiany patologiczne w przypadku nagłej śmierci, rozróżnić rany wejściowe i wyjściowe po pocisku, określić odległość strzału, a także zmiany skórne i urazy powstałe po eksplozji materiałów wybuchowych. Daje też możliwość bezpośredniego trójwymiarowego obrazowania mikroskopowego pojedynczych komórek ludzkich lub kawałków tkanek (zdj. 4).

⁶ A. Raczkowska i in., *Pleiotropic effects of a Yersini enterocolitica ompR mutation on adherent-invasive abilities and biofilm formation*, „FEMS Microbiology Letters” 2011, nr 321, s. 43–49.



Zdj. 4. Obraz 3D komórek ludzkich: limfocytów (A) oraz HeLa (B) wykonany za pomocą odwróconego laserowego mikroskopu konfokalnego Nikon TiE Eclipse A1.

Już w XIX w. zauważono, że część barwników ma zdolność oddziaływania na niektóre składniki komórek: białka, lipidy, kwasy nukleinowe itp. Z biegiem czasu opracowano standardowe procedury wybarwiania preparatów pozwalające na uwidocznienie elementów kluczowych dla komórki. Na zdj. 4 pokazano mikrofotografię komórek ludzkich wybarwionych mieszaniną trzech barwników. Dzięki takiej kombinacji barwników widać jednocześnie błony komórkowe i jądra komórek. Również niektóre barwniki fluorescencyjne mają zdolność wybiórczego wiązania się z elementami komórki. Zastosowanie barwników fluorescencyjnych ma wiele zalet i pozwala m.in. na:

- obserwację emisji światła na ciemnym tle, co zwiększa czułość metody i poprawia kontrast obserwowanych szczegółów. Ten wzrost czułości jest na tyle istotny, że we wszystkich technikach wybiórczego wybarwiania konkretnych makrocząsteczek stosuje się w zasadzie barwniki fluorescencyjne, a nie klasyczne barwniki absorpcyjne,
- zróżnicowanie komórek lub ich fragmentów ze względu na panujące w nich warunki, do czego wykorzystuje się siłę i barwę fluorescencji zależną od warunków panujących w środowisku, czyli: pH, potencjału redox, lipofilowości, potencjału błonowego. Na zdj. 4 pokazano jądra komórkowe wybarwione barwnikiem DAPI. Ten związek fluoryzuje na niebiesko po interkalacji⁷ do DNA;
- wykrycie różnic w stężeniu niektórych jonów, np. Ca^{2+} , od czego zależy siła i barwa fluorescencji.

Zaawansowane systemy mikrodysekcji laserowej są obecnie wyposażone w moduły laserowe emitujące promieniowanie UV lub IR, zintegrowane z mikroskopem

⁷ *I n t e r k a l a c j a* – zjawisko wiązania niewielkich cząsteczek wewnątrz cząsteczek związków wielkocząsteczkowych lub wewnątrz struktur ponadcząsteczkowych zbudowanych z cząsteczek związanych ze sobą np. wiązaniami wodorowymi czy oddziaływaniami van der Waalsa, za: [https://pl.wikipedia.org/wiki/Interkalacja_\(chemia\)](https://pl.wikipedia.org/wiki/Interkalacja_(chemia)) [dostęp: 29 XII 2017] (przyp. red.).

fluorescencyjnym lub konfokalnym wysokiej klasy oraz zmotoryzowanym stolikiem. Całość jest uzupełniona systemem komputerowym pozwalającym na sterowanie procesem wycinania komórek za pomocą oprogramowania, kamery i monitora komputera.

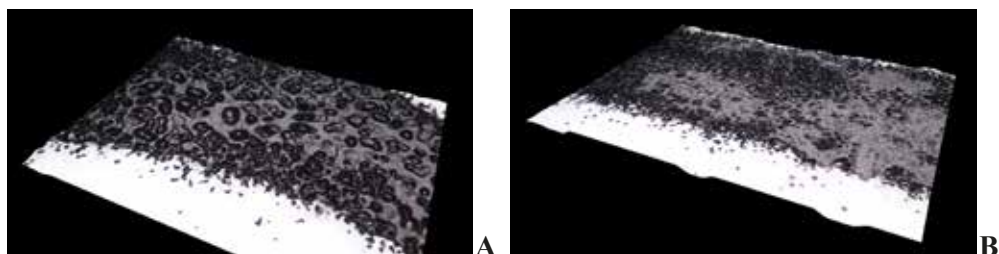
Systemy mikrodysekcji, opracowane pierwotnie z myślą o wykorzystaniu w dziedzinie onkologii, szybko znalazły zastosowanie także w innych dziedzinach nauk biologicznych, w tym na potrzeby kryminalistyki. Mikroskopia konfokalna w połączeniu z mikrodysekcją laserową stworzyły nowe możliwości profilowania genetycznego śladów biologicznych, tradycyjnie zabezpieczanych na pałeczkach wymazowych oraz na taśmach kryminalistycznych⁸. Pojedyncze komórki lub fragmenty tkanek są odseparowywane od reszty preparatu wraz z fragmentem membrany na skutek zjawiska zimnej ablacji (pod wpływem wiązki promieniowania laserowego). Moduł mikrodysekcji laserowej stanowi pulsacyjny, pikosekundowy laser na ciele stałym o mocy 4 mW, emitujący promieniowanie w zakresie widma UV (o długość fali 355 nm). Obrazowanie i kwalifikacja fragmentów preparatu poddawanych mikrodysekcji odbywa się w świetle przechodzącym z wykorzystaniem wysokoczułej wewnętrznej kamery cyfrowej. Mikrodysekcja jest prowadzona przy zmiennych parametrach mocy oraz ogniskowej wiązki promieniowania laserowego.

Obecnie inną najnowszą metodą analizy i izolacji komórek jest mikroselekcja. System jest kontrolowany oraz sterowany komputerowo za pomocą dedykowanego oprogramowania. Rozpoczęcie procesu izolacji wymaga przeprowadzenia uprzednio odpowiedniej kalibracji systemu, która pozwala na uzyskanie wysokiej precyzji pozyskiwania i osadzania wyselekcjonowanych komórek. Izolowanie pojedynczych komórek odbywa się w trzech etapach: identyfikacji, pozyskiwania i osadzania. Podobnie jak w systemie z mikrodysekcją laserową, obrazowanie i kwalifikacja fragmentów preparatu odbywa się w świetle przechodzącym, z wykorzystaniem wysokoczułej wewnętrznej kamery cyfrowej.

Technika laserowej mikroskopii konfokalnej jest wykorzystywana m.in. do identyfikacji dokumentów sporządzonych na podłożu papierowym⁹, a także do określania jednorodności wykonania dokumentu przez ujawnienie, czy tekst został dopisany do już istniejącego (zdj. 5).

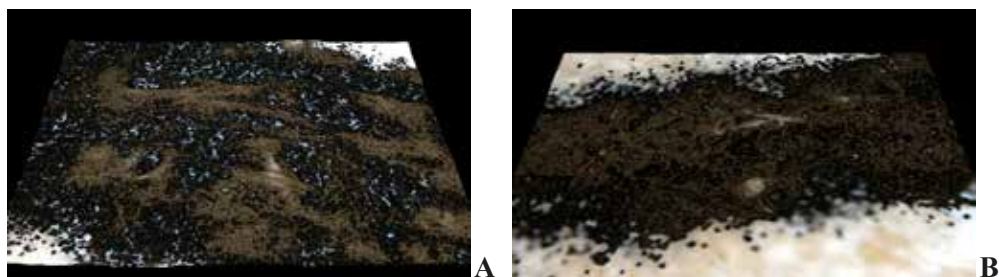
⁸ A. Łasińska i in., *Ocena przydatności folii adhezyjnych do zabezpieczania śladów biologicznych oraz izolacji komórek ludzkich metodą mikrodysekcji laserowej*, „Problemy kryminalistyki” 2014, nr 283, s. 18–28.

⁹ S. Szczepańczyk, U. Konarowska, *Zastosowanie mikroskopii optycznej w weryfikacji dokumentów przerobionych za pomocą drukarki laserowej*, „Problemy Kryminalistyki” 2012, nr 276, s. 65–73; A. Łasińska, *Badania mikrośladów*, w: *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, B. Hołyst (red. nauk.) Warszawa 2014, s. 804–840; A. Łasińska, U. Konarowska, *Zastosowanie mikroskopii optycznej i elektronowej w badaniach autentyczności dokumentów*, w: *Dokumenty a prawo prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, s. 105–112.



Zdj. 5. Obraz 3D powierzchni tonera widoczny na wydruku z drukarki laserowej: dokument przeszedł przez urządzenie dwukrotnie (A), dokument przeszedł przez urządzenie jednokrotnie (B). Zdjęcia wykonane w powiększeniu 200 razy za pomocą mikroskopu Nikon 80i.

W celu ustalenia cech charakterystycznych budowy tonera widocznych na wydrukach wykorzystano mikroskop optyczny Nikon Eclipse 80i z wyposażeniem konfokalnym C1 (zdj. 5 B). Fragmenty wydruków stron testowych poddawano obserwacji w świetle przechodzącym z zastosowaniem kolorowej kamery CCD Nikon DS5NC z chłodzeniem, o rozdzielczości 2560 x 1980 oraz obiektywu LU Plan Fluor 200x, N.A. 0,90, WD 1.0. Konstrukcja mikroskopu pozwala na wykonywanie badań metodą nieniszczącą dokumentów o formacie A4. Z obserwacji mikroskopowych wynika, że powierzchnia tonera naniesionego przez urządzenie na papier jest silnie rozbudowana (zdj. 6). Dla każdego wydruku tworzy swoisty indywidualny układ struktur. Widoczne są dwa rodzaje charakterystycznych obszarów, tj. powierzchnia lita, bardziej płaska, oraz ziarnista, tworząca mniejsze lub większe skupiska o różnym zagęszczeniu.



Zdj. 6. Obraz 3D tonera na wydrukach uzyskanych z kolorowej drukarki laserowej C734/C736w (A) oraz z monochromatycznej drukarki laserowej T650n/T652/T654n (B). Zdjęcia wykonane w powiększeniu 200 razy za pomocą mikroskopu Nikon 80i.

Dobłą metodą obrazowania może być również **spektroskopia Ramana**. Podobnie jak spektroskopia absorpcyjna w podczerwieni należy ona do technik badania widm oscylacyjnych materiałów. Może być stosowana zarówno do gazów, cieczy, jak

i ciał stałych. W większości spektrometrów ramanowskich jako źródła wzbudzenia używa się laserów. Ta technika jest komplementarna do spektroskopii w podczerwieni. W praktyce najczęściej rejestruje się widma z maksimum stokesowskimi¹⁰, które mają większe natężenia niż antystokesowskie¹¹, ponieważ liczba molekuł w pierwszym oscylacyjnym stanie wzbudzonym jest mniejsza niż w stanie podstawowym. Ze wzrostem temperatury wzrasta liczba molekuł w pierwszym stanie wzbudzonym, wzrasta zatem natężenie linii antystokesowskich. Całkowite widmo ramanowskie składa się z: maksimum rozpraszania Rayleigha¹² (duże natężenie, długość fali taka sama jak długość fali wzbudzającej), maksimum stokesowskich (niższe częstotliwości, większe długości fali) oraz maksimum antystokesowskich (wyższe częstotliwości, mniejsze długości fali). Przesunięcia ramanowskie w widmach Ramana są identyczne co do wartości z położeniem pików absorpcyjnych w widmach w podczerwieni, różnią się jednak ich względne natężenia. Niektóre maksima mogą być widoczne w jednym widmie, w drugim zaś nie. Rozpraszanie Ramana jest związane ze zniekształceniem rozkładu gęstości elektronów wokół wiązania, po którym następuje reemisja promieniowania połączona z powrotem wiązania do pierwotnego kształtu. Molekuły homojądrowe, nieaktywne w podczerwieni, dają linie ramanowskie, ponieważ polaryzowalność wiązań (czyli siła wiązania elektronów w molekułe) zmienia się periodycznie i zgodnie w fazie z drganiami rozciągającymi. Warunkiem pojawienia się pasma ramanowskiego w widmie jest zmiana polaryzowalności w czasie normalnego drgania.

W czasie drgania powodującego periodyczne zmiany struktury szkieletu zębów atomowych może zmieniać się periodycznie również polaryzowalność. To zróżnicowanie reguły wyboru widma w podczerwieni i Ramana powoduje, że niektóre drgania nieaktywne w podczerwieni mogą być aktywne w widmie Ramana i na odwrót. Na przykład drganie dwuatomowej molekuly homonuklearnej (m.in. O_2 , N_2) jest w podczerwieni nieaktywne, natomiast pojawia się w widmie Ramana, ponieważ w tym drganiu zmienia się polaryzowalność. W przypadku molekuł $NaCl$, KCl nie obserwujemy widm Ramana nawet w fazie gazowej, gdzie nie są one zdysocjowane. Dzieje się tak dlatego, że są to molekuły jonowe, ich elektrony walencyjne należą do odpowiednich zębów atomowych i w czasie drgania poruszają się ze swymi zębami atomowymi.

¹⁰ Pasma stokesowskie – powstają, gdy cząsteczka po oddziaływaniu z promieniowaniem przenosi się na wyższy poziom oscylacyjny i rozproszony foton ma energię mniejszą o różnicę energii poziomów oscylacyjnych $h\nu$.

¹¹ Pasma antystokesowskie – jeśli molekula przed oddziaływaniem z promieniowaniem znajdowała się na wzbudzonym poziomie oscylacyjnym, to oddziaływanie przenosi ją na podstawowy (zerowy) poziom oscylacyjny. Energia rozproszonego fotonu jest większa o różnicę energii poziomów oscylacyjnych $h\nu$. Pasma antystokesowskie pojawia się w widmie Ramana po stronie przeciwnej co pasmo stokesowskie w stosunku do pasma Rayleigha. To pasmo ma zwykle niższą intensywność niż pasma stokesowskie.

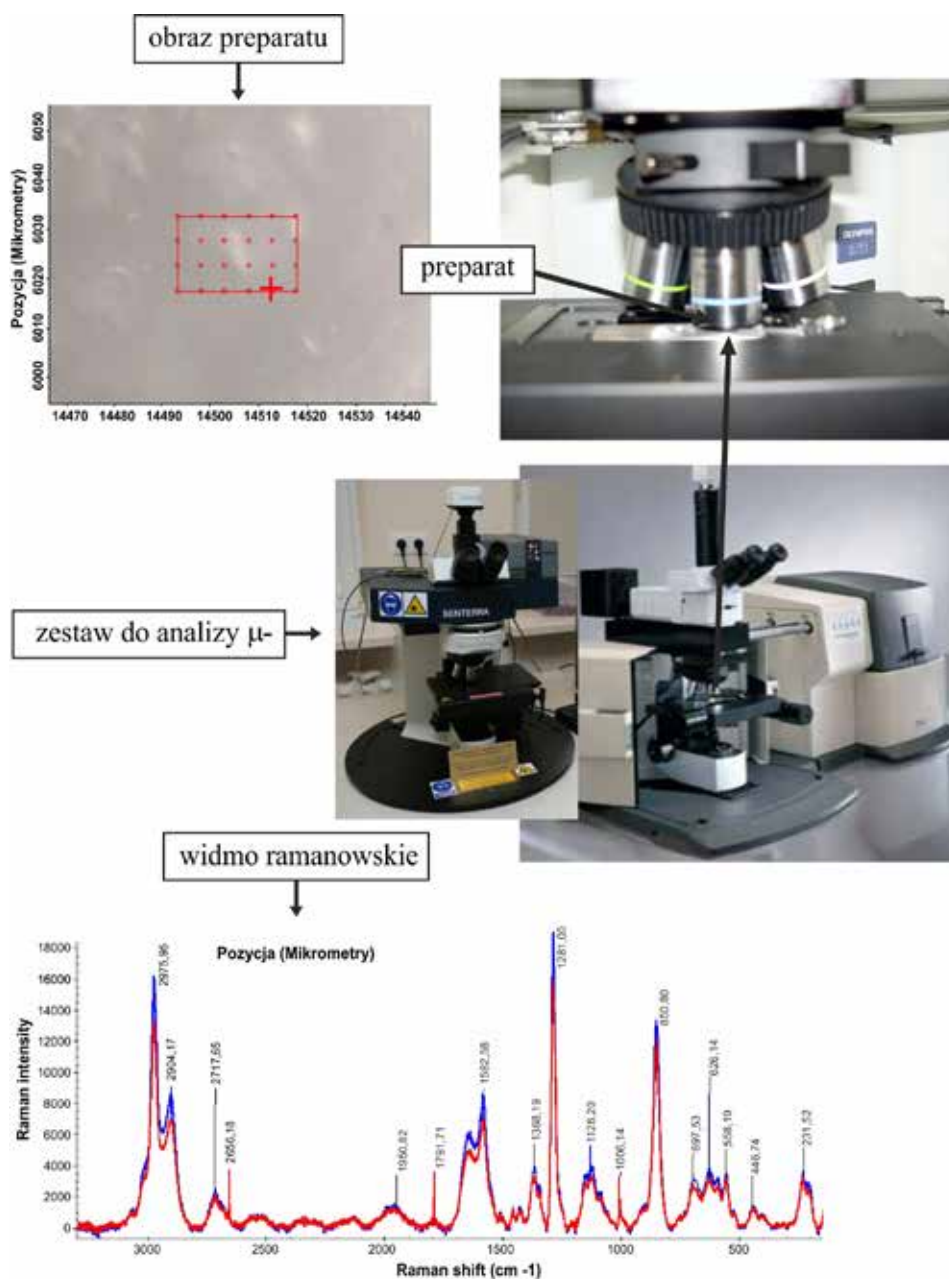
¹² Pasma Rayleigha – powstają na skutek oddziaływania fotonów padającego promieniowania o częstości ν_0 , niepasujących do poziomów energetycznych cząsteczki. Gdy molekula po oddziaływaniu z promieniowaniem powraca na ten sam poziom energetyczny, to zjawisko to sprowadza się do klasycznego rozproszenia Rayleigha.

Przemieszczanie zrębów atomowych nie ma wpływu na polaryzowalność. W rzeczywistości wiązania w cząsteczkach nie są idealnie jonowe i dlatego jest możliwe otrzymanie pasma ramanowskiego takich cząsteczek. Te pasma mają jednak tak małą intensywność, że są praktycznie niemożliwe do zaobserwowania. Innym przykładem jest cząsteczka HCl, która daje widmo Ramana nie tylko w stanie gazowym, lecz także w roztworze wodnym na tyle stężonym, że cofnięta jest dysocjacja kwasu. Świadczy to o dość dużym udziale wiązania kowalencyjnego w wiązaniu H–Cl. W przypadku silnie spolaryzowanych wiązań jonowych zarówno moment dipolowy, jak i jego zmiana w czasie są dość duże, co objawia się w widmie w podczerwieni dużą intensywnością pasm o silnie spolaryzowanych wiązaniach, odwrotnie niż w widmie Ramana. W literaturze pojawiło się tzw. spektroskopowe kryterium polarności wiązania, które mówi, że jeżeli rośnie intensywność pasma w podczerwieni, a w widmie Ramana maleje, oznacza to, że odpowiednie wiązanie w molekułe staje się bardziej spolaryzowane. I na odwrót – jeżeli rośnie intensywność pasma ramanowskiego, a maleje intensywność pasma w podczerwieni, to będzie to oznaczać wzrost kowalencyjności odpowiedniego wiązania.

Zaletą spektroskopii Ramana jest łatwość przygotowania próbek. Ta technika nie wymaga stosowania niestabilnych chemicznie okienek KBr. Można wykonywać pomiary wodnych roztworów próbek. Możliwe jest też wykonywanie pomiarów w wyższych temperaturach. Spektroskopia Ramana jest szczególnie przydatna do pomiarów częstości oscylacyjnych kompleksów metal – ligand, których drgania przypadają na obszar 100–700 cm^{-1} . Pomiary widm w podczerwieni są w tym obszarze bardzo trudne do przeprowadzenia. Kolejną zaletą tej techniki jest to, że źródła wzbudzania emitują promieniowanie w zakresie widzialnym, co pozwala na precyzyjne zestrojenie układu optycznego mikroskopów ramanowskich.

Widma Ramana mogą być wykorzystywane do identyfikowania nieznanymi substancji, wykrywania w cząsteczce określonych grup atomów lub rodzajów wiązań chemicznych, ustalania struktury geometrycznej cząsteczek oraz analizy drgań cząsteczki. Cenną modyfikacją spektroskopii ramanowskiej jest **spektrometria mikro-Ramana**, która znalazła zastosowanie również w badaniach kryminalistycznych. Procedura wyznaczania intensywności pasm jest bardzo ważnym elementem prawidłowego stworzenia obrazu ramanowskiego. Spektrometria mikro-Ramana to połączenie spektrometrii Ramana i mikroskopii optycznej¹³. Na ekranie monitora jest widoczny (przy odpowiednim powiększeniu) obraz mikroskopowy badanej powierzchni preparatu (zdj. 7).

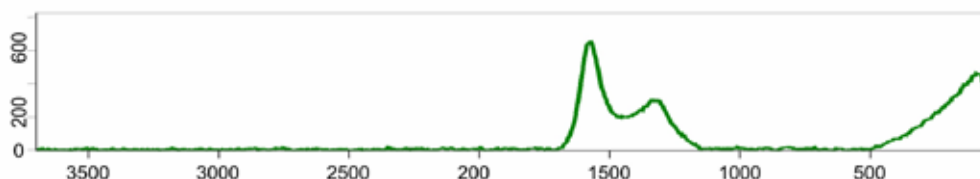
¹³ M. Bowden i in., *Thermal degradation of polyurethane-backed poly(vinyl chloride) studied by Raman microline focus spektrometry*, „Polymer” 1994, nr 35, s. 1654.



Zdj. 7. Schemat analizy powierzchni ziarna niespalonego prochu za pomocą spektrometrii mikro-Ramana.

Typowe urządzenie do przesuwania preparatu pod mikroskopem pozwala wybrać odpowiednie miejsce do analizy za pomocą spektrometrii ramanowskiej. Spektroskopia mikro-Ramana jest uważana za metodę nieniszczącą substancję podczas jej badania i pozwala na uzyskanie informacji o składzie chemicznym próbki w mikroskali.

Badania tonerów przeprowadzone metodą spektroskopii ramanowskiej wykazały obecność węglowych struktur cząsteczkowych, na podstawie pasm pochodzących od węgla amorficznego lub (i) grafitu, a także obecność krzemionki amorficznej. W zależności od linii wzbudzenia obserwowano pasma w 1574 cm^{-1} i 1332 cm^{-1} (zdj. 8) oraz 1375 cm^{-1} , 1253 cm^{-1} , a także 2693 cm^{-1} .



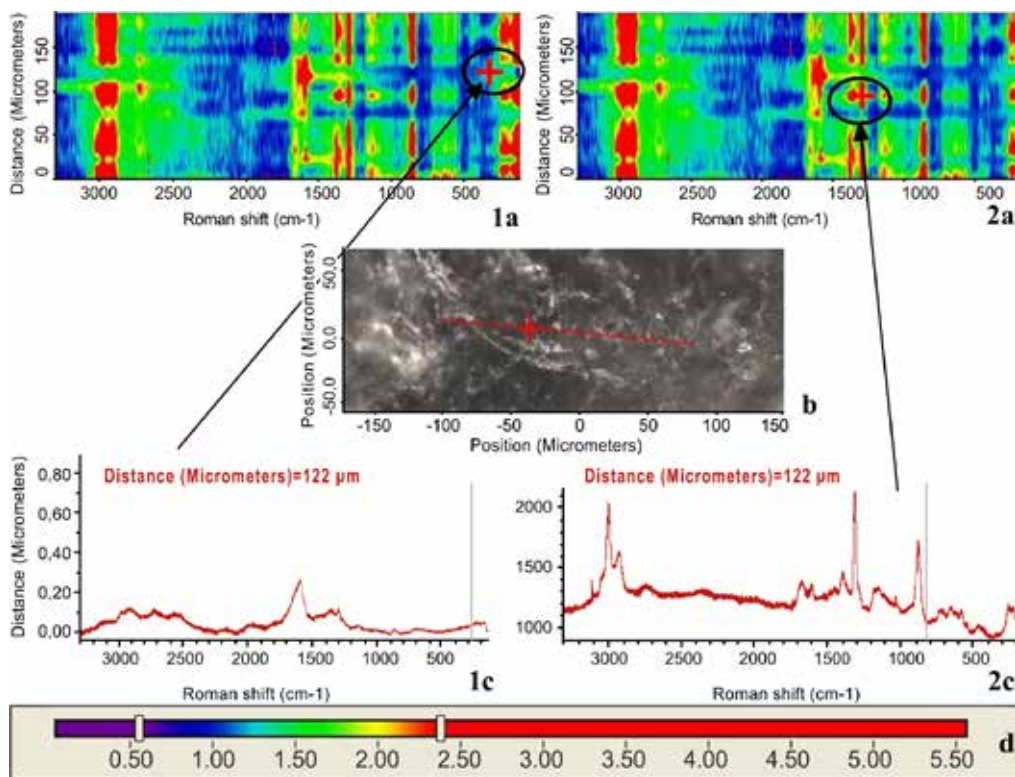
Zdj. 8. Widmo Ramana próbki tonera w postaci proszku pobranego bezpośrednio z kartridża urządzenia Lexmark C780 – zamiennik, wykonane przy wzbudzeniu laserem o długości fali 532 nm.

Dzięki sprzężeniu spektrometru ramanowskiego z mikroskopem wyposażonym w przesuw skanujący jest możliwe zebranie widm z kilku punktów powierzchni górnej lub dolnej próbki i sporządzenie map na podstawie wielkości wybranej do porównywania widm. Właściwy obraz, jaki się uzyskuje, jest przedstawiony w postaci mapki składającej się z kolorowych kwadracików. W ten sposób otrzymuje się rozkład funkcji dyskretnej i dopiero sam program za pomocą odpowiedniego wielomianu aproksymuje¹⁴ do rozkładu funkcji ciągłej.

W celu zbadania homogeniczności mikrodrobiny niespalonego lub częściowo spalonego prochu wykonano mapowanie ramanowskie kilku ziaren prochu. Jedynie niektóre ziarna wykazały obecność ostrych pasm charakterystycznych. Najbardziej wyraźne w widmie ramanowskim mikrodrobiny pozostałości powystrzałowych są pasma odpowiadające grupom NO_2 oraz CH_2 , nitrogliceryny i nitrocelulozy.

Na zdj. 9 pokazano mapy zmiany intensywności pasma drgań rozciągających grupy NO_2 oraz pasma drgań rozciągających symetrycznych grupy CH_2 . W przypadku mikrodrobiny pochodzącej z pozostałości od amunicji G.F.L $9 \times 19\text{ mm}$ Fiocchi zawierającej nitroglicerynę i nitrocelulozę intensywność pasma grupy NO_2 zmienia się od 0,10 do 5,50. Ta zmiana pozwala sądzić, że układ nie jest homogeniczny. Pojawiają się obszary niemal pozbawione związków chemicznych zawierających pasma grupy NO_2 .

¹⁴ Aproksymacja (łac. *approximare* – ‘przybliżyć’) – proces określania rozwiązań przybliżonych na podstawie rozwiązań znanych, które są bliskie rozwiązaniom dokładnym w ściśle sprecyzowanym sensie, za: <https://pl.wikipedia.org/wiki/Aproksymacja> [dostęp: 8 I 2018] (przyp. red.).



Zdj. 9. Mapy zmiany intensywności pasma drgań rozciągających grupy NO_2 w ziarnie niespalonego prochu z amunicji G.F.L 9×19 mm Fiocchi (1a, 2a); obraz analizowanego fragmentu powierzchni próbki z mikroskopu konfokalnego (b); widma Ramana w punktach zaznaczonych czerwonym krzyżykiem odpowiednio na mapach (1c, 2c); skala przyporządkowania kolorów wartościom zmiany intensywności pasma grupy NO_2 (d)¹⁵.

Widma przedstawione na zdj. 9 odzwierciedlają charakter badanej mikrodrobiny pod względem składu chemicznego w jednym punkcie na mapie. W zależności od rozkładu barw na mapie obserwowano zmiany intensywności pasm. W punkcie zaznaczonym na mapie czerwonym krzyżykiem w obszarze jasnozielonym (zdj. 9.1a) widoczne w widmie jest głównie pasmo odpowiadające drganiom rozciągającym C–C (zdj. 9.1c). Natomiast w punkcie zaznaczonym na mapie czerwonym krzyżykiem w obszarze czerwonym (zdj. 9.2a) w widmie są widoczne wszystkie pasma związane z obecnością nitrogliceryny i nitrocelulozy (zdj. 9.2c)¹⁶.

Metoda analityczna wykazała możliwość identyfikacji niektórych związków organicznych zawartych w pozostałościach powystrzałowych, a także możliwość

¹⁵ A. Łasińska, *Analiza nieorganicznych i organicznych pozostałości po wystrzale z broni palnej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 16, s. 182.

¹⁶ Tamże.

obrazowania (mapowania) zmian intensywności pasm niektórych grup funkcyjnych substancji organicznych obecnych w pojedynczym ziarnie. Pełną identyfikację materiału dowodowego zapewniają badania morfologii oraz nieorganicznych składników typowych cząstek pozostałości powystrzałowych.

W spektroskopii Ramana stosuje się obecnie wiele nowych technik, które przede wszystkim zwiększają czułość tej metody. **Rezonansowa spektroskopia Ramana** (ang. *Resonance Raman Spectroscopy*, RRS) jest techniką, w której częstość wiązki monochromatycznej lasera jest dostrojona do częstości przejścia elektronowego analizowanego związku, co prowadzi do selektywnego wzrostu intensywności pasm ramanowskich 10^2 – 10^6 razy w stosunku do klasycznej dyspersyjnej spektroskopii Ramana.

W badaniach stosuje się również **powierzchniowo wzmocnioną spektroskopię Ramana** (ang. *Surface Enhanced Raman Spectroscopy*, SERS), w której mierzy się rozproszenie ramanowskie cząsteczek zaadsorbowanych na powierzchni metalu lub metalicznego zolu (głównie srebra). Zjawisko wzmocnienia tłumaczy się dwoma różnymi mechanizmami: chemicznym i elektromagnetycznym. SERS zwiększa intensywność sygnału ramanowskiego 10^3 – 10^7 razy w stosunku do sygnału otrzymanego w klasycznym eksperymencie ramanowskim¹⁷. Wykorzystując **konfokalną mikroskopię ramanowską** (ang. *Confocal Raman Microscopy*), można wykonać widma z bardzo małego, precyzyjnie wybranego obszaru próbki (ok. $1 \mu\text{m}^2$). Dzięki możliwościom, jakie daje mikroskop konfokalny, uzyskuje się przekroje optyczne badanych materiałów, obrazy trójwymiarowe oraz wizualizację komórek i fragmentów tkanek powłok lakierniczych pochodzących od różnych samochodów, pozostałości powystrzałowych, detekcji śladowych ilości substancji lub zanieczyszczeń, trudnych do podrobienia zabezpieczeń dokumentów.

Niektóre rodzaje nowoczesnej mikroskopii świetlnej mogą dawać zdjęcia o bardzo wysokiej rozdzielczości. W przeszłości podstawowym ograniczeniem jakości uzyskiwanych obrazów mikroskopowych były wady soczewek (aberracja chromatyczna, aberracja sferyczna). Ten problem pokonano, przynajmniej w najdroższych modelach, w drugiej połowie XIX w. Napotkano jednak kolejną barierę – zjawiska dyfrakcji oraz interferencji, które powodują, że odpowiednią ostrość obrazu można uzyskać jedynie dla obiektów o rozmiarach wielokrotnie większych niż długość stosowanej fali. Obiekty mniejsze niż $1/2$ długości fali nie są w ogóle widoczne. Obiekty o wielkości rzędu długości fali pojawiają się w obrazie mikroskopowym, ale w formie zniekształconej: otoczone barwnymi obwódkami. Dlatego też nawet najlepsze mikroskopy optyczne pracujące w zakresie światła widzialnego dają maksymalne powiększenia rzędu 1500 razy. Mikroskopy pracujące w zakresie ultrafioletu osiągają maksymalne powiększenie do ok. 3500 razy. Potrzeba uzyskania dużych powiększeń obiektów, niemożliwych do uzyskania w mikroskopach optycznych, zdeterminowała rozwój mikroskopii elektronowej. Jeśli chce się zobaczyć coś bardzo małego o bardzo wysokiej

¹⁷ B. Sharma i in., *SERS: Materials, applications, and the future*, „Materials today” 2012, nr 15, s. 16–25.

rozdzielczości, a także poznać skład pierwiastkowy badanej substancji, to należy wykorzystać technikę, jaką jest **mikroskopia elektronowa sprzężona z mikroanalizatorem rentgenowskim** (zdj. 10).



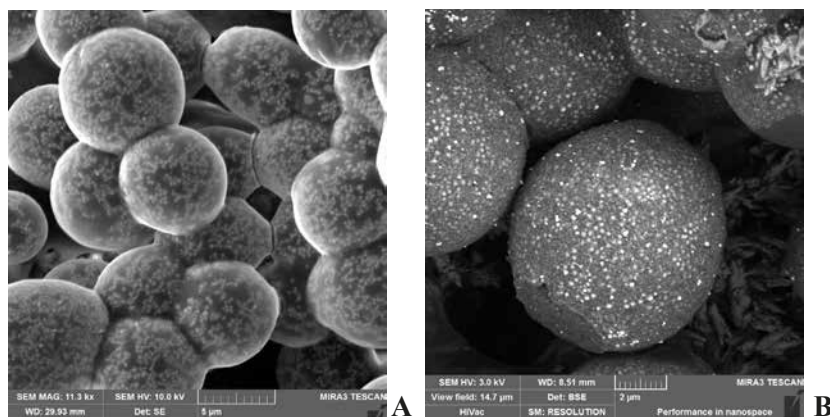
Zdj. 10. Skaningowy mikroskop elektronowy z detektorem mikroanalizy rentgenowskiej.

Od 70 lat **mikroskop elektronowy** stał się powszechnie stosowanym urządzeniem zarówno w nauce, przemyśle, jak i kryminalistyce. Mikroskopy elektronowe różnią się od mikroskopów świetlnych tym, że tworzą obraz próbki za pomocą wiązki elektronów, a nie promieni światła. Elektrony mają znacznie krótszą długość fali niż światło widzialne, co pozwala mikroskopom elektronowym uzyskiwać obrazy o wyższej rozdzielczości, niż standardowe obrazy uzyskiwane w mikroskopach świetlnych.

Po opracowaniu odpowiedniej metodyki analitycznej mikroskop elektronowy daje szerokie możliwości badawcze dla mikroskopijnych próbek substancji chemicznych oraz złożonych materiałów w postaci ciał stałych. Umożliwia przeprowadzenie jednoczesnych badań ich składu chemicznego i morfologii, a dodatkową jego zaletą jest to, że nie wymaga on w wielu przypadkach zniszczenia próbki – ani w procesie jej przygotowania do analizy, ani podczas pomiaru.

W **skaningowym mikroskopie elektronowym** (SEM) obraz jest uzyskiwany w wyniku detekcji elektronów wtórnych i (lub) odbitych, którymi próbka jest bombardowana. Techniki obrazowania, takie jak: BSE (elektrony wstecznie rozproszone), SE (elektrony wtórne), CL (katodoluminescencja), LVSTD (w zmiennej próżni) oraz mikroanaliza rentgenowska, pozwalają na dokonanie analizy próbek – poza gazem – zarówno przewodzących, jak i nieprzewodzących prąd. Elektrony wtórne i wstecznie rozproszone są powszechnie używane do obrazowania próbek. Najbardziej wartościowymi dla ukazania morfologii i topografii próbek są elektrony wtórne, natomiast elektrony wstecznie rozproszone służą do zilustrowania kontrastu w składzie

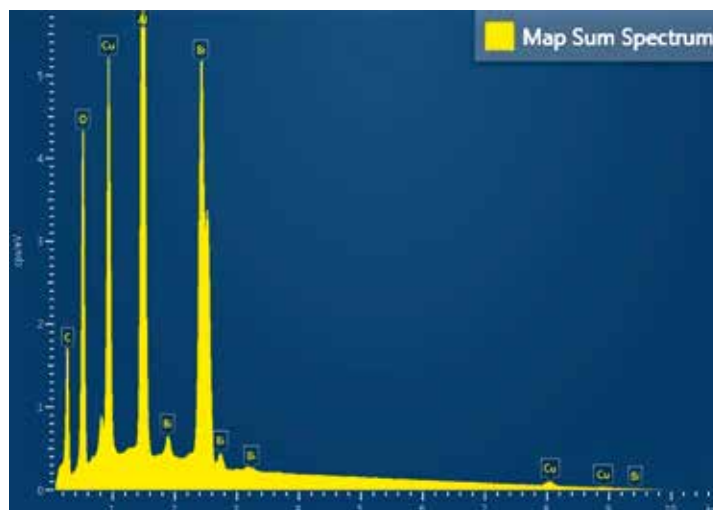
wielofazowych próbek. Sygnał elektronów wtórnych pochodzi z obszaru leżącego blisko powierzchni próbki, dlatego obrazy z tego detektora dobrze odzwierciedlają topografię (ukształtowanie) powierzchni próbek. Charakteryzują się one dużą głębią ostrości. Sygnał elektronów wstecznie rozproszonych (elektronów odbitych) pochodzi z dużego obszaru położonego w głębi struktury próbek, dlatego obrazy z tego detektora zwykle mają niższą rozdzielczość niż obrazy SE. Obrazy BSE charakteryzują się mniejszą głębią ostrości i nie oddają dobrze topografii próbki, ale dostarczają informację na temat gęstości obserwowanych powierzchni. Pokazują jakościowe zróżnicowanie fazowe (chemiczne) powierzchni próbek. W zależności od liczby atomowej pierwiastka Z , która opisuje liczbę protonów w jądrze, większa lub mniejsza liczba elektronów wiązki pierwotnej zostaje rozproszona wstecznie. To oznacza, że sygnał pochodzący od pierwiastków ciężkich jest dużo silniejszy niż od pierwiastków lekkich. Pozwala to na detekcję wtrąceń metalicznych lub pierwiastków ciężkich w obserwowanych próbkach. Kontrast charakteryzujący obrazowanie BSE jest proporcjonalny do kwadratu liczby masowej i zamiast kontrastu topograficznego (dla obrazowania SE) można obserwować kontrast materiałowy (zdj. 11).



Zdj. 11. Obraz wykonany skaningowym mikroskopem elektronowym techniką obrazowania SE (A) i BSE (B).

Kolejną bardzo użyteczną techniką jest **spektroskopia EDS**. Jej działanie jest oparte na detekcji promieniowania charakterystycznego, emitowanego przez atomy próbki wzbudzone przez elektrony wiązki. Podczas bombardowania próbki wiązką elektronów następuje wybijanie elektronów pierwiastków wchodzących w skład próbki. Puste miejsca po wybitych elektronach są zastępowane elektronami z wyższych orbitali. Podczas tego przejścia, w celu wyrównania różnic energii między elektronami, są emitowane promienie rentgenowskie charakterystyczne dla danego pierwiastka. Detektor EDS analizuje promienie rentgenowskie, i na tej podstawie można określić skład pierwiastkowy badanej próbki. Dodatkowo można wykonać badania półilościowe, dzięki czemu można przeanalizować różne próbki nie tylko pod kątem różnorodności, która jest widoczna

po wykonaniu fotografii BSE, lecz także określić zmiany jakościowe i ilościowe ich składu. Analizy liniowe i mapy zawartości pozwalają także na badanie powierzchni próbek w celu uchwycenia subtelnych zmian w składzie pierwiastkowym, niewidocznych na fotografii BSE. Skład pierwiastkowy przeliczony na procenty wagowe można łatwo zinterpretować, a podając skład w przeliczeniu na procent atomowy można wyciągać wnioski na temat stechiometrii związków budujących daną próbkę (zdj. 12 i tab. 2).



Zdj. 12. Widmo EDS uzyskane podczas obserwacji SEM. Symbolami pierwiastków glinu, miedzi, tlenu, i bizmutu zostały oznaczone linie K, L, M charakterystycznego promieniowania rentgenowskiego.

Tab. 2. Wyniki ilościowe mikroanalizy rentgenowskiej. Tabelę wyników wygenerowano za pomocą programu Aztek wchodzącego w skład oprogramowania mikroskopu SEM Mira 3XMU¹⁸.

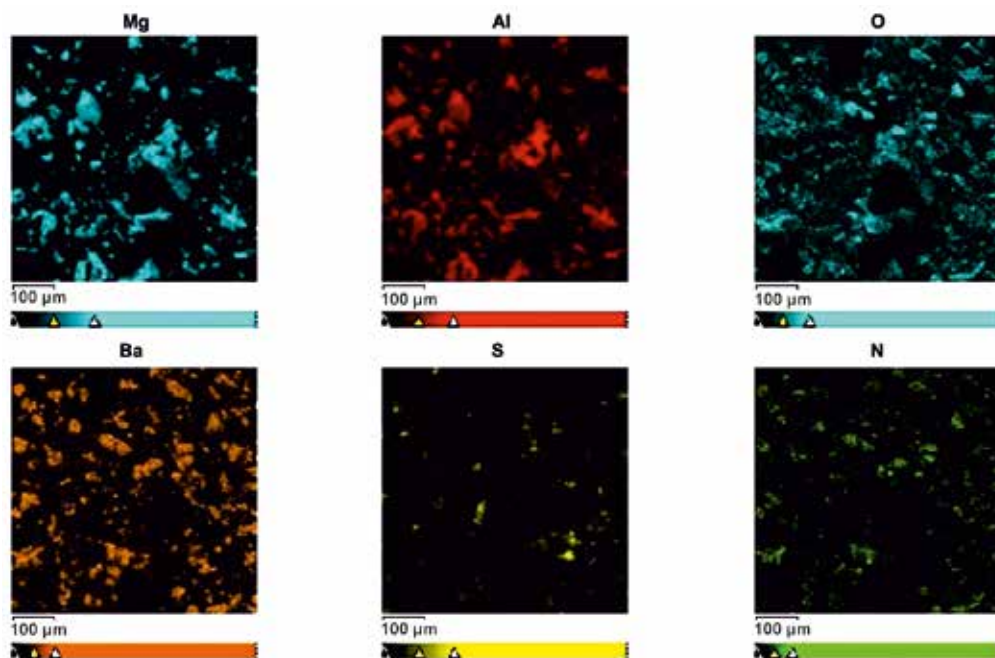
| Pierwiastek | Typ linii | k-Ratio | Wt% | Wt% Sigma | Proponowany związek chemiczny |
|-------------|-----------|---------|-------|-----------|--------------------------------|
| O | K | 0,00576 | 10,38 | 0,05 | SiO ₂ |
| Al | K | 0,01818 | 19,11 | 0,06 | Al ₂ O ₃ |
| Cu | L | 0,01357 | 18,53 | 0,08 | Cu |
| Bi | M | 0,04348 | 51,97 | 0,12 | Bi |

Wyniki analizy ilościowej zawierają następujące informacje:

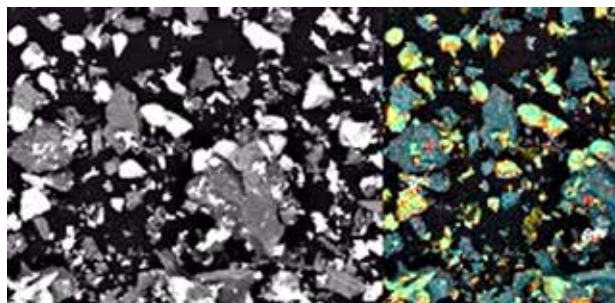
- Wt % – procent wagowy danego pierwiastka w próbce,
- Wt% Sigma – błąd procentu wagowego,
- k-Ratio – stosunek natężenia promieniowania linii charakterystycznej danego pierwiastka w próbce do natężenia od czystego pierwiastka w tych samych warunkach.

¹⁸ A. Łasińska, *Badania mikrośladów...*, s. 810.

Charakterystyczne promieniowanie rentgenowskie jest wykorzystywane do otrzymywania map rozkładu stężenia pierwiastków (ang. *mapping*). Wiązka analityczna skanuje badany obszar punkt po punkcie. Spektrometr jest tak ustawiany, aby rejestrował punkt w zadanym obszarze, gdy wykryje impuls rentgenowski o energii charakterystycznej dla danego pierwiastka. W ten sposób powstaje mapa odwzorowująca rozmieszczenie tego pierwiastka w badanym obszarze. Nowoczesne systemy EDS potrafią utworzyć kolorowe mapy w odpowiednich odcieniach, na których jest ukazana wartość względna intensywności impulsu w każdym punkcie. Wymaga to jednak zastosowania wystarczająco długiego czasu postoju wiązki w każdym punkcie analitycznym. Podczas jednego przebiegu wiązki analitycznej można zarejestrować mapy rozkładu dla kilkunastu pierwiastków (zdj. 13a i 13b). Mapa jest zbiorem plamek odpowiadających impulsom promieniowania rentgenowskiego. Stopień zagęszczenia plamek odpowiada stężeniu pierwiastka. Istotny wpływ na ocenę rozkładu stężenia pierwiastka ma czas zbierania impulsów. Mapki nie pozwalają jednak na wychwytywanie małych różnic w stężeniach oraz niskich stężeń (ze względu na obecność plamek pochodzących od tła – promieniowanie ciągłe).

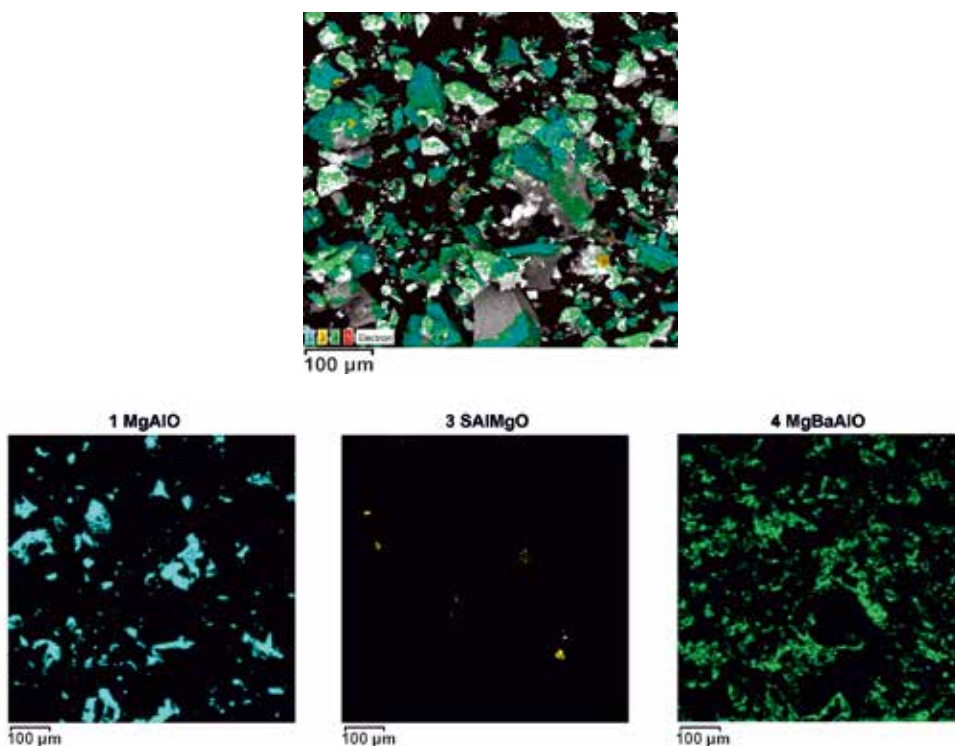


Zdj. 13a. Przykłady map rozkładu stężenia pierwiastków. Mapy wygenerowano za pomocą programu Aztek wchodzącego w skład oprogramowania mikroskopu SEM Mira 3XMU, na podstawie zmierzonego widma EDS.



Zdj. 13b. Obraz BSE oraz sumaryczny obraz nałożenia map stężeń pierwiastków. Mapy wygenerowano za pomocą programu Aztek wchodzącego w skład oprogramowania mikroskopu SEM Mira 3XMU, na podstawie zmierzonego widma EDS.

Na podstawie map określa się wstępnie, za pomocą odpowiedniego oprogramowania, związki chemiczne wchodzące w skład badanego materiału oraz udział procentowy tych związków. Przykładową mapę rozkładu faz oraz ich udział procentowy przedstawiono na zdj. 14 i w tab. 3.



Zdj. 14. Przykłady map rozkładu faz. Mapy wygenerowano za pomocą programu Aztek wchodzącego w skład oprogramowania mikroskopu SEM Mira 3XMU.

Tab. 3. Wartości procentowego udziału znalezionych frakcji.

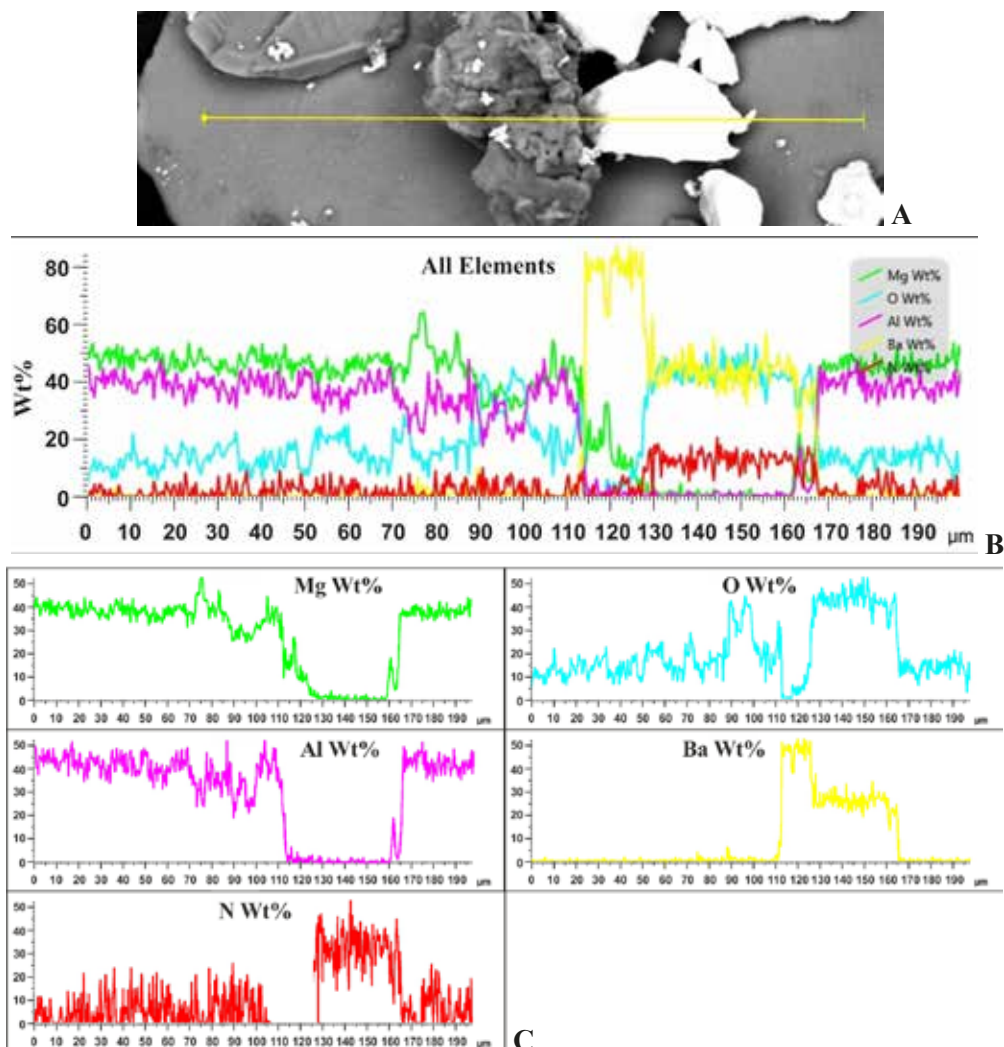
| Związki chemiczne | Frakcja (%) | Liczba pikseli |
|-------------------|-------------|----------------|
| 1 MgAlO | 9,1 | 23 849 |
| 3 SAlMgO | 0,2 | 553 |
| 4 MgBaAlO | 11,9 | 31 172 |

W mikroanalizie rentgenowskiej można stosować również technikę analizy liniowej. Polega ona na skanowaniu wiązką elektronową wzdłuż określonej linii na powierzchni próbki z jednoczesną rejestracją zmian natężenia emitowanego promieniowania rentgenowskiego. Liniowa analiza składu chemicznego pokazuje zmiany stężenia danego pierwiastka wzdłuż linii wybranej na powierzchni badanej próbki. Na wykresach umieszczonych pod zdj. 15 przedstawiono przykład analizy liniowej.

Jedną z cech najbardziej atrakcyjnych w mikroskopii elektronowej jest szeroka gama jej zastosowań w różnych dziedzinach kryminalistyki. Jest ona wykorzystywana do badań identyfikacyjnych i porównawczych materiałów dowodowych, takich jak: drobiny szkła i lakierów, metali, tonerów do urządzeń drukujących, morfologii włókien, mas pirotechnicznych oraz ich pozostałości, urządzeń pirotechnicznych oraz pozostałości po wystrzale z broni palnej (ang. *gunshot residue*, GSR). Dzięki niej można analizować mikroślady substancji stałych na poziomie mikrometrycznym (pyłki roślin, ziarna gleby) znalezione na ubraniach, odpryski farby z miejsca przestępstwa, a nawet stwierdzić, czy samochód w momencie wypadku miał włączone reflektory. Mikroskopia elektronowa pozwala analizować słabo widoczne lub niewidoczne mikroskopijne ślady dowodowe przez ich obrazowanie, porównywanie obrazów i mikroanalizę rentgenowską.

Z punktu widzenia kryminalistyki istotnym problemem dotyczącym analizy jest między innymi identyfikacja urządzenia wykonawczego. W ramach przeprowadzonego projektu naukowo-badawczego podjęto rozszerzone badania zmierzające do identyfikacji indywidualnej urządzeń drukujących i powielających. Przeprowadzono testy oryginalnych tonerów oraz ich zamienników, analizując wydruki pochodzące ze 134 laserowych urządzeń drukujących produkowanych przez 10 różnych firm. Uzyskane obrazy mikroskopowe pozwoliły przyporządkować charakterystyczne cechy tonerów do poszczególnych grup urządzeń, tj. monochromatycznych drukarek laserowych, kolorowych drukarek laserowych, monochromatycznych urządzeń wielofunkcyjnych oraz kolorowych urządzeń wielofunkcyjnych. Ustalono kryteria oceny indywidualnej, przyporządkowując i segregując cechy szczególne tonerów przez nadanie im konkretnych nazw. Na podstawie obrazów SEM i ustalonych kryteriów ujawniono szczegółową topografię struktury tonerów. Wykonane badania pozwoliły określić różnice lub podobieństwa między poszczególnymi tonerami

na wydrukach. Przeprowadzona analiza powierzchni tonera na wydrukach uzyskanych z różnych laserowych urządzeń drukujących wykazała, że nie w każdym przypadku warstwę tonera tworzy powierzchnia lita oraz ziarnista. Jeżeli obserwowano oba rodzaje powierzchni, to różnica między nimi polegała na stosunku rozmiaru jednej warstwy do drugiej i formie rozmieszczenia ich w obszarze jednego znaku, w zależności od typu urządzenia i firmy.

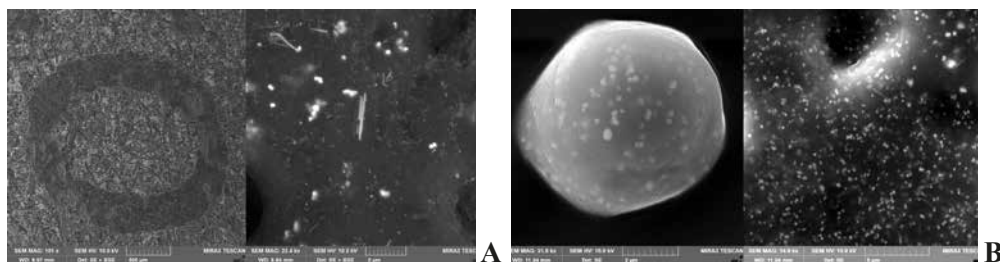


Zdj. 15. Mikrofotografia SEM w trybie BSE powierzchni ziarna z zaznaczoną linią skanowania (A); wykresy: sumaryczny wynik analizy linowej EDX wzdłuż linii (B); analiza liniowa EDX rozmieszczenia pierwiastków Mg, O, N, Al, Ba w pojedynczym ziarnie (C). Analizę liniową wygenerowano za pomocą programu Aztek wchodzącego w skład oprogramowania mikroskopu SEM Mira 3XMU.

W niektórych przypadkach oryginalnych tonerów takie cechy, jak: proste struktury pałeczkowate czy struktury nieregularne w modelu Lexmark T650n/T652/T654n (zdj. 16), wygięte struktury pałeczkowate w modelu Lexmark X264/X363/X364, pojedyncze struktury sferyczne wyglądające niczym piłeczki porożrzucane na powierzchni tonera w modelu Lexmark X940e/X945e, ziarna o zbliżonym do siebie rozmiarze w modelu Lexmark MX410, struktury w postaci kul i sześcianników na powierzchni ziaren w modelu Canon iRAAdv C9070 lub struktury samych sześcianników na powierzchni ziaren w modelu OKI MB461/MB471/MB491, są indywidualne dla konkretnego wydruku. Niektóre cechy mogą występować jedynie w nielicznych przypadkach, np. struktury pałeczkowate charakterystyczne dla dwóch modeli Dell (5310n i 5350dn), jednego modelu kolorowego urządzenia wielofunkcyjnego OKI C5550M-FP oraz kilku modeli firmy Lexmark, głównie typu monochromatycznych urządzeń.

Jeszcze inne cechy mogą być charakterystyczne dla konkretnego typu urządzenia, np. struktury nieregularne lub kuliste tuż pod powierzchnią ziarna i powierzchnią litą tonera charakteryzujące się innym kontrastem na obrazie SEM. Tego typu struktury występowały w monochromatycznych drukarkach laserowych i monochromatycznych laserowych urządzeniach wielofunkcyjnych.

Oryginalne tonery tworzące tekst na wydrukach charakteryzują się cechami, które pozwalają na odróżnianie ich jedynie w pewnych granicach. Niestety, wiele z tych cech powtarza się w różnych modelach u różnych producentów, co znacznie utrudnia ich identyfikację. Niemniej jednak można dokładnie określić grupę urządzeń drukujących (monochromatyczne, kolorowe).

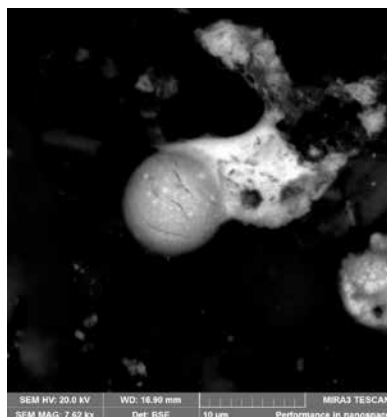


Zdj. 16. Obrazy SEM powierzchni litej (A) oraz ziarna i jego powierzchni (B) tonera dla wydruku wytworzonego z modelu Lexmark T650n/T652/T654n.

Mikroskopy elektronowe do badań kryminalistycznych mogą być wyposażone również w dodatkowe oprogramowanie umożliwiające analizę cząsteczek pozostałości po wystrale z broni palnej (GSR) o charakterystycznej morfologii i swoistym składzie pierwiastkowym. Pozwala ono między innymi analizować pozostałości znalezione na ubraniu lub skórze osoby oddającej strzał z broni palnej oraz cząstki pozostałości po reakcjach pirotechnicznych¹⁹. W kryminalistyce analiza pozostałości

¹⁹ H. Krüsemann, *SEMs and Forensic Science*, „Problems of Forensic Science” 2001, nr 47,

powystrzałowych jest często stosowaną metodą badań w celu wyjaśniania okoliczności zdarzeń z użyciem broni palnej. Ślady po wystrzale z broni palnej rutynowo zabezpiecza się na stoliku mikroskopowym. Na podstawie wysokiej średniej liczby atomowej (Z) cząstek GSR, pochodzących ze składu mieszanin spłonkowych, przeszukiwanie takich cząstek jest przeprowadzane na podstawie ich jasności w obrazie elektronów wstecznie rozproszonych (BSE) (zdj. 17).



Zdj. 17. Zdjęcie SEM cząstki „charakterystycznej” pozostałości po wystrzale z broni palnej na powierzchni stolika mikroskopowego.

Skład pierwiastkowy cząstek jest analizowany przez system EDX, w którym powszechnym typem detektora jest detektor krzemowy domieszkowany litem Si(Li) w stanie stałym.

Ponad 25 lat temu wprowadzono automatyczne systemy przeszukiwania, które zastąpiły manualne przeszukiwanie cząstek z pozostałości po wystrzale pochodzących ze spłonki²⁰. Takie automatyczne systemy przeszukiwania lokalizują cząstki, analizują ich skład pierwiastkowy i dokonują ich identyfikacji. W związku z niewielkim rozmiarem cząstki GSR (np. 0,5–10 µm) w stosunku do obszaru próbki (120–480 mm² w zależności od rozmiaru podstawki mikroskopu SEM) i dużą liczbą cząstek środowiskowych o wysokiej średniej liczbie atomowej (Z) znajdujących zazwyczaj w analizowanych próbkach, czas potrzebny na przeprowadzenie automatycznego przeszukiwania jest długi. Wynikiem analizy GSR jest automatycznie generowany raport z badań, który zawiera liczbę znalezionych cząsteczek z uwzględnieniem zdefiniowanych klas. Dzięki nieustannemu rozwojowi technologicznemu

s. 110–121.

²⁰ R.S. White, A.D. Owens, *Automation of Gunshot Residue Detection and Analysis by Scanning Electron Microscopy/Energy Dispersive X-ray Analysis (SEM/EDX)*, „Journal of Forensic Science” 1987, nr 32, s. 1595–1603; M. Germani, *Evaluation of Instrumental Parameters for Automated Scanning Electron Microscopy/Gunshot Residue Particle Analysis*, „Journal of Forensic Science” 1991, nr 36, s. 331–342.

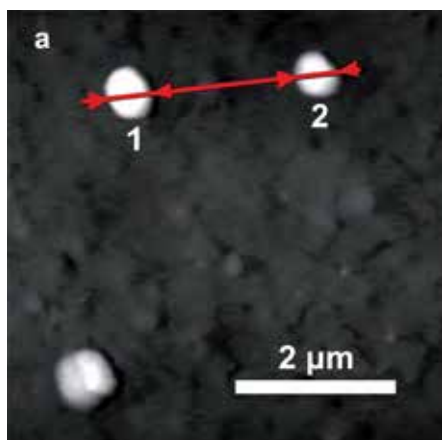
sprzętu komputerowego i oprogramowania zwiększają się możliwości automatycznych systemów w zakresie detekcji większej liczby cząstek i o mniejszych rozmiarach, które są dokonywane w krótszym czasie.

Innym sposobem obrazowania jest uzyskanie obrazu powierzchni ze zdolnością rozdzielczą rzędu wymiarów pojedynczego atomu. Do tego służy **mikroskop sił atomowych** (ang. *atomic force microscope*, AFM). Wśród wielu urządzeń kojarzonych z nanotechnologią żadne nie jest tak dobrze rozpoznawalne i proste w założeniu swojej budowy jak mikroskop sił atomowych, zwany również mikroskopem bliskich oddziaływań. W ciągu ostatnich kilku lat rozszerzył się obszar zastosowań AFM, głównie ze względu na jego olbrzymie możliwości niedostępne dla innych technik badawczych. Jego duża rozdzielczość umożliwia badania pojedynczych cząsteczek, ich ugrupowań oraz elementów struktur nadcząsteczkowych. AFM wykorzystuje siły oddziaływań międzyatomowych na zasadzie prowadzenia ostrza nad lub pod powierzchnią próbki. Ostrze jest przymocowane do sprężyny (dźwigni), której odchylenie umożliwia wyznaczenie siły oddziaływania międzyatomowego między atomami ostrza i badanej powierzchni. Mapa sił dla każdego punktu powierzchni próbki jest przetwarzana komputerowo na obraz. Pomiar ugięcia dźwigni jest dokonywany metodami optycznymi. Czułość odczytu ugięcia dźwigni sięga dziesiątych części angstroma²¹. Czubek ostrza składa się z kilkuset atomów do nawet jednego atomu. Te ostrza produkuje się zazwyczaj z krzemu i azotku krzemu. AFM może pracować w trybie kontaktowym, w którym dźwigenka jest utrzymywana w odległości mniejszej niż kilka dziesiątych nanometra od powierzchni próbki, siły zaś, jakie występują, są siłami odpychania. Podczas pracy w trybie bezkontaktowym dźwigenka jest utrzymywana w odległości od kilku do kilkudziesięciu nanometrów od powierzchni badanego materiału. W tym przypadku między próbką a sondą działają siły przyciągania (oddziaływania van der Waalsa). Właściwy wybór sposobu prowadzenia badań za pomocą AFM ma istotne znaczenie, gdyż od tego zależy poprawność uzyskanych wyników. Komputer stanowiący część składową AFM musi charakteryzować się dużą szybkością działania i mieć dużą pojemność pamięci.

Programy komputerowe służące do generowania obrazu próbki oraz określania jej właściwości są ciągle doskonałe. Ich opracowywanie wymaga głębokiej wiedzy nie tylko z zakresu matematyki i informatyki, lecz także z fizycznych i chemicznych właściwości badanych materiałów. Ważne są także badania wpływu rodzaju materiału i wymiarów promienia ostrza pomiarowego AFM na siłę działającą między tym ostrzem a badaną próbką. Są również rozwijane procedury badawcze oraz sposoby obliczeń statystycznych stanowiących podstawę określania właściwości struktury geometrycznej powierzchni badanych. Możliwości zastosowania AFM w różnych dziedzinach nauki, techniki i kryminalistyki są bardzo duże. Należą do nich przede

²¹ Angstrom (Å) – jednostka długości równa 10^{-10} m. Służy do liczbowego wyrażania wartości bardzo małych długości, porównywalnych z rozmiarami atomów, za: <https://pl.wikipedia.org/wiki/Angstrom> [dostęp: 3 I 2018] (przyp. red.).

wszystkim badania metali, struktur ceramicznych i krzemowych oraz prowadzone ostatnio na coraz większą skalę badania z biologii. Technika AFM w kryminalistyce jest wykorzystywana m.in. do badań skutków pożaru, a także do badań krwi, włosów, włókien, tekstury papieru oraz głębokości wnikania środków kryjących (tuszy, past długopisowych)²². Można ją też stosować do analizy pozostałości po wystrzale z broni palnej (zdj. 18), m.in. do określania kształtu, wielkości oraz średniej gęstości cząstek wokół otworu wlotowego pocisku²³.



Zdj. 18. Obraz AFM pojedynczych cząstek GSR²⁴.

A.J. Goddard i współpracownicy wykorzystali technikę AFM do badania ukrytych odcisków palców na mosiężnych powierzchniach. Mosiądz jest bardzo popularnym materiałem do produkcji amunicji. AFM w tym przypadku posłużyła do wizualizacji korozji metali w skali nanometrowej między śladami linii papilarnych a metalem po obróbce cieplnej²⁵.

Mikroskop AFM zastosowano również do analiz włókien tekstylnych. Obrazy AFM wykorzystano do ilościowego pomiaru parametrów tekstury powierzchni tkanin narażonych na czynniki środowiskowe (różne rodzaje gleby, woda) w funkcji czasu. Badania wykazały różnicę między uszkodzeniami włókien pod wpływem czynników środowiskowych a uszkodzeniami mechanicznymi²⁶.

²² S. Kasas, A. Khanmy-Vital, G. Dietler, *Examination of Line Crossings by Atomic Force Microscopy*, „Forensic Science International” 2001, nr 119, s. 290–298.

²³ Y. Mou, J. Lakadwar, J.W. Rabalais, *Evaluation of Shooting Distance by AFM and FTIR/ATR analysis of GSR*, „Journal of Forensic Science” 2008, nr 58, s. 1381–1386.

²⁴ Tamże.

²⁵ A.J. Goddard, A.R. Hillman, J.W. Bond, *High Resolution Imaging of Latent Fingerprints by Localized Corrosion on Brass Surfaces*, „Journal of Forensic Sciences” 2010, nr 55, s. 58–65.

²⁶ E. Canetta, K. Montiel, A.K. Adya, *Morphological changes in textile fibres exposed to environmental stresses: Atomic force microscopic examination*, „Forensic Science International” 2009, nr 191, s. 6–14.

Technika AFM została wykorzystana także do wykrywania materiałów wybuchowych. Analizowano między innymi morfologie powierzchni takich substancji, jak: triamino-trinitro-benzen, nadchloran amonu i PBX, w celu dokładniejszego określenia cech charakterystycznych materiałów wybuchowych²⁷.

Możliwości mikroskopu AFM są coraz większe dzięki ciągłemu prowadzeniu prac, zarówno nad konstrukcją samego mikroskopu, jak i podstawami fizycznymi stosowanej metody. Pomimo ciągłego doskonalenia mikroskopu sił atomowych i rozwoju oprogramowania komputerowego, a także nowych osiągnięć z dziedziny podstaw teoretycznych i eksperymentalnych, interpretacja wyników uzyskanych metodą AFM jest wciąż zagadnieniem trudnym i złożonym.

Podsumowanie

Wykorzystanie zaawansowanej technologii do badania materiału dowodowego pozwala na niezwykle dokładną jego analizę. Obejrzenie materiału w dużych powiększeniach jest niezbędne przy wykonywaniu dokumentacji różnych próbek (badaniu morfologii powierzchni, ustalaniu cech diagnostycznych). Zastosowanie mikroskopii optycznej, elektronowej czy sił atomowych oraz zintegrowanych z nimi systemów spektroskopowych jest podstawowym, ale jednocześnie potężnym narzędziem służącym do wykonywania obserwacji różnorodnych materiałów. Mimo swej wysokiej wartości rynkowej i wysokich cen eksploatacyjnych, takie systemy powinny być obecnie urządzeniami dostępnymi w każdym laboratorium kryminalistycznym i powinny być stosowane jako podstawowe urządzenia wykorzystywane rutynowo w ekspertyzach sądowych. Pozwalają one na szybkie wykonanie nieskomplikowanych badań nieniszczących materiału. Dzięki temu w krótkim czasie można uzyskać informacje o badanych próbkach, które można łatwo dalej przetwarzać i wizualizować, wykonując dokumentację fotograficzną, z uwzględnieniem różnych szczegółów budowy, zbadania ich własności optycznych oraz ustalenia ich składu chemicznego. Na podstawie uzyskanych wyników można dokonać wstępnych klasyfikacji materiału dowodowego oraz przekazać go do dalszych badań z użyciem innych wysoko zaawansowanych instrumentów.

²⁷ M. Tourne, *Developments in Explosives Characterization and Detection*, „Journal of Forensic Research” 2013, nr S12, s. 2–10; G.C. Yang i in., *Pang Preparation and Charakterization of nano-TATB Explosive*, „Propellants Explosives, Pyrotechnics” 2006, nr 31, s. 390–394; A. Kumarii in., *Nano-ammonium Perchlorate: Preparation, Characterization and Evaluation in Composite Propellant Formulation*, „Journal of Energetic Materials” 2013, nr 31, s. 192–202; A.E.D.M van der Heijden i in. *Energetic Materials: Crystallization, Characterization and Insensitive Plastic Bonded Explosives*, „Propellants Explosives, Pyrotechnics” 2008, nr 33, s. 25–32.

Bibliografia:

1. Bowden M. i in., *Thermal degradation of polyurethane-backed poly(vinyl chloride) studied by Raman microline focus spektrometry*, „Polymer” 1994, nr 35, s. 1654–1657.
2. Canetta E., Montiel K., Adya A.K., *Morphological changes in textile fibres exposed to environmental stresses: Atomic force microscopic examination*, „Forensic Science International” 2009, nr 191, s. 6–14.
3. Germani M.S., *Evaluation of Instrumental Parameters for Automated Scanning Electron Microscopy/Gunshot Residue Particle Analysis*, „Journal of Forensic Science” 1991, nr 36, s. 331–342.
4. Goddard A.J., Hillman A.R., Bond J.W., *High Resolution Imaging of Latent Fingerprints by Localized Corrosion on Brass Surfaces*, „Journal of Forensic Sciences” 2010, nr 55, s. 58–65.
5. Heijden van der A.E.D.M. i in., *Energetic Materials: Crystallization, Characterization and Insensitive Plastic Bonded Explosives*, „Propellants Explosives, Pyrotechnics” 2008, nr 33, s. 25–32.
6. Kasas S., Khanmy-Vital A., Dietler G., *Examination of Line Crossings by Atomic Force Microscopy*, „Forensic Science International” 2001, nr 119, s. 290–298.
7. Krüsemann H., *SEMs and Forensic Science*, „Problems of Forensic Science” 2001, nr 47, s. 110–121.
8. Kumari A. i in., *Nano-ammonium Perchlorate: Preparation, Charkterization and Evaluation in Composite Propellant Formulation*, „Journal of Energetic Materials” 2013, nr 31, s. 192–202.
9. Łasińska A., *Analiza nieorganicznych i organicznych pozostałości po wystrzale z broni palnej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 16, s. 157–189.
10. Łasińska A., *Badania mikrośladów*, w: *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, B. Hołyst (red. nauk.), Warszawa 2014, Wydawnictwo Naukowe PWN, s. 804–840.
11. Łasińska A., *Skaningowa mikroskopia elektronowa w badaniach kryminalistycznych*, „Prokuratura i Prawo” 2013, nr 10, s. 145–166.
12. Łasińska A. i in., *Ocena przydatności folii adhezyjnych do zabezpieczania śladów biologicznych oraz izolacji komórek ludzkich metodą mikrodyssekcji laserowej*, „Problemy Kryminalistyki” 2014, nr 283, s. 18–28.

13. Łasińska A., Barszcz K., *Ilościowa i jakościowa analiza mieszanin pirotechnicznych SEM/EDS*, „Przeгляд Bezpieczeństwa Wewnętrzneгo” 2014, nr 11, s. 177–205.
14. Łasińska A., Konarowska U., *Zastosowanie mikroskopii optycznej i elektronowej w badaniach autentyczności dokumentów*, w: *Dokumenty a prawo prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, s. 105–112.
15. Mou Y., Lakadwar J., Rabalais J.W., *Evaluation of Shooting Distance by AFM and FTIR/ATR analysis of GSR*, „Journal of Forensic Sciences” 2008, nr 58, s. 1381–1386.
16. Raczkowska A. i in., *Pleiotropic effects of a Yersinia enterocolitiae ompR mutation on adherent-invasive abilities and biofilm formation*, „FEMS Microbiology Letters” 2011, nr 321, s. 43–49.
17. Sharma B. i in., *SERS: Materials, applications, and the future*, „Materials today” 2012, nr 15, s. 16–25.
18. Szczepańczyk S., Konarowska U., *Zastosowanie mikroskopii optycznej w weryfikacji dokumentów przerobionych za pomocą drukarki laserowej*, „Problemy Kryminalistyki” 2012, nr 276, s. 65–73.
19. Tourne M., *Developments in Explosives Characterization and Detection*, „Journal of Forensic Research” 2013, nr S12, s. 2–10.
20. White R.S., Owens A.D. *Automation of Gunshot Residue Detection and Analysis by Scanning Electron Microscopy/Energy Dispersive X-ray Analysis (SEM/EDX)*, „Journal of Forensic Sciences” 1987, nr 32, s. 1595–1603.
21. Yang G.C. i in., *Pang preparation and characterization of nano-TATB explosive*, „Propellants Explosives, Pyrotechnics” 2006, nr 31, s. 390–394.

Abstrakt

W artykule przedstawiono zagadnienia obejmujące różne techniki obrazowania wykorzystywane w kryminalistyce. Rozwój technologii obserwowany we współczesnym świecie pociąga za sobą zmiany we wszystkich dziedzinach życia, usprawniając, przyspieszając oraz otwierając je na nowe możliwości badawcze. Wykorzystanie zaawansowanej technologii pozwala na precyzyjną analizę materiału dowodowego. Możliwość obserwacji różnych próbek w dużych powiększeniach jest niezbędna przy wykonywaniu ich dokumentacji (badanie morfologii powierzchni, ustalanie cech

diagnostycznych). Zastosowanie mikroskopii optycznej, elektronowej lub sił atomowych, a także zintegrowanych z nimi systemów spektroskopowych jest podstawowym, a zarazem potężnym narzędziem służącym wykonywaniu obserwacji różnorodnych materiałów.

Słowa kluczowe: techniki obrazowania, mikroskopia, SEM, mikroanaliza rentgenowska, EDS, spektroskopia Ramana, mikroskopia sił atomowych, AFM.

Podziękowania

W artykule przedstawiono niektóre wyniki badań przeprowadzonych w zakresie pirotechniki oraz badań struktury powierzchni tonera w ramach projektu badawczego Narodowego Centrum Badań i Rozwoju nr 0023/R/ID3/2012/02.

Sławomir Gładysz

Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego

Wejście w życie przepisów ustawy o działaniach antyterrorystycznych¹ wywołało liczne głosy krytyki i spowodowało pojawienie się obaw związanych z przyznanymi służbom, a w zasadzie Agencji Bezpieczeństwa Wewnętrznego, uprawnieniami o charakterze operacyjnym. Te uprawnienia – zdaniem sceptyków regulacji, o której mowa – godzą w prawa i wolności obywatelskie oraz naruszają konstytucyjne zasady ochrony prawa obywatela do swobodnego komunikowania się i prywatności.

Podstawą powyższych twierdzeń jest najczęściej obawa o takie opracowania przepisów prawnych uzasadniających naruszanie przez aparat państwa konstytucyjnie chronionych dóbr, aby pod żadnym pozorem nie zostały one naruszone. Oceny sytuacji dokonuje się przez pryzmat stanu bezpieczeństwa a priori – nikt przy zdrowych zmysłach nie będzie godził w bezpieczeństwo państwa i nie będzie się na nie porywał. Wówczas założenie postawione na początku niniejszego akapitu o niezbywalności pewnych wolności, a nawet braku możliwości ich zawieszenia, byłoby słuszne. Niestety, takie podejście do spraw związanych z bezpieczeństwem graniczy z naiwnością.

Racjonalna i zarazem pragmatyczna postawa w tych sprawach niesie za sobą konieczność wyjścia poza ramy ideałów i przygotowania państwa oraz jego instytucji do działań w sytuacjach najwyższego zagrożenia bądź do przeciwdziałania skutkom już zaistniałych zdarzeń. Te przygotowania powinny obejmować zarówno aspekty formalne i określać podstawy oraz granice działań, jak i rzeczywiste – przez wskazanie, w jaki sposób z tych narzędzi w świetle prawa skorzystać.

W polskim porządku prawnym obowiązują już konstrukcje prawne umożliwiające ograniczenie lub zawieszenie możliwości korzystania z pełni praw obywatelskich w określonych sytuacjach². Przewidują one, że w przypadku zaistnienia szczególnych zagrożeń uniemożliwiających normalne funkcjonowanie instytucji państwowych w trybie zwykłych środków konstytucyjnych, można wprowadzić określony stan nadzwyczajny wiążący się z ograniczeniem wolności i praw człowieka i obywatela.

¹ Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r. poz. 904, ze zm.).

² Są to stany nadzwyczajne, tj.: stan wojenny – Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j.: Dz.U. z 2017 poz. 1932), stan wyjątkowy – Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j.: Dz.U. z 2017 r. poz. 1928) i stan klęski żywiołowej – Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j.: Dz.U. z 2017 r. poz. 1897).

Według autora nieniejszego artykułu do katalogu zdarzeń stwarzających szczególne zagrożenie można dopisać różne stadia zjawisk o charakterze terrorystycznym, z uwzględnieniem tych, które wypełniają znamiona przestępstwa. Uzasadnieniem takiego stanowiska jest m.in. omawiana regulacja dotycząca szeroko pojętych działań antyterrorystycznych³.

Logiczne jest to, że dla ratowania wspólnego „wyższego dobra” jako obywatele będziemy gotowi zrezygnować z określonych atrybutów funkcjonowania w państwie. Co do tego nikt nie ma, a przynajmniej nie powinien mieć, wątpliwości. Powszechne poczucie zagrożenia bezpieczeństwa, jakie jest odczuwane przez obywateli, powoduje elastyczność, dzięki której zastosowanie nawet dolegliwych ograniczeń będzie przez nich akceptowane.

Niezależnie od konieczności wskazania podstaw i granic działania instytucji państwowych przy rozpoznawaniu i zwalczaniu terroryzmu, a także przeciwdziałaniu temu zjawisku argumentem przemawiającym za koniecznością wdrożenia nowych regulacji⁴ jest, zdaniem autora, to, że od długiego czasu instytucje odpowiedzialne za bezpieczeństwo posługują się środkami uznanymi przez ustawodawcę w latach 90. XX w. za skuteczne. Praca operacyjna i procesowa, oparte wówczas na „starych”, sprawdzonych metodach, zostały wsparte „nowymi” rozwiązaniami, tj. możliwością przeprowadzenia kontroli operacyjnej bądź procesowej mobilnych środków łączności, niekoniecznie na określony numer telefonu, ale także na indywidualny numer aparatu telefonicznego (IMEI), oraz możliwością śledzenia widm częstotliwości telekomunikacyjnych itp.

Na przełomie lat 90. XX w. i w początkach XXI w. zdawało się, że powiedzenie „przestępcy są zawsze krok przed nami” może będzie choć na chwilę nieaktualne. Z początkiem tego stulecia podczas prowadzenia jednej ze spraw autor ustalił sposób komunikowania się podejrzanych, którymi byli obywatele sąsiednich krajów. Uzgodnili oni swoisty „system bezpieczeństwa”, który miał ochronić ich działania przed dekonspiracją. Polegał on na używaniu jednej karty SIM maksymalnie przez miesiąc. Jeden aparat telefoniczny obsługiwał nie więcej niż trzy karty SIM i po sześciu miesiącach musiał być zmieniony. To byli prości przestępcy...

Powyższy przykład świadczy o tym, że rozwój techniki, technologii, komunikacji i jej sposobów, zwłaszcza w odniesieniu do globalizacji każdej dziedziny życia, powoduje, że organy powołane do rozpoznawania, przeciwdziałania i zwalczania przestępczości zawsze będą w tyle za przestępcami dążącymi do zachowania hermetyczności swoich środowisk, niejawności połączeń i ukrycia rzeczywistych planów i zamiarów. Pytanie tylko, jak daleko w tyle zostaną.

³ Można podjąć dyskusję, czy przestępczość o charakterze terrorystycznym jest „szczególnym zagrożeniem” mieszczącym się w ramach konstytucyjnego pojęcia wynikającego z art. 228 ust. 1, niemniej jednak wykładania logiczna norm powiązanych przemawia za takim stanowiskiem. Otóż w regulacji dotyczącej stanu wyjątkowego jako przesłankę jego wprowadzenia wskazano m.in. zagrożenie bezpieczeństwa obywateli i porządku publicznego. Należy się zgodzić, że ewentualny zamach terrorystyczny godziłby w te dobra. Kwestią oceną będzie, czy dane zdarzenie o charakterze terrorystycznym może powodować sytuację, w której zwykle środki konstytucyjne będą niewystarczające do przeciwdziałania mu lub jego zwalczania.

⁴ Dostosowanych do nowych czasów, technologii, społeczeństwa itd.

Oczywiście przed 10 czerwca 2016 r. służby nie były bezradne, jeśli chodzi o realizację swoich ustawowych kompetencji, szczególnie w zakresie zapewniania bezpieczeństwa. Jak pokazały różnego rodzaju wydarzenia, działania podejmowane przez służby gwarantują bezpieczeństwo wewnętrzne na określonym, wydaje się – zadowalającym – poziomie, kryterium tej oceny sprowadza się bowiem do zaistnienia zdarzeń o charakterze terrorystycznym. Jednocześnie granica między świadomością obywateli, że bezpieczeństwo to było zapewnione, bo nikt nic nie planował, a świadomością, że określone działania zostały przez służby w odpowiednim momencie zniweczone, a ich potencjalni kontynuatorzy odstraszeni skutecznością służb, jest (a może już była) niewyraźna.

We wstępie przedstawiono dwa zasadnicze punkty widzenia na problematykę związaną z uprawnieniami służb postrzeganych przez pryzmat praw i wolności obywatelskich. Pierwszy odnosi się do dopuszczalności stosowania określonych narzędzi, drugi zaś dotyczy zakresu i sposobów korzystania z nich.

Naświetlenie problematyki związanej z domeną państwa w obszarze bezpieczeństwa, zwłaszcza ochrony przed zagrożeniami o charakterze terrorystycznym, oraz uregulowaniami prawnymi w tym zakresie może rozwiązać wątpliwości co do zasadności wyposażenia organów państwowych w określone instrumenty działania.

Z przeprowadzonej analizy wynika, że regulacje dotyczące tego obszaru wynikają z różnych aktów prawnych, a ich przytoczenie, chociażby sygnałne, być może pozwoli na obiektywną i racjonalną ocenę zapisów ustawy o działaniach antyterrorystycznych.

1. Zagadnienia ogólne

Zgodnie z art. 5 Konstytucji RP⁵ *Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli (...)*. Ta norma określa podstawowe, generalne funkcje państwa oraz jego fundamentalne cele, na które składa się przede wszystkim ochrona terytorium, wolności i bezpieczeństwa obywateli. Wymienione wartości są także podstawą funkcjonowania aparatu państwa, a szczególnie jego instytucji, które zostały powołane do stania na ich straży, niezależnie od źródła potencjalnego zagrożenia.

Dobrami podlegającymi ochronie są przede wszystkim: państwo jako niepodległy podmiot wraz ze swoim terytorium oraz obywatele wraz z ich prawami, tj. najcenniejszy element państwa. Ochrona sprowadza się tu do zapewnienia stanu bezpieczeństwa, czyli do stworzenia takiej sytuacji, w której – niezależnie od poziomu zagrożenia – działania podejmowane przez organy państwa będą cieszyć się zaufaniem obywateli i zrozumieniem niezbędności ich przeprowadzenia, a przy tym prawidłowości i skuteczności. Pojęcie *zapewnienie bezpieczeństwa* wymaga jednak wąskiej interpretacji, powinno być bowiem jedynie pewną reakcją – choć także o charakterze profilaktycznym – na rzeczywiste bądź potencjalne (ale realne) zagrożenia i zamachy⁶.

⁵ *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. nr 78 poz. 483).

⁶ P. Sarnecki, *Artykuł 5*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz I, Wstęp*, art. 29, L. Garlicki, M. Zubik (red. nauk.), Warszawa 2016, s. 234.

Na potrzeby niniejszego artykułu autor skupił się na zdefiniowaniu określenia bezpieczeństwo obywateli. Zgodnie z definicjami *Słownika języka polskiego* bezpieczeństwo rozumie się jako stan niezagrożenia, funkcjonowania w normalnym trybie bez widma groźby wystąpienia określonego zdarzenia, negatywnego w skutkach. Z kolei bezpieczeństwo publiczne to ogół warunków oraz instytucji chroniących państwo i obywateli przed zjawiskami groźnymi dla ładu prawnego oraz ochrona ustroju przed zamachami na podstawowe instytucje polityczne państwa⁷. Ta definicja, wyłączająca ze swojego zakresu osoby niebędące obywatelami, przebywające lub funkcjonujące w strukturach danego państwa, byłaby nieuprawnionym zawężeniem tego pojęcia. „Inne osoby” również podlegają ochronie, także są elementem bezpieczeństwa publicznego.

Zdaniem autora powyższe uprawnienia do twierdzenia, że określenie bezpieczeństwo obywateli jest swoistym *lex specialis* do bezpieczeństwa publicznego, co do którego państwo wzięło na siebie szczególny prawny obowiązek jego strzeżenia.

Kolejnym obowiązkiem państwa wynikającym z art. 5 Konstytucji RP jest zapewnienie wolności oraz praw człowieka i obywatela, które to określenia bezpośrednio prowadzą do rozdziału II Konstytucji RP. Warto tu przytoczyć francuską *Deklarację Praw Człowieka i Obywatela*⁸, a zwłaszcza jej *Artykuł IV* mówiący o tym, że *Wolność polega na możliwości czynienia wszystkiego, co nie szkodzi drugiemu; w ten sposób wykonywanie praw naturalnych każdego człowieka nie ma innych granic niż te, które zapewniają korzystanie z takich samych praw innym członkom społeczeństwa. Granice te może określić tylko ustawa*. Pomimo upływu blisko 230 lat od ogłoszenia tej regulacji, komentarz do jej zapisów jest w zasadzie zbędny.

W polskim prawodawstwie pod pojęciem wolność powszechnie rozumie się sferę tych uprawnień, których prawo nie tworzy, a tylko określa ich granice. W tym przypadku właśnie na państwie ciąży obowiązek udowodnienia, że jednostka naruszyła te granice. Natomiast w przypadku praw, których katalog ustala państwo, to jednostka w toku ich dochodzenia musi się powołać na określoną podstawę prawną⁹. Oznacza to wolność działania człowieka wszędzie tam, gdzie prawo nie wprowadza zakazów. Widać tu całkowite odwrócenie sytuacji istniejącej w odniesieniu do państwa i jego organów. Organ państwa działa tam, gdzie został do tego przez prawo umocowany, i działa z powołaniem się na podstawę prawną. Obywatel zaś może działać wszędzie tam, gdzie ustawa nie wprowadziła zakazów, nie zabroniła mu określonych czynów¹⁰.

Nawiązując do definicji bezpieczeństwa publicznego, w której wskazano jego kwalifikowaną formę odnoszącą się do „obywateli”, również w przypadku wolności ustanowiono uprawnienia generalne dla wszystkich ludzi oraz uprawnienia

⁷ <http://sjp.pwn.pl/slowniki>.

⁸ Tekst *Deklaracji Praw Człowieka i Obywatela z 26 sierpnia 1789 r.* został opublikowany na stronie <http://libr.sejm.gov.pl/tek01/txt/konst/francja-18> [dostęp: 23 I 2017].

⁹ W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, s. 42.

¹⁰ Tamże, s. 45.

ściśle związane z formalną przynależnością państwową. Jest to wynikiem szczególnego zobowiązania państwa do zapewnienia ochrony oraz poczucia bezpieczeństwa, zwłaszcza jego obywatelom, bez pomijania przy tym podstawowych, niezbywalnych praw przynależnych wszystkim ludziom przebywającym na terytorium RP, niezależnie od ich statusu państwowego, narodowościowego, rasowego, religijnego czy politycznego.

Przejawem powyższych rozważań jest art. 31 Konstytucji RP, w którym ustanowiono ochronę prawną wolności człowieka, ale jednocześnie wskazano, kiedy i na jakiej podstawie te prawa i wolności mogą zostać ograniczone. Jest bowiem oczywiste, że prawa, a zwłaszcza wolności, nie mogą być nieograniczone. Przepis art. 31 ust. 3 dostarcza wskazówek, w jaki sposób wyznaczyć granice tych praw oraz jak daleko mogą sięgać dopuszczalne ograniczenia¹¹. Omawiane wskazówki wynikają bezpośrednio z redakcji normy i zgodnie z nimi ograniczenia mogą być ustanawiane w demokratycznym państwie tylko w ustawie i tylko wtedy, gdy są konieczne dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób.

Gwarancje ochrony praw i wolności wprowadzają dwutorowe klauzule ograniczające te prawa i wolności: formalne, ustalające minimalną rangę aktu prawnego¹² konstytuującego ograniczenie, oraz materialne, uzależnione od realizacji przez państwo określonego zadania. Zadania realizowane przez państwo zostały podzielone na trzy grupy obejmujące: bezpieczeństwo i porządek publiczny, środowisko, zdrowie publiczne, moralność publiczną oraz wolność i prawa innych osób. Ograniczenia wprowadzone z powodu którejkolwiek z przyczyn wymienionych w art. 31 nie godzą w zasady demokratycznego państwa prawnego, przeciwnie – są w nim konieczne¹³.

Przy omawianiu norm konstytucyjnych warto zwrócić uwagę na istotny z punktu widzenia art. 31 Konstytucji RP zapis, a mianowicie na art. 37 tego aktu prawnego. Wprowadza on zasadę równego korzystania z wolności i praw konstytucyjnych przez wszystkich ludzi, zarówno obywateli RP, jak i cudzoziemców znajdujących się na obszarze objętym władztwem Rzeczypospolitej.

Cudzoziemcem, zgodnie z ustawą o cudzoziemcach¹⁴, jest każdy, kto nie posiada obywatelstwa polskiego¹⁵, bez względu na to, czy ma jakiegokolwiek obywatelstwo obce (bezpaństwowiec, apatryda). Wyjątki od wskazanej wyżej zasady mogą zostać uregulowane w ustawach¹⁶. Ustawodawca nie wskazał tym samym konkretnego aktu

¹¹ P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Warszawa 2008, s. 48.

¹² Jak już wskazano wyżej, ten akt powinien mieć rangę ustawy, a więc aktu prawnego powszechnie obowiązującego, wydanego przez najwyższy organ prawodawczy w trybie szczególnym i zajmującego wysokie miejsce w strukturze źródeł prawa.

¹³ P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej...*, s. 49.

¹⁴ *Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach* (t.j.: Dz.U. z 2017 r. poz. 2206).

¹⁵ Art. 3 pkt 2 ustawy o cudzoziemcach.

¹⁶ Art. 37 ust. 2 Konstytucji RP.

prawnego, który mógłby wprowadzać ograniczenia w korzystaniu z praw i wolności przez cudzoziemców, ale określił jego rangę i potwierdził¹⁷ konieczność uregulowania tego w drodze ustaw.

Podsumowując, należy stwierdzić, że Konstytucja RP nakłada na państwo szczególnie obowiązek zapewnienia bezpieczeństwa publicznego przy jednoczesnym zagwarantowaniu respektowania wolności oraz praw człowieka i obywatela. Te wolności i prawa mogą być wprawdzie ograniczone, jednak można to uczynić aktem prawnym parlamentu rangi ustawy.

Jedną z przyczyn wprowadzenia ograniczeń praw oraz wolności człowieka i obywatela jest konieczność zapewnienia bezpieczeństwa, w które mogą godzić m.in. zjawiska i zagrożenia o charakterze terrorystycznym. Tego typu zagrożenie jest duże zwłaszcza teraz, kiedy wymyka się tradycyjnie rozumianym definicjom zagrożeń, a potencjalni sprawcy ataków terrorystycznych działają niesablonowo i często obierają za cel przypadkowych ludzi, infrastrukturę lub po prostu chcą dokonać jak największych zniszczeń. Aby temu przeciwdziałać, państwo musi się w sposób kompleksowy przygotować przez wyposażenie właściwych organów w instrumenty i narzędzia umożliwiające podjęcie natychmiastowych i adekwatnych środków reagowania na zagrożenia, a w przypadku dokonania zamachu – także usuwania jego skutków.

Precyzyjne uregulowanie działalności organów państwowych w obliczu zagrożeń terrorystycznych, niezależnie od ich poziomu, powinno być standardem w funkcjonowaniu państw bez względu na środowisko polityczne, z którego wywodzi się obóz rządzący. Skuteczność takich regulacji będzie zależała od bliskiej i wszechstronnej współpracy wszystkich służb, organów oraz instytucji zaangażowanych w szeroko rozumiane działania antyterrorystyczne, przy aprobacie – a można zakładać, że nawet przy wsparciu – środków masowego przekazu, organizacji pozarządowych oraz całego społeczeństwa.

2. Organy właściwe w sprawach z zakresu terroryzmu

W Polsce organami powołanymi wprost z ustawy do zajmowania się szeroko rozumianymi zagadnieniami związanymi z terroryzmem są służby specjalne, tj.: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, a także Żandarmeria Wojskowa i Policja. Główną rolę w rozpoznawaniu i wykrywaniu przestępstw związanych z terroryzmem oraz zapobieganiu im przypisano Agencji Bezpieczeństwa Wewnętrznego, co znajduje odzwierciedlenie w stosownych przepisach kompetencyjnych.

Wprawdzie trudno pominąć inne organy, których działalność na różnych etapach zjawisk związanych z terroryzmem jest nie do przecenienia, jednak ich zadania nie wynikają wprost z przepisów, a raczej z wykładni logicznej bądź systemowej

¹⁷ Patrz: art. 31 ust. 3 Konstytucji RP.

ich uprawnień. Mowa tutaj m.in. o Państwowej Straży Pożarnej¹⁸, Straży Granicznej¹⁹ i Biurze Ochrony Rządu²⁰, jednak ze względu na obszerność tematu autor skupił się na głównych organach powołanych do zajmowania się zjawiskiem terroryzmu i przydzielonych im instrumentach działania.

Przedstawienie zadań związanych ze zwalczaniem terroryzmu oraz narzędzi, w jakie ustawodawca wyposażył organy do realizacji tych zadań, stworzy punkt wyjścia do omówienia i oceny zapisów ustawy o działaniach antyterrorystycznych.

2.1. Agencja Bezpieczeństwa Wewnętrznego

Art. 5 ust. 1 pkt 2 lit. a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu²¹ (dalej: ustawa o ABW oraz AW) wskazuje, że rozpoznawanie i wykrywanie przestępstw, m.in. terroryzmu, oraz zapobieganie im należy do zadań ABW. W tym też zakresie działalność Agencji może być prowadzona zarówno w kraju, jak i poza jego granicami.

Przywołany art. 5 zawiera stosunkowo szerokie ujęcie zadań ABW w zakresie zwalczania przestępczości o charakterze terrorystycznym. Składają się na nie czynności podejmowane na czterech płaszczyznach, które ustawodawca pogrupował w następujące pojęcia²²:

- **rozpoznanawanie** – zgodnie z definicją rozpoznawanie oznacza identyfikację kogoś lub czegoś, badanie oraz podejmowanie działalności mającej na celu zdobycie informacji o przeciwniku²³;
- **wykrywanie** – oznacza ustalenie faktów dotyczących czyjegoś udziału w czymś, ujawnienie rzeczy, które miały mieć charakter niejawni²⁴;

¹⁸ Państwowa Straż Pożarna jest główną służbą odpowiedzialną za prowadzenie akcji ratowniczych w zakresie ratowania życia i zdrowia ludzi oraz ochronę mienia i środowiska w sytuacji powstania nagłego zagrożenia. Do zadań PSP należy podejmowanie czynności z zakresu rozpoznawania zagrożeń, w tym skażeń substancjami chemicznymi i radiacyjnymi, oraz prowadzenie wstępnego rozpoznania biologicznego. Podmioty podejmujące działania ratownicze funkcjonują w ramach Krajowego Systemu Ratowniczo-Gaśniczego. Wszelkie działania ratownicze w czasie zagrożenia o charakterze terrorystycznym są oparte na zachowaniu priorytetu ratowania życia i zdrowia oraz technologii działań służących minimalizacji skutków zdarzenia.

¹⁹ Te działania obejmują m.in. ochronę granicy państwowej, w tym morskiej, organizowanie i dokonywanie kontroli ruchu granicznego oraz zapobieganie nielegalnemu przekraczaniu granicy państwowej i ściganie sprawców tego rodzaju czynów zabronionych. Straż Graniczna realizuje również działania w zakresie zapewniania bezpieczeństwa w komunikacji międzynarodowej, w tym na pokładach statków powietrznych wykonujących przewozy lotnicze pasażerów.

²⁰ Biuro Ochrony Rządu (od 1 II 2018 r. Służba Ochrony Państwa – przyp. red.) jest właściwe w zakresie ochrony ustawowo określonych osób, obiektów i urzędzeń, które mogą stać się potencjalnym celem zamachów terrorystycznych.

²¹ *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2016 r. poz. 1897).

²² Być może są one oczywiste, ale w kontekście zasadniczego celu niniejszego artykułu, tj. analizy ustawy o działaniach antyterrorystycznych, warto zdefiniować ich podstawy znaczeniowe.

²³ <http://sjp.pwn.pl/szukaj/rozpoznanawanie.html> [dostęp: 23 I 2017].

²⁴ <http://sjp.pwn.pl/szukaj/wykrywanie.html> [dostęp: 23 I 2017].

- **z a p o b i e g a n i e** – podejmowanie działań, których celem jest niedopuszczenie do czegoś złego²⁵.

Ustawodawca wskazał dodatkowo, że ABW ma obowiązek ścigania sprawców przestępstw pozostających w jej właściwości rzeczowej. To oznacza, że Agencja Bezpieczeństwa Wewnętrznego ma możliwość wykorzystania swoich materiałów operacyjnych²⁶. Jest to ważne na etapie współpracy operacyjnej i procesowej, często bowiem funkcjonariusze z określonych pionów mogą pozwolić sobie na prowadzenie swobodnego dialogu i luźną, niesformalizowaną wymianę uwag, m.in. dotyczących potrzeb zmierzających do wytyczenia właściwych kierunków zarówno danej sprawy operacyjnej, jak i prowadzonego postępowania karnego.

Wskazane zadania sprowadzają się do identyfikacji zagrożenia, potwierdzenia jego zaistnienia oraz podjęcia działań prewencyjnych i procesowych, które mogą występować zarówno pojedynczo, jak i kumulatywnie. Modelowe byłoby posiadanie takich możliwości operacyjno-analitycznych, dzięki którym proces rozpoznania byłby najszybszy, najskuteczniejszy i najtrafniejszy. Od niego bowiem zależą dalsze działania o charakterze operacyjnym oraz czynności podejmowane w ostatniej fazie procesowej.

Rozpoznanie daje przewagę, czas i możliwości do podjęcia skutecznych i adekwatnych reakcji na określone zagrożenie. Kolejny etap – wykrywanie – jest konsumpcją działań identyfikacyjnych. Na tym etapie ABW potwierdza istnienie uzasadnionego podejrzenia o popełnieniu przestępstwa. Wtedy też następuje weryfikacja zgromadzonego materiału operacyjnego oraz jego ewentualna waloryzacja procesowa. W zależności od rodzaju stwierdzonego zagrożenia, jego skali i aktualności, dalsze działania ABW mogą przybrać formę reakcji adekwatnej do zagrożenia, mającej na celu jego zniwelowanie lub zlikwidowanie. Może to być osiągnięte zarówno przez dynamiczne użycie środków siłowych²⁷, jak i długofalowych działań o charakterze prewencyjnym. Podejmując jednak omawiane działania, należy uwzględnić ich potencjalne zakończenie, tj. albo nie dopuścić do eskalacji zidentyfikowanego zagrożenia, albo zgromadzić materiały uzasadniające ujęcie potencjalnych sprawców i skierowanie aktu oskarżenia.

Zgodnie z art. 21 ustawy o ABW oraz AW podczas realizacji ustawowych zadań m.in. z zakresu przestępstw o charakterze terrorystycznym funkcjonariusze wykonują czynności analityczno-informacyjne, operacyjno-rozpoznawcze i dochodzeniowo-śledcze. Ten podział, pomimo istotnej dyferencji i zależności tych czynności, ma zasadnicze znaczenie wpływające na finalny obraz działań ABW. Sprowadza się on do stwierdzenia, że im lepsza baza informacyjna zgromadzona na etapie operacyjno-rozpoznawczym, tym trafniejsze hipotezy śledcze i skuteczniejsze czynności procesowe²⁸.

²⁵ <http://sjp.pwn.pl/szukaj/zapobieganie.html> [dostęp: 23 I 2017].

²⁶ Autor spotkał się z licznymi głosami przedstawicieli innych służb nieposiadających tych możliwości, wskazującymi na to, że śledztwa prowadzone na podstawie ich materiałów operacyjnych nie miały właściwego wsparcia operacyjnego, co przekładało się na niezadowalające rezultaty procesowe.

²⁷ Dlatego, zdaniem autora, tak ważna jest możliwość ich zastosowania przez pion postępowań karnych, ewentualnie bezpośrednio na polecenie szefa ABW.

²⁸ Ciekawe, że nie jest to oczywiste dla funkcjonariuszy.

To spowodowało, że ustawodawca przyznał funkcjonariuszom ABW uprawnienia procesowe Policji wynikające z przepisów kodeksu postępowania karnego²⁹. Znaczenie tego zapisu wskazano już na wstępie niniejszego rozdziału. Jest on systemowo powiązany z art. 22a ust. 3 ustawy o ABW oraz AW, który wskazuje, że jeżeli informacje zgromadzone przez ABW wskazują na uzasadnione podejrzenie popełnienia przestępstwa lub przestępstwa skarbowego albo potwierdzają jego popełnienie, szef ABW przedstawia je właściwemu prokuratorowi w celu podjęcia decyzji co do ich dalszego procesowego wykorzystania. Z powyższych zapisów można domniemywać, że w przypadku przydatności danego materiału operacyjnego do wszczęcia śledztwa³⁰, którego przedmiot pozostaje we właściwości rzeczowej ABW, prokuratura, rozważając decyzje o powierzeniu śledztwa danemu organowi, w pierwszej kolejności powinna brać pod uwagę właśnie Agencję Bezpieczeństwa Wewnętrznego.

Od zasady wyrażonej w art. 22a ust. 3 ustawy o ABW oraz AW ustawodawca przewidział wyjątek. Jeżeli ABW zgromadzi materiały m.in. uprawdopodobniające działalność o charakterze terrorystycznym, szef ABW może, w przypadku gdy jest to uzasadnione względami bezpieczeństwa państwa, odstąpić od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia tego przestępstwa oraz o osobie, która według uzyskanych informacji lub materiałów może być sprawcą tej działalności³¹.

Kolejna jednostka redakcyjna wprowadziła prawną możliwość³² podjęcia współpracy z osobą podejrzaną o przestępstwa o charakterze terrorystycznym. Jej warunkiem jest świadome i dobrowolne ujawnienie wszelkich okoliczności popełnionego czynu lub prowadzonej działalności oraz jednoczesne zobowiązanie do podjęcia niejawniej współpracy z ABW³³. Decyzja szefa ABW o odstąpieniu od obowiązku poinformowania właściwej prokuratury w takim przypadku musi zostać zaopiniowana przez prokuratora generalnego i członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych³⁴. Wyjątki, o których mowa, są pierwszymi wymienionymi w ustawie narzędziami, jakimi może posłużyć się ABW w realizacji swoich zadań, a zwłaszcza w zakresie rozpoznawania i wykrywania przestępstw o charakterze terrorystycznym oraz zapobiegania im.

²⁹ Art. 21 ust. 3 ustawy o ABW oraz AW.

³⁰ Zgodnie z art. 303 kpk, czyli jeżeli zachodzi uzasadnione podejrzenie popełnienia przestępstwa z określeniem czynu będącego przedmiotem ewentualnego postępowania oraz jego kwalifikacji prawnej.

³¹ Art. 22b ust. 1 ustawy o ABW oraz AW dodany ustawą o działaniach antyterrorystycznych. Tego wyjątku nie da się zastosować, gdy osoba podejrzana o działalność terrorystyczną popełniła przestępstwo przeciwko życiu lub zdrowiu, których skutkiem była śmierć człowieka lub ciężki uszczerbek na zdrowiu, współdziałała w popełnieniu takiego przestępstwa lub nakłaniała do jego popełnienia. Dotyczy to również osoby, która nie ujawniła wszystkich posiadanych danych oraz która – niezgodnie z warunkami współpracy – w dalszym ciągu prowadzi działalność na szkodę RP lub popełniła jedno z wyżej wymienionych przestępstw, pomimo podjęcia tajnej współpracy.

³² Takiej możliwości brakowało w zasadzie od początku działalności i w UOP, i w ABW, zarówno na płaszczyźnie kontrwywiadowczej, jak i terrorystycznej.

³³ Pojawia się tutaj pytanie, w jaki sposób miałyby to nastąpić – na zasadach „oferenctwa” czy też po identyfikacji takiej osoby i przedstawieniu jej przez funkcjonariuszy oferty na zasadzie: „albo dobrowolnie współpracujesz, albo będziemy cię ścigać”.

³⁴ Art. 22b ust. 4 ustawy o ABW oraz AW.

Jak już wspomniano, ustawodawca wyraźnie określił, co państwo, a w tym przypadku reprezentujący je funkcjonariusze, może wykonać, realizując zadania wyznaczone Agencji Bezpieczeństwa Wewnętrznego. Analiza przyznaných uprawnień wskazuje na ich podział na uprawnienia o charakterze administracyjno-porządkowym³⁵, operacyjnym oraz procesowym³⁶. Z uwagi na cel niniejszego opracowania, jakim jest omówienie przepisów ustawy o działaniach antyterrorystycznych, autor ograniczył się do wskazania zasadniczych czynności operacyjnych służących zwalczaniu przestępczości terrorystycznej, w które ustawodawca wyposażył ABW. Oprócz wcześniej opisanej możliwości podjęcia współpracy z osobą podejrzaną o udział w przestępczości terrorystycznej, są nimi:

- zarządzenie uniemożliwienia telekomunikacji,
- zarządzenie zablokowania dostępności określonych danych informatycznych w systemie teleinformatycznym,
- przeprowadzenie oceny bezpieczeństwa systemu teleinformatycznego,
- zarządzenie kontroli operacyjnej,
- gromadzenie, także niejawnie, wszelkich danych osobowych,
- korzystanie z informacji stanowiących tajemnicę bankową oraz informacji dotyczących umów o rachunek papierów wartościowych, umów o rachunek pieniężny, umów ubezpieczenia lub innych umów dotyczących obrotu instrumentami finansowymi, świadczenia usług płatniczych lub zawieranych z uczestnikami funduszy inwestycyjnych,
- niejawne nabycie lub przejęcie przedmiotów pochodzących z przestępstwa,
- zarządzenie niejawnego nadzoru nad wytwarzaniem, przemieszczaniem, przechowywaniem i obrotem przedmiotami przestępstwa,
- korzystanie z pomocy osób niebędących funkcjonariuszami ABW.

Pierwsze z wymienionych uprawnień, tj. uniemożliwienie telekomunikacji³⁷, jest odpowiedzią na wysoki poziom zagrożenia na określonym obszarze. Zostały one wymienione w normie kompetencyjnej Agencji Bezpieczeństwa Wewnętrznego. Są nimi: zagrożenia bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego, a także przestępstwa najpoważniejsze i najbardziej zagrażające państwu. Pomimo tak szerokiego ujęcia możliwości skorzystania z udaremnienia komunikacji, autor artykułu jest zdania, że logicznie ogranicza się ono do sytuacji wyjątkowych, tj. do wystąpienia szczególnego, kwalifikowanego zagrożenia. Może nim być np. zamach na konstytucyjne organy państwa czy próba dokonania zamachu terrorystycznego. Wówczas, np. w przypadku zamachu terrorystycznego, uniemożliwienie telekomunikacji staje się narzędziem, dzięki któremu można zyskać na czasie w celu zmobilizowania sił i środków, a następnie skierowania ich w rejon

³⁵ Wydawanie poleceń dotyczących określonego zachowania się, legitymowanie, kontrola osobista, fotografowanie, daktyloskopowanie, użycie broni i środków przymusu bezpośredniego.

³⁶ Ich źródłem jest kodeks postępowania karnego oraz przepisy okołoprocesowe wynikające z wewnętrznej, obowiązującej w pionie postępowań przygotowawczych, „instrukcji śledczej”.

³⁷ Art. 26a ust. 1 ustawy o ABW oraz AW.

przeprowadzania czynności służbowych. Nietrudno sobie wyobrazić, że wykorzystanie tego uprawnienia może ograniczyć eskalację przestępczych działań godzących w bezpieczeństwo publiczne oraz zmniejszyć potencjalne zniszczenia.

Zastosowanie uprawnienia, o którym mowa powyżej, zarządza szef ABW, określając obszar działania i przekazując informację na ten temat prezesowi Urzędu Komunikacji Elektronicznej. Znamienny jest tutaj brak precyzyjnego wskazania okresu, na jaki może zostać wydane takie zarządzenie. Ustawodawca posłużył się w ustawie nieostrym sformułowaniem: „na czas niezbędny do wykonania czynności”, co wynika z nieprzewidywalności takiej sytuacji, w której konieczne stałoby się uniemożliwienie komunikacji. Granicą tych działań jest ich stosowanie z uwzględnieniem minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

Wyżej opisane działania wiążą się z możliwością zablokowania w systemie teleinformatycznym dostępności określonych danych lub usług, które są związane ze zdarzeniem o charakterze terrorystycznym³⁸. Odbyna się to na wniosek szefa ABW o zastosowanie blokady dostępności w celu „zapobiegania, przeciwdziałania i wykrywania przestępstw (...) oraz ścigania ich sprawców”³⁹ złożony do Sądu Okręgowego w Warszawie, który podejmuje decyzje w tym zakresie.

Nadanie wnioskowi biegu formalnego jest uwarunkowane uzyskaniem pisemnej zgody wydanej przez prokuratora generalnego. Omawianą możliwość obwarowano koniecznością niezwłocznego zastosowania. W takiej sytuacji szef ABW może zarządzić blokadę dostępności danych lub usług, jednak musi uzyskać na to pisemną zgodę prokuratora generalnego oraz złożyć jednocześnie wniosek do sądu o jej zatwierdzenie. W sytuacji niez uzyskania zgody sądu w terminie pięciu dni od zastosowania blokady dostępności, zaprzestaje się działań w tym zakresie. Blokadę zarządza się na okres nie dłuższy niż 30 dni, z możliwością jednorazowego przedłużenia do trzech miesięcy.

Przy pomocy innego narzędzia z zakresu systemów teleinformatycznych będących w dyspozycji szefa ABW ustanowiono także możliwość przeprowadzenia o c e n y b e z p i e c z e ń s t w a tych systemów, polegającej na sprawdzeniu zabezpieczeń przed atakami, które mogą mieć wpływ na integralność, poufność, rozliczalność oraz dostępność tych systemów⁴⁰. Co ciekawe, ustawodawca wyposażył ABW w możliwość wytwarzania i pozyskiwania urządzeń lub programów komputerowych, o których mowa w art. 269b kk⁴¹, oraz ich stosowania.

³⁸ Art. 32c ust. 1 ustawy o ABW oraz AW.

³⁹ Autor celowo ujął fragment tekstu ustawy w cudzysłów, ponieważ uważa, że wdarła się tutaj nieścisłość legislacyjna. Zgodnie z art. 5 ust 1 pkt 2 do zadań ABW należy „(...) rozpoznawanie, zapobieganie i wykrywanie przestępstw (...)”. Przeciwdziałanie jest nową, kolejną formą zadań, jakie reguluje ustawa o działaniach antyterrorystycznych, ale o tym dalej.

⁴⁰ Art. 32a ust. 1 i 6 ustawy o ABW oraz AW.

⁴¹ Jest to o tyle nieprecyzyjne, że wskazana norma kodeksu karnego dotyczy niszczenia, uszkodzenia, usuwania lub zmiany danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, albo zakłócania lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Można się

Kontrola operacyjna polega na uzyskiwaniu i utrwalaniu: treści rozmów prowadzonych przy użyciu środków technicznych, w tym sieci telekomunikacyjnych; obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; treści korespondencji, w tym korespondencji prowadzonej za pośrednictwem środków komunikacji elektronicznej; danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych, a także uzyskiwaniu dostępu do przesyłek i kontroli ich zawartości⁴².

To uprawnienie zostało dostosowane do realiów po latach dyskusji na ten temat. Kontrola operacyjna daje szerokie możliwości ingerowania w czyjąś prywatność, ale przede wszystkim należy założyć, że to organy państwa stoją na straży praworządności. Hipoteza, z jaką autor spotkał się przy okazji wprowadzania konstrukcji „zgody następczej”, mówiąca o tym, że „łatwo sobie wyobrazić, że funkcjonariusz nielegalnie korzysta z bezprawnie uzyskanych danych” jest, zdaniem autora, niedopuszczalna. Zasadą jest korzystanie z przyznanych uprawnień zgodnie z ich przeznaczeniem, po spełnieniu określonych przesłanek i przy zachowaniu kryterium najwyższej staranności. Dotychczasowe doświadczenia autora zdobyte podczas służby w ABW pozwalają na stwierdzenie, że takie właśnie standardy, często nawet jeszcze bardziej obostrzone, obowiązują na co dzień przy stosowaniu uprawnienia wynikającego z art. 27 ustawy o ABW oraz AW. Parafrazując cytowane zdanie, trudno sobie wyobrazić, aby funkcjonariusz bezprawnie wykorzystywał informacje uzyskane w trakcie kontroli operacyjnej⁴³.

W celu realizacji zadań związanych z rozpoznawaniem, wykrywaniem i zapobieganiem przestępczości, m.in. o charakterze terrorystycznym, sąd, na pisemny wniosek szefa ABW złożony po uzyskaniu pisemnej zgody prokuratora generalnego, może w drodze postanowienia zarządzić kontrolę operacyjną⁴⁴. Dodatkową okolicznością wymaganą przy wnioskowaniu o tego typu kontrolę jest bezskuteczność albo nieprzydatność innych środków pracy operacyjnej.

Wnioski o zastosowanie kontroli operacyjnej wymagają dwuetapowej weryfikacji. W pierwszej kolejności wniosek szefa ABW musi być zaaprobowany przez prokuratora generalnego, który powinien przekazać swoje stanowisko w formie pisemnej.

domyślić, że chodzi raczej o symulację ewentualnych skutków, ale ustęp 8 art. 32 ustawy o ABW oraz AW zawiera stwierdzenie: „(...) uzyskać dostęp do informacji (...), przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie”, co z kolei mogłoby sugerować bardziej ofensywne działania.

⁴² Art. 27 ust. 6 ustawy o ABW oraz AW.

⁴³ Aby nie idealizować, nie można również wykluczyć sytuacji naruszenia tej zasady, ale w formie wyjątków ją potwierdzających. Powszechnie uważa się, że materiały operacyjne, szczególnie z podsłuchów, są sensacyjne, odkrywają najbardziej skryte tajemnice i trzymają w napięciu od samego początku do samego końca. Życie jest jednak bardziej prozaiczne i ukazuje świat sensacyjnych podsłuchów jako żmudną, męczącą i obciążającą psychicznie i fizycznie pracę, z której potencjalny uzysk informacyjny wymaga przesłuchania, spisania i zweryfikowania ogromnych ilości danych.

⁴⁴ Art. 27 ust. 1 ustawy o ABW oraz AW.

Dopiero taka legitymacja upoważnia szefa ABW do wystąpienia z wnioskiem do sądu, który może zarządzić kontrolę operacyjną lub odmówić jej zastosowania, o ile uzna, że materiały operacyjne nie dają ku temu podstaw.

Istnieje także możliwość działania w trybie niecierpiącym zwłoki. Zgodnie z art. 27 ust. 3 ustawy o ABW oraz AW w sytuacji niebezpieczeństwa utraty informacji lub zatarcia albo zniszczenia dowodów przestępstwa to szef ABW może zarządzić kontrolę operacyjną. Jednak i tutaj istnieje obowiązek uzyskania pisemnej zgody prokuratora generalnego przed zarządzeniem takiej czynności oraz równoczesne wystąpienie do sądu o wydanie postanowienia w tej sprawie⁴⁵.

Jak już wcześniej wskazano, kontrola operacyjna stwarza wiele możliwości, m.in.: zastosowanie podsłuchu telefonicznego, podglądu oraz podsłuchu wnętrza pomieszczeń⁴⁶ i pojazdów⁴⁷, kontroli korespondencji, w tym korespondencji elektronicznej, uzyskiwanie i utrwalanie danych na nośnikach elektronicznych, a także uzyskiwanie dostępu do zawartości przesyłek oraz ich kontrolowanie. Mimo że niektóre z wymienionych rodzajów kontroli operacyjnej nie są jeszcze w sposób kompletny opisane (określone) w przepisach prawa, to odnoszą się do możliwości prześledzenia aktywności osoby będącej w orbicie zainteresowań ABW w aspekcie wielowymiarowym: od jej poruszania się tradycyjnymi środkami komunikacji do aktywności w sieci Internet i korzystania z elektroniki osobistej. W dobie globalizacji usług internetowych nie zawsze występuje kompatybilność przepisów różnych państw, które są związane z dostępem organów ścigania do danych, do jakich polskie prawo je upoważniło. Niemniej jednak przynajmniej polskie przepisy zostały w dużej części uregulowane⁴⁸.

Przy omawianiu kontroli operacyjnej należy wspomnieć o możliwości Agencji Bezpieczeństwa Wewnętrznego w zakresie uzyskiwania i przetwarzania danych⁴⁹ dotyczących wykazów połączeń (m.in. bilingów⁵⁰), przesyłek pocztowych⁵¹,

⁴⁵ Jeżeli w ciągu pięciu dni od zarządzenia kontroli operacyjnej sąd nie udzieli na nią zgody, szef ABW wstrzymuje stosowaną kontrolę operacyjną, a dotychczasowe materiały są komisyjnie niszczone.

⁴⁶ Odmiennie niż w regulacji zawartej w art. 23 ust. 1 pkt 6 ustawy o ABW oraz AW te czynności dotyczą pomieszczeń prywatnych.

⁴⁷ Choć w dalszym ciągu brakuje przepisów wykonawczych.

⁴⁸ Wprawdzie zdarzają się jeszcze nieporozumienia z polskimi dostawcami usług internetowych, ale dotychczasowa praktyka i współpraca zwiększa poziom zrozumienia.

⁴⁹ Art. 28 ust. 1 oraz art. 34 ust. 1 ustawy o ABW oraz AW.

⁵⁰ Przede wszystkim dotyczy danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego: inicjującego połączenie; do którego kierowane jest połączenie; określenia daty i godziny połączenia oraz czasu jego trwania; rodzaju połączenia; lokalizacji telekomunikacyjnego urządzenia końcowego – art. 180c i 180 d *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (t.j.: Dz.U. z 2017 r. poz. 1907).

⁵¹ Dotyczy danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających: identyfikację korzystających z tych usług; udostępniania przesyłek pocztowych w celu kontroli treści korespondencji lub zawartości przesyłek; udostępniania zatrzymanej przez operatora przesyłki pocztowej w przypadku podejrzenia, że stanowi przedmiot przestępstwa do oględzin przez uprawnione podmioty; dopuszczenia do dalszego przewozu przesyłki pocztowej zawierającej przedmioty przestępstwa w stanie nienaruszonym lub po ich usunięciu albo zastąpieniu

danych internetowych⁵² oraz wszelkich danych osobowych⁵³ osób pozostających w kręgu zainteresowań ABW, wynikających z realizacji zadań wymienionych w art. 5 ustawy o ABW oraz AW. Również w tych przypadkach, zwłaszcza dotyczących danych telekomunikacyjnych, internetowych i pocztowych, wprowadzono sądową kontrolę podstaw ich uzyskiwania. Oznacza to, że sąd może zapoznać się z materiałami uzasadniającymi udostępnienie ABW takich danych⁵⁴.

Zakres informacji, do jakich Agencja Bezpieczeństwa Wewnętrznego została upoważniona, w ostatnim czasie został poszerzony o dane z zakresu tajemnicy bankowej oraz informacji pochodnych⁵⁵. Przesłanką wniosku o ich uzyskanie jest dążenie do skutecznego zapobieżenia przestępstwom określonym w art. 5 ust. 1 pkt 2 lub ich wykrycie albo ustalenie ich sprawców i uzyskanie dowodów w tym zakresie. Procedura udostępnienia wyżej wymienionych danych wymaga akceptacji Sądu Okręgowego w Warszawie, który w postanowieniu powinien określić ich rodzaj, zakres oraz podmiot zobowiązany do ich udostępnienia⁵⁶. Trzeba jednak zaznaczyć, że szef ABW w terminie 120 dni od uzyskania wnioskowanych danych jest zobowiązany do poinformowania o tym podmiotu, o którego dane się zwraca. W przypadkach, w których mogłoby to zaszkodzić wynikom podjętych czynności operacyjno-rozpoznawczych⁵⁷, sąd na wniosek szefa ABW może odroczyć ten termin⁵⁸. Przekazanie informacji o uzyskaniu danych dotyczących tajemnicy bankowej lub jej pochodnych podmiotowi, wobec którego jest prowadzone rozpoznanie operacyjne, zostało uzależnione również od zgromadzenia materiałów uzasadniających wszczęcie postępowania karnego bądź braku ich zgromadzenia⁵⁹. W sytuacji zgromadzenia materiałów taką informację przekazuje prokurator (lub na jego polecenie szef ABW) – przed zamknięciem śledztwa lub niezwłocznie po jego umorzeniu, natomiast w sytuacji braku takich materiałów – niezwłocznie, po postanowieniu właściwej prokuratury o odmowie wszczęcia śledztwa.

w całości lub w części zgodnie z zasadami i trybem określonym w przepisach odrębnych – art. 82 ust. 1 pkt 1 *Ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe* (t.j.: Dz.U. z 2017 r. poz. 1481).

⁵² Zwłaszcza: nazwisk oraz imion usługobiorcy; numeru PESEL lub gdy ten numer nie został nadany – numeru paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość; adresu zameldowania na pobyt stały, ewentualnie adresu do korespondencji; danych służących do weryfikacji podpisu elektronicznego usługobiorcy – art. 18 ust. 1–5 *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz.U. z 2017 r. poz. 1219).

⁵³ Szczególnie: numerów PESEL oraz danych ujawniających pochodzenie rasowe lub etniczne; poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej; danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym – art. 27 i 28 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz.U. z 2016 r. poz. 922).

⁵⁴ Art. 28a ust. 3 ustawy o ABW oraz AW.

⁵⁵ Art. 34a ust. 1 ustawy o ABW oraz AW.

⁵⁶ Art. 34a, ust. 6 ustawy o ABW oraz AW.

⁵⁷ Konieczne jest uprawdopodobnienie tego niebezpieczeństwa.

⁵⁸ Art. 34a ust. 9 i 10 ustawy o ABW oraz AW.

⁵⁹ Art. 34a, ust. 11 i 12 ustawy o ABW oraz AW.

W przypadku uzyskania wiarygodnych informacji o przestępstwie pozostającym we właściwości rzeczowej ABW ten organ może przedsięwziąć czynności operacyjne polegające na niejawnym nabyciu lub przejęciu przedmiotów pochodzących z przestępstwa lub których wytwarzanie, posiadanie, przewożenie oraz którymi obrót są zabronione. Dotyczy to także kontrolowanego przyjęcia i wręczenia korzyści majątkowej⁶⁰. Te czynności nie mogą polegać na kierowaniu wykonaniem opisywanej czynności, będą natomiast zmierzały do wykrycia sprawców i zgromadzenia bezpośrednich dowodów przestępstwa.

Zarządzenie powyższych działań leży w gestii szefa ABW, po uzyskaniu pisemnej zgody prokuratora generalnego. Szef Agencji jest także adresatem materiałów operacyjnych w sytuacji potwierdzenia informacji o rozpoznawanym przestępstwie.

W podobnym trybie, jak w wyżej opisanym, a więc po uzyskaniu zgody prokuratora generalnego, może być zarządzane niejawne nadzorowanie wytwarzania, przemieszczania i przechowywania przedmiotów przestępstwa oraz obrotu nimi⁶¹. Warunkiem jest niedopuszczenie do zagrożenia życia lub zdrowia ludzkiego. W tym przypadku ustawodawca zobligował organy państwa (zwłaszcza organy celne i Straż Graniczną) oraz instytucje świadczące usługi w zakresie poczty i transportu do ścisłej współpracy z ABW.

Na uwagę zasługuje tutaj także wywodząca się z zasady *argumentum a maiori ad minus* możliwość stosowania kontroli operacyjnej zarówno przy „niejawnym nabyciu”, jak i przy „przesyłce nadzorowanej”⁶². Wynika to tego, że realizowanie wymienionych czynności jest podyktowane wysokim prawdopodobieństwem zaistnienia przestępstwa oraz koniecznością nadzoru nad uczestnikami takich działań. Pozwala to także na wielostronne uzyskanie dowodów potwierdzających źródła inspiracji przestępczych działań bądź motywację sprawców, a nierzadko – rzeczywistych mocodawców oraz inicjatorów takich transakcji.

Całość wymienionych narzędzi łączy praca z osobami⁶³ udzielającymi pomocy funkcjonariuszom w realizacji zadań ABW. Jest to podstawa, na której powinna być budowana zdolność informacyjna danej służby. Jednak paradoksalnie jest ona przez „młodych” funkcjonariuszy niedoceniana, przez „starych” zaś – przeceniana. Siła tej metody pracy operacyjnej tkwi w jej pozornej prostocie i bezpośredniości uzyskiwania informacji. Dochodzą tu także szerokie możliwości modyfikowania i planowania tej formy pracy: od działań jednostkowych, konkretnych, do długofalowych przedsięwzięć obejmujących liczne zagadnienia.

Z przedstawionych narzędzi pracy funkcjonariusze mogą korzystać przy rozpoznawaniu i wykrywaniu przestępstw m.in. o charakterze terrorystycznym oraz zapobieganiu im.

Do powyższego dochodzą jeszcze uprawnienia analityczno-informacyjne oraz koordynacyjne ABW. Kwintesencją uprawnień koordynacyjnych jest treść art. 40

⁶⁰ Art. 29 ust. 1 ustawy o ABW oraz AW.

⁶¹ Art. 30 ust. 1 ustawy o ABW oraz AW – na zasadach określonych w art. 27.

⁶² Art. 31 ustawy o ABW oraz AW.

⁶³ Art. 36 ust. 1 ustawy o ABW oraz AW.

ustawy o ABW oraz AW wskazująca, że to (...) *Szef ABW koordynuje podejmowane przez służby specjalne czynności operacyjno-rozpoznawcze mogące mieć wpływ na bezpieczeństwo państwa.*

2.2. Agencja Wywiadu

Zgodnie z art. 6 ust. 1 pkt 5 i pkt 7a ustawy o ABW oraz AW do zadań Agencji Wywiadu należy: (...) *rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej, a także (...) rozpoznawanie, przeciwdziałanie i zapobieganie zdarzeniom o charakterze terrorystycznym wymierzonym przeciwko obywatelom lub mieniu Rzeczypospolitej Polskiej poza granicami państwa, z wyłączeniem zdarzeń o charakterze terrorystycznym wymierzonych przeciwko personelowi lub mieniu Sił Zbrojnych Rzeczypospolitej Polskiej.*

Oprócz przywołanych i zdefiniowanych już wcześniej (przy okazji omawiania zakresu zadań ABW) pojęć *rozpoznawanie i zapobieganie zdarzeniom terrorystycznym* lub zdarzeniom o takim charakterze Agencja Wywiadu podejmuje także czynności w celu przeciwdziałania im.

Przeciwdziałanie to, zgodnie z definicją, zapobieganie czemuś negatywnemu przez działanie w określony sposób⁶⁴. To działanie – przez pryzmat zadań Agencji Wywiadu – będzie zmierzać do zgromadzenia informacji oraz analizowania ich pod kątem ewentualnego przekazania lub wykorzystania przez inne organy.

Znamieniem kwalifikującym właściwość AW jest narażenie bezpieczeństwa obywateli RP lub polskiego mienia poza granicami Polski. W ramach powyższego funkcjonariusze Agencji Wywiadu podejmują czynności operacyjno-rozpoznawcze i analityczno-informacyjne.

O ile uprawnienia o charakterze administracyjno-porządkowym oraz czynności o charakterze stricte informacyjnym⁶⁵ są wspólne dla obydwu omawianych Agencji, o tyle w przypadku AW możliwości realizowania czynności operacyjnych są ograniczone. Co więcej, działania operacyjne o charakterze „ofensywnym”⁶⁶ na terytorium RP są dopuszczalne, ale (...) *wyłącznie za pośrednictwem Szefa ABW*⁶⁷.

Z powyższych uprawnień na pierwszy plan wysuwa się obowiązek wszystkich organów administracji rządowej w zakresie informowania szefa Agencji Wywiadu o wydarzeniach istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej, szczególnie dotyczących międzynarodowego terroryzmu i ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej⁶⁸.

⁶⁴ <http://sjp.pwn.pl/szukaj/przeciwdzialanie.html>.

⁶⁵ Zgodnie z rolą, jaką AW ma odgrywać. Są nimi: gromadzenie, także niejawnie, wszelkich danych osobowych.

⁶⁶ Czyli: kontrolę operacyjną, niejawnie nabycie lub przejęcie przedmiotów oraz niejawnie nadzorowanie wytwarzania, przemieszczania i przechowywania przedmiotów przestępstwa oraz obrotu nimi.

⁶⁷ Art. 6 ust. 3 ustawy o ABW oraz AW.

⁶⁸ Art. 41 ust. 1 pkt 3 ustawy o ABW oraz AW.

2.3. Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego

Art. 5 ust. 1 pkt 2a oraz następny, art. 6 ust. 1 pkt 2b oraz ust. 3a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego⁶⁹ (dalej: ustawa o SKW oraz SWW) wskazują na zadania tych służb w zakresie zwalczania terroryzmu.

W przypadku SKW te zadania obejmują rozpoznawanie i wykrywanie zdarzeń oraz przestępstw o charakterze terrorystycznym godzących w bezpieczeństwo potencjału obronnego państwa, sił zbrojnych jednostek organizacyjnych Ministerstwa Obrony Narodowej oraz zapobieganie im. Z kolei SWW podejmuje działania związane z rozpoznawaniem międzynarodowego terroryzmu i przeciwdziałaniem mu oraz rozpoznawaniem zdarzeń o charakterze terrorystycznym wymierzonym przeciwko personelowi i mieniu Sił Zbrojnych RP poza granicami państwa oraz przeciwdziałaniem i zapobieganiem im, a także zwalcza skutki takich zdarzeń.

Analogicznie do cywilnych służb specjalnych działających na terytorium RP właściwa do podejmowania wyżej wymienionych zadań jest Służba Kontrwywiadu Wojskowego⁷⁰, a poza jego granicami – Służba Wywiadu Wojskowego.

Podobnie jak w przypadku ABW uregulowano możliwości operacyjne Służby Kontrwywiadu Wojskowego, z kilkoma jednak wyjątkami⁷¹. Pierwszą, i wydaje się najbardziej dobitną, różnicą jest realizowanie przypisanych zadań przez stosowanie czynności operacyjno-rozpoznawczych i analityczno-informacyjnych, z wyłączeniem czynności o charakterze dochodzeniowo-śledczym. To sprawia, że SKW jest aktywnym uczestnikiem procedury rozpoznania danego zagrożenia pozostającego w jej właściwości rzeczowej do momentu uzyskania informacji uzasadniających podejrzenie popełnienia przestępstwa. Kolejnym działaniem, zgodnie z art. 27 ustawy o SKW oraz SWW, będzie zawiadomienie właściwej jednostki prokuratury bądź przekazanie informacji właściwemu organowi.

Wśród uprawnień brakuje natomiast możliwości korzystania z informacji z zakresu tajemnicy bankowej oraz z narzędzi związanych z blokowaniem dostępności w systemie informatycznym. Pozostałe czynności, tj. zarządzenie uniemożliwienia telekomunikacji, zarządzenie kontroli operacyjnej, uzyskiwanie danych telekomunikacyjnych, internetowych i pocztowych, gromadzenie, także niejawnie, wszelkich danych osobowych, niejawnie nabycie lub przejęcie przedmiotów pochodzących z przestępstwa, zarządzenie niejawnego nadzoru nad wytwarzaniem, przemieszczaniem, przechowywaniem i obrotem przedmiotami przestępstwa,

⁶⁹ Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j.: Dz.U. z 2017 r. poz. 1879).

⁷⁰ W ramach działań poza granicami RP SKW może podejmować zadania w celu realizacji rozpoznania oraz wykrywania przestępstw popełnionych przez żołnierzy, funkcjonariuszy SKW i SWW oraz pracowników Sił Zbrojnych RP i jednostek MON, zapobiegania im, a także w ramach współdziałania m.in. z Żandarmerią Wojskową – ale tylko w wyżej wymienionym celu. Co ciekawe, brakuje możliwości wykonywania tych zadań w zakresie nowo dodanej kompetencji, o której mowa w ust. 2a, podczas gdy Agencja Bezpieczeństwa Wewnętrznego takie możliwości otrzymała.

⁷¹ Mają one istotne znaczenie dla określenia pozycji tej służby w systemie antyterrorystycznym.

korzystanie z pomocy osób niebędących funkcjonariuszami SKW, podobnie jak procedura wdrażania wymienionych czynności, odpowiadają uprawnieniom Agencji Bezpieczeństwa Wewnętrznego.

W wojsku uprawnienia zbieżne z uprawnieniami Agencji Wywiadu ma Służba Wywiadu Wojskowego, która również realizuje czynności operacyjno-rozpoznawcze i analityczno-informacyjne. Prowadzenie ofensywnych działań operacyjnych na terytorium RP jest dopuszczalne jedynie za pośrednictwem Służby Kontrwywiadu Wojskowego lub ABW.

2.4. Żandarmeria Wojskowa i Policja

Wymienione formacje mundurowe uzupełniają system organów administracji rządowej powołanych wprost z ustawy do zajmowania się terroryzmem. Zarówno Żandarmeria Wojskowa, jak i Policja otrzymały te kompetencje w związku z wejściem w życie ustawy o działaniach antyterrorystycznych.

Uprawnienia Żandarmerii Wojskowej zostały uregulowane w art. 4 ust. 1 pkt 3a ustawy o ŻW i wojskowych organach porządkowych⁷². Zgodnie z nim na obszarach lub w obiektach należących do komórek i jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne to właśnie Żandarmeria Wojskowa prowadzi działania antyterrorystyczne⁷³.

Na uwagę zasługuje zakres czynności podejmowanych przez ŻW w ramach realizacji jej zadań ustawowych, który obejmuje zarówno pracę operacyjno-rozpoznawczą, jak i dochodzeniowo-śledczą⁷⁴. Te uprawnienia, oczywiście w zakresie realizacji własnych zadań, są analogiczne do uprawnień Służby Kontrwywiadu Wojskowego: zarządzanie uniemożliwienia telekomunikacji oraz kontroli operacyjnej, uzyskiwanie danych telekomunikacyjnych, internetowych i pocztowych, gromadzenie, także niejawnie, danych osobowych⁷⁵, niejawne nabycie lub przejęcie przedmiotów pochodzących z przestępstwa, zarządzanie niejawnego nadzoru nad wytwarzaniem, przemieszczaniem, przechowywaniem i obrotem przedmiotami przestępstwa, korzystanie z pomocy osób niebędących żołnierzami tej formacji.

Przyznanie uprawnień dochodzeniowo-śledczych Żandarmerii Wojskowej powoduje, że ta służba, przynajmniej zdaniem autora⁷⁶, wysuwa się na pierwsze miejsce wśród organów działających w ramach Ministerstwa Obrony Narodowej. Co ciekawe, nie są to wojskowe służby specjalne, o których była wyżej mowa, mające – w świetle analizy przepisów oraz kompetencji – zadania stricte informacyjne⁷⁷.

⁷² Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j.: Dz.U. z 2016 poz. 1483, ze zm.).

⁷³ O definicji działań antyterrorystycznych oraz o jej źródle – w dalszej części artykułu.

⁷⁴ Art. 4 ust. 2 pkt 4, 5 i 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

⁷⁵ Z uwzględnieniem ograniczeń wynikających z ustawy o ochronie danych osobowych.

⁷⁶ Autor ma świadomość istnienia wielu oponentów takiego stanowiska.

⁷⁷ Trudno ocenić, czy jest to wada, czy zaleta. Jak pokazuje doświadczenie, im dalej od źródła

Z kolei Policja w myśl art. 1 ust 3a ustawy o Policji⁷⁸ prowadzi działania kontrterrorystyczne, które umieszczają tę służbę na pozycji organu wykonawczego, zabezpieczającego fizyczne wyeliminowanie zagrożeń.

3. Ustawa o działaniach antyterrorystycznych

W dotychczasowych rozważaniach przedstawiono organy administracji rządowej, które, mając stosowne kompetencje do zajmowania się zagrożeniami związanymi z terroryzmem, zostały mocą ustawy wyposażone w określone środki i narzędzia do ich rozpoznawania, wykrywania oraz zapobiegania i przeciwdziałania im. Te środki, pomimo ingerencji w określone prawa i wolności człowieka i obywatela, mają służyć przede wszystkim realizacji celu, jakim jest zapewnienie bezpieczeństwa państwa, w najszerszym tego słowa znaczeniu. Przyznanie możliwości ich stosowania do realizacji ustawowych zadań, zwłaszcza służb specjalnych, nie powinno budzić wątpliwości.

Z przytoczonych wniosków wyłania się obraz służb wyposażonych w możliwości operacyjno-rozpoznawcze i dochodzeniowo-śledcze, a więc mających zaplecze do identyfikacji danego problemu na każdym poziomie jego rozpoznania i realizacji, oraz służb dysponujących narzędziami operacyjno-rozpoznawczymi i analityczno-informacyjnymi, tj. zorientowanych jedynie na uzyskanie informacji i przekazanie ich do właściwego wykorzystania. Takie uszeregowanie instytucji państwowych znalazło również odzwierciedlenie w przepisach szczególnych związanych z zagrożeniami o charakterze terrorystycznym.

W stosunku do przedstawionych ustaw kompetencyjnych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Żandarmerii Wojskowej i Policji 10 czerwca 2016 r. uchwalono *lex specialis* w kontekście zagrożeń zdarzeniami o charakterze terrorystycznym, a mianowicie ustawę o działaniach antyterrorystycznych. Jest ona odpowiedzią na długo oczekiwaną regulację prawną. Ustawa ma na celu umożliwienie przygotowania się do działania w sytuacji największego zagrożenia, mobilizacji sił i środków, a w przypadku zaistnienia zdarzenia terrorystycznego – do skutecznej reakcji i przeciwdziałania jego skutkom.

Należy zaznaczyć, że dzięki uregulowaniu spraw związanych z rozpoznawaniem i wykrywaniem przestępstw o charakterze terrorystycznym oraz zapobieganiem im doprecyzowano zakres odpowiedzialności poszczególnych organów, ich możliwości i realnego działania przez położenie nacisku na sprawne działanie państwa w sytuacji największego zagrożenia.

informacji, tym bardziej informacja jest zniekształcona bądź też akcenty są rozłożone niewłaściwie. To z kolei powoduje wysokie prawdopodobieństwo jej niepełnego lub niewłaściwego wykorzystania. W opisywanej sytuacji nie dość że będzie się miało do czynienia z poziomą strukturą jednej instytucji na etapie operacyjnym, to jeszcze na etapie procesowym cała ta procedura zostanie powtórzona, z tym że w odwrotnym kierunku.

⁷⁸ Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j.: Dz.U. z 2017 r. poz. 2067).

Potwierdzając konieczność tej regulacji, można przytoczyć postulaty *de lege ferenda*, wysunięte przez kolegialne gremia Departamentu Postępowań Karnych ABW⁷⁹ kilka lat wcześniej. Proponowano wówczas rozważenie podjęcia prac nad opracowaniem aktu rangi ustawowej kompleksowo regulującego problematykę rozpoznawania zagrożeń terrorystycznych, przeciwdziałania im, reagowania na nie oraz ich zwalczania, neutralizację i usuwanie skutków ewentualnych zamachów terrorystycznych, a także regulującego działania podejmowane bezpośrednio przez uprawnione do tego służby oraz instytucje na miejscu zdarzenia.

Przechodząc do omówienia norm ustawy o działaniach antyterrorystycznych, należy przypomnieć kilka definicji, co pozwoli na wysnucie wniosków również w zakresie prawidłowości i zasadności regulacji.

3.1. Definicje

Przestępstwo o charakterze terrorystycznym określone w art. 115 § 20 kk⁸⁰ jest to czyn zabroniony, zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu⁸¹.

Takie ujęcie przestępstwa o charakterze terrorystycznym znajduje swoje odzwierciedlenie w różnych przestępstwach spenalizowanych w kodeksie karnym, np. w rozdziałach XVI–XXII, z których najbardziej charakterystycznymi są te ujęte w art. 163 kk⁸², art. 164 kk⁸³, art. 165 kk⁸⁴, art. 165a kk⁸⁵, art. 166 kk⁸⁶ i art. 167 kk⁸⁷. Wymienione przestępstwa mogą, a nawet co do zasady będą, występować w zbiegu realnym z innymi czynami. Nie ma zatem możliwości popełnienia tego rodzaju przestępstwa bez związku z innym czynem zabronionym, określonym w przepisach prawa karnego. Może natomiast zaistnieć sytuacja, w której dopiero po upływie określonego czasu okaże się, że czyn zabroniony był popełniony w związku z przestępstwem o charakterze terrorystycznym.

Sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, lub zagrożenie taką sytuacją to **z d a r z e n i e**

⁷⁹ Zespół Zadaniowy do spraw opracowania propozycji współdziałania i zarządzania czynnościami na miejscu zdarzenia o charakterze terrorystycznym, powołany w 2013 r.

⁸⁰ Zob. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (tj.: Dz.U. z 2017 r. poz. 2204).

⁸¹ Motywy działania potencjalnego sprawcy mogą mieć różne podłoże, np. religijne, polityczne lub rasowe.

⁸² Sprowadzenie zdarzenia powszechnie niebezpiecznego.

⁸³ Sprowadzenie bezpośredniego niebezpieczeństwa zdarzenia.

⁸⁴ Sprawdzenie stanów powszechnie niebezpiecznych dla życia lub zdrowia.

⁸⁵ Finansowanie przestępstwa o charakterze terrorystycznym.

⁸⁶ Zawładnięcie statkiem wodnym lub powietrznym.

⁸⁷ Umieszczenie na statku wodnym lub powietrznym niebezpiecznego urządzenia lub substancji.

o charakterze terrorystycznym⁸⁸. Chodzi tutaj o wszystkie okoliczności, w tym znamiona wyżej opisanych przestępstw, oraz zaistniałe lub potencjalne skutki takich działań.

W ramach opisywanej sytuacji można wyselekcjonować miejsce zdarzenia o charakterze terrorystycznym będące otwartą lub zamkniętą przestrzenią, w której nastąpiło takie zdarzenie lub w której wystąpił lub miał wystąpić jego skutek, a także przestrzeń, w której występują zagrożenia związane ze zdarzeniem o charakterze terrorystycznym⁸⁹. Działania podejmowane przez poszczególne służby bezpośrednio na miejscu zdarzenia, o którym mowa, będą stanowić wprawdzie istotny, ale tylko wycinek wszystkich czynności prowadzonych przez uprawnione podmioty w związku z zaistnieniem konkretnego zdarzenia, które może mieć charakter terrorystyczny. Miejsce zdarzenia oraz podejmowane tam czynności będą, zgodnie z powyższą definicją, elementem większej całości związanej z kompleksowym (tzn. operacyjno-rozpoznawczym oraz dochodzeniowo-śledczym) rozpoznaniem zdarzenia o charakterze terrorystycznym.

Omawiana ustawa określiła zadania organów państwowych polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania kontroli nad tymi zdarzeniami w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, a także odtwarzaniu zasobów przeznaczonych do reagowania na nie, których ogół został nazwany działaniami antyterrorystycznymi⁹⁰.

Pośród tych zadań wymieniono również działania kontrterrorystyczne, o których wcześniej wspomniano. Należy je rozumieć jako działania wobec sprawców, osób przygotowujących lub pomagających w dokonaniu przestępstwa o charakterze terrorystycznym, prowadzone w celu wyeliminowania bezpośredniego zagrożenia życia, zdrowia lub wolności osób, a także mienia – przy wykorzystaniu specjalistycznych sił i środków oraz specjalistycznej taktyki działania⁹¹.

3.2. *Terroryzm – rozpoznawanie, zapobieganie i zwalczanie*

W centrum przepisów o działaniach antyterrorystycznych umiejscowiono szefa Agencji Bezpieczeństwa Wewnętrznego oraz ministra spraw wewnętrznych. Te organy, współdziałając ze sobą, mają za zadanie nie dopuścić do wystąpienia zdarzeń o charakterze terrorystycznym, a gdy one wystąpią – przejąć nad nimi kontrolę przez reakcję aparatu państwowego adekwatną do zagrożenia.

Ustawodawca, zwiększając nacisk na zwalczanie terroryzmu, nałożył na szefa ABW oraz ministra spraw wewnętrznych odpowiedzialność⁹² za prawidłowe,

⁸⁸ Art. 2 pkt 7 ustawy o działaniach antyterrorystycznych.

⁸⁹ Art. 2 pkt 6 ustawy o działaniach antyterrorystycznych.

⁹⁰ Art. 2 pkt 1 ustawy o działaniach antyterrorystycznych.

⁹¹ Art. 2 pkt 2 ustawy o działaniach antyterrorystycznych.

⁹² Art. 3 ust 1 i 2 ustawy o działaniach antyterrorystycznych.

profesjonalne działania służb, a także instytucji, które współpracują ze służbami w sytuacji zagrożenia lub choćby wystąpienia obaw i podejrzeń co do jego zaistnienia.

Przy omawianiu poszczególnych płaszczyzn działania trzeba zaznaczyć te, które wynikają z ustawy o działaniach antyterrorystycznych. Są to: **rozpoznawanie, zapobieganie i zwalczanie terroryzmu**. Ustawodawca przewidział rolę szefa ABW jako organu podejmującego działania mające na celu przede wszystkim zapobieganie zdarzeniom o charakterze terrorystycznym. Ustawa antyterrorystyczna jest prawem szczególnym, odwołującym się do zagrożeń i zdarzeń o charakterze terrorystycznym, dlatego większość czynności, jakie może wykonywać ABW, została uregulowana w ustawie o ABW oraz AW. Przypisanie ABW wspomnianych uprawnień realizuje tezę o konieczności zapewnienia jednego centrum zbierającego wszelkie informacje dotyczące zdarzenia o charakterze terrorystycznym oraz wydającego dyspozycje w celu zapewnienia sprawnego, szybkiego i adekwatnego do zagrożeń działania. Te obowiązki zostały powierzone szefowi ABW, który w ramach działań analityczno-informacyjnych oraz operacyjno-rozpoznawczych uzyskuje informacje na podstawie przepisów o ABW oraz koordynuje działania innych instytucji i organów państwowych, prowadząc jednocześnie czynności operacyjne w stosunku do osób podejrzewanych o działalność terrorystyczną⁹³.

Szef ABW został uprawniony do koordynowania działań o charakterze analityczno-informacyjnym pomiędzy służbami specjalnymi, tj. Służbą Kontrwywiadu Wojskowego, Agencją Wywiadu, Służbą Wywiadu Wojskowego, Centralnym Biurem Antykorupcyjnym oraz pozostałymi organami, tj. Policją, Strażą Graniczną, Biurem Ochrony Rządu⁹⁴, Państwową Strażą Pożarną, Służbą Celną, Generalnym Inspektorem Informacji Finansowej, Generalnym Inspektorem Kontroli Skarbowej, Żandarmerią Wojskową i Rządowym Centrum Bezpieczeństwa. Zakres tej koordynacji obejmuje zarówno informacje dotyczące ewentualnego zdarzenia o charakterze terrorystycznym⁹⁵, jak i osób, które mogą mieć z nim związek.

W celu realizacji wyznaczonych zadań szczególnym zainteresowaniem objęto cztery kategorie osób:

- 1) osoby podejmujące działalność na rzecz organizacji terrorystycznych lub organizacji związanych z działalnością terrorystyczną lub członków tych organizacji;
- 2) osoby poszukiwane, prowadzące działalność terrorystyczną lub podejrzewane⁹⁶ o popełnienie przestępstw o charakterze terrorystycznym, wobec których

⁹³ Należy zwrócić uwagę na kategorię stwierdzenia: „szef ABW prowadzi”, „koordynuje”, które nakładają obowiązek takiego działania. Brakuje tutaj miejsca na samodzielną decyzję o podjęciu określonych czynności. Powoduje to konieczność zdecydowania przez szefa ABW o rozpoczęciu działań koordynacyjnych w sytuacji zaistnienia zagrożenia.

⁹⁴ Obecnie: Służba Ochrony Państwa (przyj. red.).

⁹⁵ Szczególnie zdarzeń wymienionych w katalogu incydentów o charakterze terrorystycznym zawartym w *Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym* (t.j.: Dz.U. z 2017 r. poz. 1517).

⁹⁶ W ustawie użyto stwierdzenia „podejrzewanych”, jednak najprawdopodobniej chodziło o osoby już podejrzane, tj. takie, wobec których zgromadzono materiały do wydania postanowienia

w Rzeczypospolitej Polskiej zostało wydane zarządzenie o zatrzymaniu lub poszukiwaniu albo postanowienie o poszukiwaniu listem gończym, a także poszukiwane na podstawie europejskiego nakazu aresztowania;

3) osoby wobec których istnieje uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa o charakterze terrorystycznym, w tym osoby stanowiące zagrożenie bezpieczeństwa lotnictwa cywilnego;

4) uczestnicy szkoleń terrorystycznych lub podejmujący podróż w celu popełnienia przestępstwa o charakterze terrorystycznym⁹⁷.

Uzyskane informacje są zawarte w formie wykazu będącego w dyspozycji szefa ABW.

Zarówno osoby objęte wykazem, jak i osoby niebędące obywatelami polskimi, wobec których istnieje wątpliwość co do ich tożsamości lub podejrzenie nielegalnego przekroczenia przez nie granicy Rzeczypospolitej Polskiej, nielegalnego przebywania na jej terytorium albo wątpliwości co do deklarowanego celu ich pobytu w Polsce, mogą zostać sfotografowane (fotografiami sygnalitycznymi), poddane daktyloskopowaniu bądź od tych osób może być pobrany materiał biologiczny służący do oznaczenia profilu DNA. To uprawnienie mogą realizować funkcjonariusze ABW, Policji i Straży Granicznej. Uzyskane informacje są przekazywane Komendantowi Głównemu Policji i służą uzupełnieniu ewidencji prowadzonych przez KGP⁹⁸.

W celu zapobiegania zdarzeniom o charakterze terrorystycznym szef ABW może uzyskać dostęp do rejestrów i ewidencji służb specjalnych oraz różnych organów administracji publicznej: Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Straży Granicznej, Biura Ochrony Rządu⁹⁹, Państwowej Straży Pożarnej, Służby Celnej, Generalnego Inspektora Informacji Finansowej, Generalnego Inspektora Kontroli Skarbowej, Żandarmerii Wojskowej, Rządowego Centrum Bezpieczeństwa, Szefa Urzędu do Spraw Cudzoziemców, Prezesa Urzędu Komunikacji Elektronicznej, Prezesa Urzędu Lotnictwa Cywilnego, Prezesa Państwowej Agencji Atomistyki, Zakładu Ubezpieczeń Społecznych, Prezesa Kasy Rolniczego Ubezpieczenia Społecznego, Komisji Nadzoru Finansowego, Głównego Geodety Kraju, jednostek samorządu terytorialnego oraz Prokuratora Generalnego¹⁰⁰. Zakres danych, z których można skorzystać, jest poszerzony także o monitoring zainstalowany w instytucjach publicznych oraz na drogach i w miejscach publicznych¹⁰¹.

Zgodnie z art. 4 ustawy o działaniach antyterrorystycznych organy administracji publicznej, właściciele i posiadacze obiektów, instalacji oraz urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej są obowiązani

o przedstawieniu zarzutów (niekoniecznie ogłoszonego wyżej wymienionym osobom).

⁹⁷ Art. 6 ust. 1 ustawy o działaniach antyterrorystycznych.

⁹⁸ Art. 10 ust. 1–6 ustawy o działaniach antyterrorystycznych.

⁹⁹ Obecnie: Służba Ochrony Państwa (przyp. red.).

¹⁰⁰ Art. 11 ust. 1 ustawy o działaniach antyterrorystycznych. Należy wskazać, że to uprawnienie obejmuje również jednostki podległe i nadzorowane przez wyżej wymienione organy.

¹⁰¹ Co ważne, również na zasadzie transmisji online.

przekazywać szefowi ABW informacje dotyczące zagrożeń o charakterze terrorystycznym skierowanych na infrastrukturę administracji publicznej lub infrastrukturę krytyczną¹⁰², a w celu przeciwdziałania tym zagrożeniom albo minimalizacji ich skutków szef ABW może wydawać im polecenia¹⁰³.

Kolejną płaszczyzną działalności szefa ABW jest koordynowanie działań o charakterze operacyjno-rozpoznawczym pomiędzy wskazanymi służbami i organami, wspieranymi przez jednostki służby celnej uprawnione do obserwowania i rejestrowania obrazu i dźwięku w miejscach publicznych¹⁰⁴. Czynności operacyjno-rozpoznawcze muszą dotyczyć zdarzeń o charakterze terrorystycznym. Szef ABW może wydawać tym służbom i organom zalecenia¹⁰⁵ mające na celu usunięcie bądź minimalizację zaistniałego zagrożenia terrorystycznego.

W świetle zapisów ustawy o działaniach antyterrorystycznych na szczególną uwagę zasługuje art. 9. Wskazuje on na rozszerzony zakres działania Agencji Bezpieczeństwa Wewnętrznego w stosunku do dotychczas omawianego i obejmuje, oprócz zapobiegania, również rozpoznawanie i zwalczanie przestępstw o charakterze terrorystycznym. Nową, dotychczas nie wskazywaną płaszczyzną działania szefa ABW jest *zwalczanie*, które, zgodnie ze słownikową definicją, oznacza wystąpienie przeciwko komuś lub czemuś, przewyciężenie czegoś długotrwałym działaniem¹⁰⁶.

Przywołany przepis uprawnia szefa ABW do zarządzenia wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, w drodze i n i e j a w n y c h c z y n n o ś c i polegających na uzyskiwaniu i utrwalaniu: treści rozmów prowadzonych przy użyciu środków technicznych, w tym: sieci telekomunikacyjnych; obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych i wreszcie uzyskiwaniu dostępu i kontroli zawartości przesyłek¹⁰⁷.

O podjętych działaniach szef ABW informuje ministra koordynatora służb specjalnych oraz prokuratora generalnego, który może nakazać zaprzestanie czynności¹⁰⁸. Wymienione działania mogą zostać zarządzone na okres nie dłuższy niż trzy miesiące,

¹⁰² Szczególnie zagrożeń funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych, istotnych z punktu widzenia bezpieczeństwa państwa.

¹⁰³ Będą to prawdopodobnie prawnie wiążące wezwania do podjęcia określonych działań.

¹⁰⁴ Art. 8 ust. 1 ustawy o działaniach antyterrorystycznych

¹⁰⁵ Wprawdzie jest to tylko zalecenie, niemniej jednak trudno sobie wyobrazić sytuację, w której jakkolwiek organ niemający jednak obrazu całości sytuacji, odmówiłby wykonania takiego zalecenia.

¹⁰⁶ <http://sjp.pwn.pl/szukaj/zwalczanie.html>.

¹⁰⁷ Nasuwające się skojarzenia i analogie do kontroli operacyjnej opisanej w art. 27 ustawy o ABW oraz AW są jak najbardziej zasadne.

¹⁰⁸ Art. 9 ust. 4 ustawy o działaniach antyterrorystycznych.

z możliwością kolejnego przedłużenia, ale już na zasadach określonych w art. 27 ustawy o ABW oraz AW¹⁰⁹.

Na pierwszy plan wysuwa się decyzja o podjęciu czynności równoznacznych z kontrolą operacyjną¹¹⁰, która jest decyzją jednoinstancyjną. Ustawodawca ograniczył krąg osób do cudzoziemców niebędących obywatelami RP, a uprawnienia szefa ABW zostały przyznane aktem rangi ustawy. To powoduje, że nie ma przesłanek do kwestionowania podstaw prawnych i legitymacji do podejmowania wyżej wymienionych działań.

Zaznaczenia wymaga szczególnie rodzaj zagrożenia, które powoduje, że ustawodawca wyposażył szefa ABW w możliwość podjęcia decyzji o zastosowaniu ofensywnych czynności operacyjnych. Z uwagi na to, że chodzi o obawę dotyczącą możliwości prowadzenia działalności terrorystycznej przez cudzoziemców¹¹¹, normalny tryb wdrażania kontroli operacyjnej na podstawie art. 27 ustawy o ABW oraz AW mógłby być znacznie utrudniony lub wręcz niemożliwy. Konieczną przesłanką jej zastosowania byłaby w tym przypadku bezskuteczność albo nieprzydatność innych środków pracy operacyjnej. Dynamiczny charakter przestępczości terrorystycznej powoduje powstawanie sytuacji, w których brakuje możliwości poprowadzenia klasycznego rozpoznania operacyjnego zaczynającego się od prostych form i środków do skomplikowanych, wymagających częstokroć wielopłaszczyznowych kombinacji lub gier operacyjnych. Istotne znaczenie będzie miał czas¹¹² rzeczywistego zainicjowania tych czynności. W przypadku uzyskania informacji operacyjnych o prawdopodobieństwie zaistnienia zagrożenia terrorystycznego nie ma miejsca na wahanie, które musi ustąpić niezwłocznemu, ale racjonalnemu podejmowaniu decyzji¹¹³. To jedna strona takich rozwiązań ustawowych.

Druga jest taka, że działalność terrorystyczna nie zawsze wygląda tak jednoznacznie, jak to jest kreowane w powszechnym odbiorze¹¹⁴. Działalność terrorystyczna to także cała logistyka otaczająca właśnie te osoby, wobec których można podjąć czynności procesowe, zgromadzić dowody i skierować sprawę do sądu. W ten sposób

¹⁰⁹ Czyli z kontrolą sądową zasadności ewentualnego przedłużenia.

¹¹⁰ Nadzór nad prawidłowością stosowania tych czynności ma prokurator generalny przez możliwość ich zakończenia, ale zgodnie z zapisem szef ABW „niezwłocznie” przekazuje zarządzenie o zastosowaniu wymienionych czynności, co w praktyce może oznaczać, że ich wykonywanie może jeszcze przez jakiś czas obowiązywać.

¹¹¹ Czyli osób, wobec których często trudno lub wręcz niemożliwe jest zweryfikowanie danych osobowych, danych o miejscu zamieszkania, o karalności itp.

¹¹² Autor nie chciał podnosić tego argumentu, ale taka jest rzeczywistość każdego organu administracji państwowej. Aby wdrożyć pewne czynności, niezbędny jest czas w komórce organizacyjnej; następnie ich wdrożenie musi zaaprobować jednostka lub departament itp., aby dokumenty na temat tych czynności zostały przekazane do innej instytucji. Przed przesłaniem przez ABW wniosku o zastosowanie kontroli operacyjnej do Sądu Okręgowego w Warszawie dokumentacja przechodzi przez kilka komórek organizacyjnych (nie wspominając o wyższych przełożonych, którzy muszą jeszcze zaaprobować tę dokumentację).

¹¹³ Łącznie z poniesieniem odpowiedzialności za podjęcie decyzji.

¹¹⁴ Bojownik – samobójca, jednego wyznania, w charakterystycznym ubiorze, z przymocowanym ładunkiem wybuchowym.

można dojść do prawdziwych uczestników i organizatorów, określić role, jakie odgrywają, a także zidentyfikować ich potencjalne cele. To z kolei – jak wspomniano wcześniej – daje służbom przewagę i możliwości.

Już te argumenty wskazują na pewną prawidłowość założenia przyjętego przez ustawodawcę wyposażającego szefa ABW w możliwość podjęcia ofensywnych metod pracy operacyjnej w świetle zagrożenia o charakterze terrorystycznym.

Nie sposób też pominąć innego podejścia, niepozostającego również bez racji wobec omawianego zagadnienia. Jak stwierdził Lech Paprzycki, Prezes Sądu Najwyższego Izby Karnej (...) *od wielu lat służby specjalne funkcjonowały (...) w systemie ograniczonej kontroli prokuratorsko-sądowej*. Dodał też, że ta kontrola jest w interesie funkcjonariuszy, aby uczynić podejmowane przez nich działania operacyjne, także te antyterrorystyczne, bezpiecznymi pod względem prawnym¹¹⁵. Możliwość zarządzenia przez szefa ABW czynności na podstawie art. 9 ustawy o działaniach antyterrorystycznych, bez konieczności uzyskania zgody sądu, może budzić pewnego rodzaju kontrowersje, zwłaszcza gdy patrzy się przez pryzmat powszechnie wprowadzonej sądowej kontroli wniosków o kontrolę operacyjną, składanych przez wszystkie uprawnione do tego służby.

Konfrontując powyższe stanowiska, wydaje się, że wynik przeprowadzonych czynności można sprowadzić do stwierdzenia, że szczególne okoliczności wymagają szczególnych uprawnień, te zaś – szczególnego profesjonalizmu, rzetelności i staranności. Powyższe przymioty będą gwarantowały prawidłowe i skuteczne korzystanie z narzędzi przyznanych szefowi ABW.

Po zakończonych czynnościach w trybie art. 9 szef ABW przekazuje wszelkie zgromadzone materiały prokuratorowi generalnemu, który z kolei podejmuje decyzję o zakresie i sposobie wykorzystania materiałów. Oceny, czy dany materiał zawiera dowody pozwalające na wszczęcie postępowania karnego, dokonuje prokurator generalny¹¹⁶, który w przypadku ich braku zarządza zniszczenie materiału.

Zapisy ustawy o działaniach antyterrorystycznych w sposób znamieny odwołują się do płaszczyzny procesowej, która została poszerzona o możliwości wykorzystania informacji uzyskanych w trybie operacyjnym, przez co umożliwiono odpowiednią reakcję na wystąpienie zagrożenia o charakterze terrorystycznym. Autor zaznacza, że o ile z perspektywy funkcjonariusza operacyjnego prowadzącego sprawę mającą na celu rozpoznanie zagrożenia terrorystycznego będzie się ona zbliżała ku końcowi, o tyle z perspektywy zapobiegania temu zagrożeniu i zwalczania go, w tym procesowego zgromadzenia i zabezpieczenia dowodów, a nierzadko ujęcia sprawców – będzie się ona dopiero rozpoczynała.

Nowością w świetle przepisów o postępowaniu karnym są rozwiązania związane z możliwością przeszukania o każdej porze dnia i nocy osób przebywających w danym

¹¹⁵ L.K. Paprzycki, *Czy Polsce potrzebna jest ustawa antyterrorystyczna?*, w: *Terroryzm, materia ustawowa?*, K. Indecki, P. Potejko (red.), Warszawa 2009.

¹¹⁶ Wskazuje na to brzmienie art. 27 ust. 15 ustawy o ABW oraz AW, zgodnie z którym to szef ABW określa, czy w zgromadzonym materiale z kontroli operacyjnej są dowody pozwalające na wszczęcie postępowania karnego, a jeżeli tak, to przekazuje je prokuratorowi generalnemu.

pomieszczeniu lub na danym terenie oraz przeszukania określonego obszaru¹¹⁷. Postanowienie w tej sprawie wydaje prokurator, działając, jak można domniemywać, na podstawie wniosku właściwej jednostki ABW zawierającego opis materiałów wskazujących na podejrzenie, usiłowanie popełnienia albo przygotowywanie przestępstwa o charakterze terrorystycznym oraz uzasadnienie podstaw do przypuszczenia, że dane rzeczy tam się znajdują. W analogicznym trybie prokurator może wydać postanowienie o zatrzymaniu osoby podejrzewanej.

Analizując powyższy przepis, można dojść do wniosku, że informacje o tym, czego albo kogo należy poszukiwać, muszą być oparte co najmniej na uzasadnionym przypuszczeniu¹¹⁸ oraz określać, w związku z jakim konkretnie przestępstwem mają być zgromadzone i zweryfikowane. Ta wiedza niekoniecznie musi spełniać przesłanki konieczne do wszczęcia śledztwa, do którego zainicjowania jest niezbędne uzasadnienie podejrzenia o popełnienie przestępstwa¹¹⁹. Wydaje się, że właśnie rezultat tych czynności będzie stanowił podstawę do podjęcia decyzji o wszczęciu bądź odmowie wszczęcia postępowania przygotowawczego. Omawiane czynności będą realizowane, używając terminologii prawa handlowego, „w śledztwie w organizacji”, tj. przed decyzją o jego formalnym wszczęciu.

Jeżeli w toku realizowanych czynności operacyjno-rozpoznawczych zostanie zgromadzony materiał wskazujący na podejrzenie popełnienia przestępstwa, prokurator, mając na względzie dobro śledztwa, może wydać postanowienie o przedstawieniu zarzutów, wyłącznie na podstawie materiałów operacyjnych¹²⁰. W przypadku uprawdopodobnienia popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym, prokurator może wystąpić do sądu o zastosowanie tymczasowego aresztowania¹²¹.

Ten przepis umożliwi przedstawienie zarzutów w sytuacji istnienia „jedynie” podejrzenia popełnienia przestępstwa, niekoniecznie uzasadnionego, pod warunkiem okoliczności kwalifikującej o działaniu dla dobra późniejszego postępowania

¹¹⁷ Art. 25 ust. 1 ustawy o działaniach antyterrorystycznych.

¹¹⁸ Trzeba zauważyć, że jest to dość karkołomna konstrukcja.

¹¹⁹ Jak stwierdził W. Grzeszczyk, „(...) podstawą decyzji o wszczęciu śledztwa mogą być tylko takie dane, które obiektywnie uprawdopodobniają popełnienie przestępstwa, subiektywnie zaś wywołują wysoki stopień podejrzenia co do jego zaistnienia. Owa podstawa jest sformułowana jako warunek minimalny, a zatem popełnienie przestępstwa tym bardziej spełnia warunek istnienia podstawy wszczęcia procesu. Ustawa o działaniach antyterrorystycznych, mówiąc o uzasadnionym podejrzeniu popełnienia przestępstwa, wymaga tym samym, aby było ono oparte na racjonalnych przesłankach. Tego warunku nie spełnia zatem pojawienie się pogłoski, domysłu lub bliżej nieokreślonego przypuszczenia na temat przestępstwa, gdyż takie podejrzenie byłoby dowolne. Uzasadnione podejrzenie ma się odnosić do konkretnego przestępstwa, a więc czynu, który daje się zakwalifikować z określonego przepisu części szczególnej Kodeksu karnego lub innej ustawy szczególnej, przy czym dotyczy to również form stadialnych i postaci zjawiskowych danego przestępstwa”, zob. W. Grzeszczyk, *Postępowanie przygotowawcze w kodeksie postępowania karnego*, Kraków 1998, s. 48.

¹²⁰ Art. 26 ust. 1 ustawy o działaniach antyterrorystycznych.

¹²¹ Art. 26 ust. 2 ustawy o działaniach antyterrorystycznych.

przygotowawczego. Z kolei w sytuacji jego uprawdopodobnienia¹²² może stanowić samoistną przesłankę do tymczasowego aresztowania.

Wyszczególnione konstrukcje działań o charakterze procesowym przed formalnym wszczęciem śledztwa mogą znajdować swoje źródło w art. 308 kpk, (tj. postępowania w niezbędnym zakresie, dostosowanym do realiów zagrożenia zdarzeniem terrorystycznym). Trudno odmówić im tutaj pewnej racji bytu, zwłaszcza patrząc przez pryzmat np. materiałów zgromadzonych zgodnie z art. 9 ustawy o działaniach antyterrorystycznych. Gorzej by było, gdyby te decyzje były podejmowane na podstawie niejasnych, niejednoznacznych sformułowań, i gdyby nie były poprzedzone obiektywną konsultacją z jednostkami ABW odpowiadającymi za współpracę z prokuraturą.

Zmienność metod wykorzystywanych przez terrorystów powoduje, że służby powinny dysponować odpowiednimi instrumentami służącymi właściwemu rozpoznawaniu i ocenianiu zagrożeń oraz skutecznemu przeciwdziałaniu ewentualnym zdarzeniom o charakterze terrorystycznym. Te instrumenty, aby były skuteczne, muszą być dostosowane do zmieniających się realiów i być na bieżąco aktualizowane.

Na zakończenie warto przytoczyć fragment jednej z analizowanych kilka lat temu przez autora spraw operacyjnych, w której na długo przed regulacjami ustawy o działaniach antyterrorystycznych wskazywał:

(...) w świetle aktualnej sytuacji rozwoju terroryzmu zarówno w Europie, na Bliskim Wschodzie, w Azji i obu Amerykach kwestie związane z decydowaniem o stwarzaniu zagrożenia dla bezpieczeństwa państwa, jak i porządku publicznego winny być rozpatrywane według zasady, że każda wątpliwość powinna być brana na niekorzyść, przynajmniej w świetle konieczności (i możliwości – dop. aut.) jej weryfikacji wobec podmiotu podejrzewanego. Zresztą, jak wynika z informacji medialnych, taktyka ta przyjęła się w praktyce innych państw szczególnie narażonych na terroryzm (USA, Anglia, Izrael itp.) i jest aktualnie realizowana.

Takie podejście daje szansę organom państwa w walce przeciwko organizacjom oraz ich uczestnikom, które mają na celu zasianie powszechnego poczucia zagrożenia.

Wnikliwa lektura ustawy o działaniach antyterrorystycznych oraz aktów prawnych z nią powiązanych daje odpowiedź na pytania, czy zasadne było wyposażenie organów państwa w określone środki działania wobec zaistnienia szczególnego zagrożenia bezpieczeństwa państwa i obywateli oraz czy te działania mają legitymację w polskim systemie prawnym. W obydwu wypadkach odpowiedź – pomimo pewnych zapisów, które mogą być kontrowersyjne – brzmi „tak”.

¹²² Ustawodawca posługuje się tutaj nieprecyzyjnymi zwrotami „uprawdopodobnione podejrzenie”, unikając kodeksowych konstrukcji „uzasadnionego podejrzenia”. Wydaje się jednak, że przed zawnioskowaniem o areszt tymczasowy właściwe byłoby uzyskanie materiałów uzasadniających podejrzenie popełnienia przestępstwa, a tym samym dających podstawę do wszczęcia śledztwa w trybie art. 303 kpk.

Oczywiście nie ustrzeżono się błędów, jednak będą one weryfikowalne dopiero przy konieczności bezpośredniego stosowania zapisów ustawy o działaniach antyterrorystycznych.

Wydarzenia ostatnich lat, miesięcy, a nawet dni pokazują, jak ten temat jest ważny, i że jego regulacja wymaga dużej uwagi oraz precyzji. Nasilające się akcje terrorystyczne, w tym także działania mające na celu wspieranie organizacji terrorystycznych, wymagają szybkiej i sprawnej reakcji¹²³, która jednocześnie powinna być działaniem legalnym.

Od 10 czerwca 2016 r. mamy punkt wyjścia, dzięki któremu wspomniany na wstępie niniejszego artykułu „krok za przestępcami” może być dużo mniejszy.

Bibliografia:

Publikacje zwarte

1. Gebethner S., *Stany szczególnego zagrożenia jako instytucja prawa konstytucyjnego*, „Państwo i Prawo” 1982, nr 8.
2. Grzeszczyk W., *Postępowanie przygotowawcze w kodeksie postępowania karnego*, Kraków 1998, Zakamycze.
3. *Konstytucja Rzeczypospolitej Polskiej. Komentarz I, Wstęp, art. 29*, L. Garlicki, M. Zubik (red. nauk.), Warszawa 2016.
4. Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013, Wolters Kluwer.
5. *Terroryzm, materia ustawowa?*, K. Indecki, P. Potejko (red.), Warszawa 2009, ABW.
6. Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Warszawa 2008, LIBER.

Akty prawne

1. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. nr 78 poz. 483).
2. *Prawa Człowieka i Obywatela z 26 sierpnia 1789 r.*, <http://libr.sejm.gov.pl/tek01/txt/konst/francja-18>.
3. *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. z 2016 r. poz. 904, ze zm.).

¹²³ Z wieloma możliwościami skutecznej realizacji celów postawionych przed organami państwa.

4. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (t.j.: Dz.U. z 2017 r. poz. 1932).
5. *Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (t.j.: Dz.U. z 2017 r. poz. 1928).
6. *Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej* (t.j. Dz.U. z 2017 r. poz. 1897).
7. *Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach* (t.j.: Dz.U. z 2017 r. poz. 2206).
8. *Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej* (t.j.: Dz.U. z 2017 r. poz. 1214, ze zm.).
9. *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j. Dz.U. z 2017 r. poz. 2365).
10. *Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu* (t.j.: Dz.U. z 2017 r. poz. 985).
11. *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz.U. z 2017 r. poz. 1920).
12. *Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (t.j.: Dz.U. z 2017 r. poz. 1907).
13. *Ustawa z dnia 23 listopada 2012 r. – Prawo pocztowe* (t.j.: Dz.U. z 2017 r. poz. 1481).
14. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (t.j.: Dz.U. z 2017 r. poz. 1219).
15. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (t.j.: Dz.U. z 2016 r. poz. 922).
16. *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: Dz.U. 2017 r. poz. 1879).
17. *Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych* (t.j.: Dz.U. z 2016 r. poz. 1483, ze zm.).
18. *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j.: Dz.U. z 2017 r. poz. 2067).
19. *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. z 2017 r. poz. 2204).
20. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym* (t.j.: Dz.U. z 2017 r. poz. 1517).

Strony internetowe:

<http://libr.sejm.gov.pl/tek01/konst/francja-18>

<http://sjp.pwn/slowniki>

<http://sjp.pwn.pl/szukaj>

Inne:

Współdziałanie i zarządzanie czynnościami na miejscu zdarzenia o charakterze terrorystycznym, opracowanie Zespołu Zadaniowego do spraw opracowania propozycji algorytmu współdziałania i zarządzania czynnościami na miejscu zdarzenia o charakterze terrorystycznym. Współdziałanie i zarządzanie czynnościami na miejscu zdarzenia o charakterze terrorystycznym, Warszawa 2013.

Abstrakt

Niezwykle popularne w ostatnim czasie w dyskusji publicznej są sprawy związane z terroryzmem. Dotyczy to zarówno komentarzy zdarzeń oraz incydentów o charakterze terrorystycznym, w tym szukania ich przyczyn, jak i podejmowanych prób wskazania stanu przygotowania naszego państwa do odparcia takich ataków lub przeciwdziałania im. Niestety, ta dyskusja odbywa się w atmosferze pewnego, niepotrzebnego, napięcia i wzburzenia wywoływanego, w zasadzie każdorazowo, charakterem komentowanego zdarzenia i odnoszeniem go do bieżących wydarzeń w Polsce, często w wymiarze czysto politycznym. Brakuje również zachowania „zimnej krwi”, jakże potrzebnej przy ocenie danego zagrożenia, nie wspominając już o realnym działaniu w jego obliczu.

Niniejszy artykuł zawiera odpowiedzi na pytania potencjalnych uczestników, widzów i słuchaczy takich dyskusji, zarówno w kwestiach elementarnych, dotyczących organów właściwych w zakresie terroryzmu oraz ich zadań, jak i bardziej zaawansowanych, wskazujących na zakres środków i metod pracy operacyjno-rozpoznawczej i dochodzeniowo-śledczej.

Rozważania zawarte w niniejszym artykule zostały poprzedzone próbą zdefiniowania roli państwa w zapewnianiu bezpieczeństwa publicznego oraz znaczenia tego zadania dla organów administracyjnych i samego społeczeństwa. Poruszone tu zagadnienia dadzą możliwość własnego, obiektywnego osądu spraw omawianych w przywołanych na wstępie komentarzach.

Słowa kluczowe: bezpieczeństwo, terroryzm, działania antyterrorystyczne, kontrola operacyjna, czynności niejawne.

Marcin Gołaszewski
Paulina Markowicz
Justyna Jastrzębska

Postrzeganie badań poligraficznych w Polsce oraz ich użyteczność w służbach i innych obszarach działalności

1. Badania poligraficzne w polskiej literaturze przedmiotu

W polskiej literaturze naukowej jest widoczne niejedolite stanowisko w sprawie oceny przydatności badań poligraficznych (wariograficznych). Wielu autorów podkreśla, że krytykowanie tej metody badań jest związane z niedostatecznym zrozumieniem istoty pomiarów wykonywanych za pomocą poligrafu. Wśród znacznej części środowiska psychologicznego, również w Polsce, funkcjonuje mylne przeświadczenie na temat badań poligraficznych, mające podstawy m.in. w pracach Paula Ekmana zajmującego się naturą emocji i metodami detekcji nieszczeroci przy wykorzystaniu mikroekspresji¹. Ten autor uważa, że kłamstwo może zostać zdemaskowane w sytuacji, gdy osoba odczuwa strach, poczucie winy, radość i inne emocje. Podkreśla, że poszukując oznak kłamstwa, należy pamiętać o ryzyku popełnienia błędu Otella² oraz możliwości pomyłek związanych z nieuwzględnieniem różnic indywidualnych w zachowaniu emocjonalnym osoby badanej. Co do badań z wykorzystaniem poligrafu Ekman przyznaje, że swoją ocenę przydatności tego urządzenia opiera na publikacjach innych naukowców, w jego pracach zaś można zauważyć, że nie uwzględnia on dowodów naukowych potwierdzających rzetelność i dokładność tej metody badawczej.

Istnieje wiele prac polskich autorów zwracających uwagę na wysoką dokładność badań poligraficznych i szeroki wachlarz możliwości ich zastosowania. Do prekursorów należą m.in. Jan Widacki i Jerzy Konieczny. Wyniki jednego z eksperymentów przeprowadzonych przez J. Widackiego dowiodły, że badania poligraficzne są równie wartościowe jak inne metody identyfikacji kryminalistycznej³. Mimo to część środowiska prawniczego przejawia sceptycyzm wobec dowodowego wykorzystania tego typu badań w polskim procesie karnym. Piotr Herbowski wskazuje, że badania poligraficzne w procesach sądowych są często postrzegane jako metoda służąca wprost do oceny szczeroci wypowiedzi osoby badanej, czyli służą wykrywaniu kłamstwa⁴. Sytuację wyjaśnił Sąd Najwyższy, wydając 29 stycznia 2015 r. postanowienie

¹ P. Ekman, *Kłamstwo i jego wykrywanie w biznesie, polityce i małżeństwie*, Warszawa 2006.

² Tytułowy bohater tragedii Szekspira, który interpretuje strach i zaniepokojenie Desdemony jako reakcję na wieść o śmierci jej domniemanego kochanka, potwierdzając w ten sposób swoje przekonanie o jej niewierności.

³ J. Widacki, *Badania poligraficzne w Polsce*, Kraków 2014, s. 135–138.

⁴ P. Herbowski, *Wykrywcze wykorzystanie wyników badań poligraficznych*, „Problemy Kryminalistyki” 2010, nr 267, s. 12–14.

(I KZP 25/14), w którym oficjalnie potwierdził możliwość przeprowadzania badań poligraficznych wobec podejrzanego, oskarżonego lub świadka oraz potraktowania opinii biegłego – sporządzonej na podstawie ekspertyzy – zarówno jako dowodu odciążającego, jak i obciążającego (na podstawie art. 199a kodeksu postępowania karnego⁵).

2. Postrzeganie badań poligraficznych przez różne środowiska w Polsce

Z analiz J. Moszczyńskiego opublikowanych w 2011 r. (patrz tabela) wynika, że główni odbiorcy ekspertyz z zakresu badań poligraficznych, czyli prokuratorzy i sędziowie, przypisywali im bardzo niską wartość poznawczą, dowodową (w skali od 1 do 10 – odpowiednio: 2,9 i 3,2). Nawet kolejny, najniżej oceniany rodzaj badań kryminalistycznych – identyfikacja osmologiczna – uzyskał dwukrotnie wyższe oceny (odpowiednio: 6,0 i 5,9).

Tabela. Preferencje badań kryminalistycznych wśród prokuratorów i sędziów.

| PROKURATORZY | |
|---|--------------------------------------|
| Badania kryminalistyczne | Ocena wartości (w skali 1–10) |
| Identyfikacja genetyczna | 9,82 |
| Identyfikacja daktyloskopijna | 9,81 |
| Identyfikacja fizykochemiczna | 9,0 |
| Identyfikacja broni palnej | 8,9 |
| Identyfikacja na podstawie pisma ręcznego | 8,8 |
| Rekonstrukcja wypadku drogowego | 7,7 |
| Identyfikacja śladów ust | 7,6 |
| Identyfikacja fonoskopijna | 7,5 |
| Identyfikacja śladów narzędzi | 7,4 |
| Identyfikacja śladów uszu | 7,3 |
| Identyfikacja śladów obuwia | 7,0 |
| Identyfikacja osmologiczna | 6,0 |
| Badania wariograficzne | 2,9 |
| SĘDZIOWIE | |
| Badania kryminalistyczne | Ocena wartości (w skali 1–10) |
| Identyfikacja genetyczna | 9,7 |
| Identyfikacja daktyloskopijna | 9,5 |
| Identyfikacja broni palnej | 8,8 |
| Identyfikacja na podstawie pisma ręcznego | 8,3 |
| Identyfikacja fizykochemiczna | 8,3 |
| Rekonstrukcja wypadku drogowego | 7,7 |

⁵ Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j.: Dz.U. z 2017 r. poz. 1904).

| | |
|-------------------------------|------------|
| Identyfikacja fonoskopijna | 7,4 |
| Identyfikacja śladów narzędzi | 7,2 |
| Identyfikacja śladów ust | 7,2 |
| Identyfikacja śladów obuwia | 7,1 |
| Identyfikacja śladów uszu | 6,7 |
| Identyfikacja osmologiczna | 5,9 |
| Badania wariograficzne | 3,2 |

Źródło: za: J. Moszczyński, *Subiektywizm w badaniach kryminalistycznych*, Olsztyn 2011, s. 205–206, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.

Kilka lat po opublikowaniu badań J. Moszczyńskiego preferencje uległy niewielkim zmianom na korzyść badań poligraficznych, ale ich miejsce w hierarchii się nie zmieniło. Z analiz K. Niziołka wynika, że aktualnie prokuratorzy i sędziowie przypisują tego typu badaniom (ocenianym w skali 1–10) wartość 4 (dla porównania – identyfikacja genetyczna: powyżej 9, daktyloskopia: prawie 9, balistyka: ponad 8, identyfikacja osmologiczna: ponad 5)⁶. Podejście oceniających do badań poligraficznych różniło się w zależności od osobistych doświadczeń. Osoby, które w jakikolwiek sposób miały do czynienia z poligrafem, przypisywały tym badaniom średnio o ponad 1 punkt wyższą wartość niż ci, którzy bazowali wyłącznie na opiniach obiegowych.

Brakuje polskich badań dotyczących stopnia akceptacji badań poligraficznych w środowisku naukowym. Dla porównania – takie analizy przeprowadzono na początku XXI w. w Stanach Zjednoczonych⁷. Wśród ankietowanych byli członkowie Towarzystwa Badań Naukowych nad Psychofizjologią (Society for Psychophysiological Research, SPR) oraz Amerykańskiego Towarzystwa Psychologii i Prawa (American Psychology-Law Society, APLS). Ponad 90 proc. ankietowanych odpowiedziało twierdząco na pytanie, czy opracowania na temat badań poligraficznych, publikowane w czasopismach naukowych recenzowanych niezależnie, są oparte na powszechnie akceptowanej metodologii? Około 70 proc. naukowców oceniło m.in., że badanie poligraficzne jest dowodem tak samo użytecznym, albo nawet bardziej, jak opinia psychologiczna na temat tego, czy dana osoba jest niebezpieczna. Siedemdziesiąt dwa procent członków APLS i sześćdziesiąt jeden procent członków SPR stwierdziło, że w przypadku dopuszczenia dowodu z opinii biegłego z zakresu badań poligraficznych w postępowaniu sądowym trafność orzeczeń się zwiększy albo pozostanie bez zmian. Pozostali uznali, że się obniży.

⁶ K. Niziołek, *Ocena trafności badań psychofizjologicznych w odniesieniu do polskiego procesu karnego*, prezentacja z Ogólnopolskiej Konferencji Naukowej „Rola badań psychofizjologicznych w rozumieniu i korekacji funkcjonowania człowieka”, 18 V 2017 r., UKSW, Warszawa.

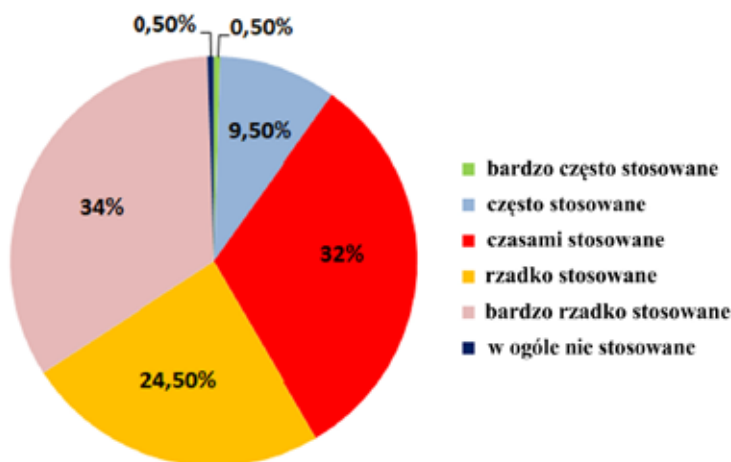
⁷ C.R. Honts i in., *General acceptance of the polygraph by the scientific community: Two surveys of professional attitudes*, referat zaprezentowany podczas zjazdu APLS w Austin (Texas, USA) w 2002 r.

W celu określenia, jak polskie społeczeństwo (różne grupy, nie tylko przedstawiciele wymiaru sprawiedliwości) postrzega obecnie badania poligraficzne, opracowano ankietę dotyczącą m.in. znajomości pojęcia badania poligraficzne, doświadczeń w zakresie wykorzystania tej metody oraz opinii dotyczących jej praktycznego zastosowania. W badaniu pilotażowym wzięło udział 200 osób w wieku 16–67 lat. Średni wiek w grupie wyniósł 25 lat. Pod względem płci większość stanowiły kobiety. Dominowały osoby z wykształceniem wyższym lub studiujące (głównie z kierunków: Prawo, Psychologia, Kryminologia, Bezpieczeństwo Wewnętrzne).

W momencie przeprowadzania ankiety 33,5 proc. osób biorących w niej udział deklaroowało, że są zatrudnione na pełny etat. Wśród miejsc pracy badani wymieniali m.in.: Ministerstwo Obrony Narodowej, Brygadę Kawalerii Pancерnej, Służbę Celną, Policję, Miejski Ośrodek Pomocy Społecznej, Wojsko Polskie, administrację państwową, centra medyczne i psychoterapii, fundacje, firmy ochroniarskie oraz firmy zajmujące się rekrutacją pracowników. Własną działalność gospodarczą prowadziło 3,5 proc. ankietowanych, 2 proc. utrzymywało się z gospodarstwa rolnego, 4,5 proc. stanowili bezrobotni, a 2,5 proc. emeryci i renciści. Dla pozostałych badanych głównym zajęciem była nauka na studiach wyższych.

W grupie osób badanych 63,5 proc. deklaroowało znajomość pojęcia badanie poligraficzne, z kolei 22 proc. przyznało, że miało pośrednią lub bezpośrednią styczność z poligrafem. U większości badanych podstawą wyobrażenia na temat tej metody była wiedza zdobyta na studiach, w miejscu pracy lub własne zainteresowania, a przede wszystkim przekazy medialne, zwłaszcza programy dokumentalne, rozrywkowe lub teleturnieje emitowane w telewizji (np. „Moment prawdy”). Osiem procent ankietowanych było poddanych badaniu z wykorzystaniem poligrafu, 36 proc. deklaroowało podstawową wiedzę na temat przebiegu badania poligraficznego, 64 proc. zaś nie wiedziało, jak wygląda procedura takiego badania.

Na wykresie 1 przedstawiono wyobrażenie osób biorących udział w ankiecie na temat częstotliwości stosowania badań poligraficznych w Polsce.



Wykres 1. Stosowanie badań poligraficznych w Polsce w ocenie ankietowanych.

Źródło: Opracowanie własne autorów.

Na wykresie 2 przedstawiono odpowiedzi ankietowanych dotyczące nieświadomych reakcji psychofizjologicznych organizmu mierzonych przez poligraf.



Wykres 2. Nieświadome reakcje organizmu mierzone przez poligraf wskazane przez ankietowanych.

Źródło: Opracowanie własne autorów.

Wśród odpowiedzi znalazły się warianty poprawne, tj.: zmiany w cyklu oddechowym (wskazane przez 59,5 proc. ankietowanych), zmiany ciśnienia krwi i tętna (68 proc.), zmiany w przewodnictwie elektrycznym skóry (57 proc.), zmiany objętości krwi w naczyniach krwionośnych (37 proc.) oraz napięcie mięśni, czyli ruchy badanego (61 proc.).

Nieprawidłowe warianty odpowiedzi obejmowały: poziom odczuwanego stresu (38 proc.), zmiany temperatury ciała (41 proc.), reakcje wskazujące na zaburzenia rytmu okołodobowego (5 proc.), ruchy gałek ocznych (16,5 proc.), aktywność gruczołów dokrewnych (21,5 proc.), emocje (16,5 proc.). Wskazanie odpowiedzi dotyczących pomiaru poziomu stresu i emocji odczuwanych przez badanego jest związane z mitami powszechnie funkcjonującymi w społeczeństwie. P. Ekman uważał między innymi, że na podstawie badania poligraficznego można stwierdzić, czy osoba badana odczuwa w czasie przeprowadzania procedury określone emocje, np. złość, strach⁸.

Na wykresie 3 przedstawiono wskazania ankietowanych dotyczące możliwości wykorzystania badań poligraficznych w procedurach naboru do pracy.

⁸ P. Ekman, *Kłamstwo i jego wykrywanie...*, s. 171–216.



Wykres 3. Stosowanie poligrafu w badaniach kadrowych w ocenie ankietowanych.

Źródło: Opracowanie własne autorów.

Poza odpowiedziami zgodnymi z rzeczywistością, np. sprawdzeniem wiarygodności kandydata (71,5 proc. ankietowanych), weryfikacją danych z CV lub informacji przekazywanych podczas rozmowy kwalifikacyjnej (36 proc.), padały także takie, które wskazywały np. na możliwość ustalenia, czy kandydat zamierza⁹ postępować uczciwie w nowym miejscu pracy (25,5 proc.), a nawet określenia prędkości procesów metabolicznych organizmu w miejscu zatrudnienia (4 proc.).

Funkcje badań poligraficznych

Pięćdziesiąt jeden procent respondentów uznało, że stosowanie badań poligraficznych na szerszą skalę przyczyniłoby się do poprawy działania organów państwowych (w tym służb mundurowych) i przedsiębiorstw prywatnych. Natomiast 49 proc. osób było przeciwnego zdania. Przedstawiciele pierwszej grupy twierdzili, że badania poligraficzne pozwalają wykluczyć nieodpowiednich kandydatów do pracy lub służby, o czym świadczą następujące wypowiedzi: *Jest to szczególnie ważne w przypadku służb. Byłaby to również dodatkowa metoda na potwierdzenie lojalności pracowników oraz weryfikacji ich działań.* Podkreślali także ich walor prewencyjny, np.: *Dzięki nim możliwe jest zmniejszenie liczby oszustw i kradzieży oraz zniechęcenie niewłaściwych osób do aplikowania na dane stanowiska.*

Prewencyjna rola badań poligraficznych znajduje swoje odzwierciedlenie przede wszystkim w badaniach osób skazanych za przestępstwa przeciwko wolności

⁹ Poligraf to nie szklana kula!

seksualnej, a zwolnionych warunkowo, które są praktykowane w Stanach Zjednoczonych i Wielkiej Brytanii. Wśród ankietowanych 75 proc. wskazało, że takie badania byłyby przydatne także w Polsce¹⁰. Argumentowano to m.in. w ten sposób: (...) można byłoby dowiedzieć się, czy takie osoby nadal nie zagrażają bezpieczeństwu innych; sprawdzić ich funkcjonowanie na wolności, np.: (...) w celu weryfikacji, czy osoba nie popełniła kolejnych przestępstw lub złamała warunki zwolnienia warunkowego. Pozostałe 25 proc. ankietowanych odpowiedziało, że badania poligraficzne nie powinny być w ten sposób wykorzystywane, ponieważ byłyby to rozwiązanie (...) niezgodne z prawem i ograniczające wolność osobistą takich osób. Jeden z ankietowanych poruszył m.in. kwestię prywatności osób badanych:

(...) dzięki badaniom poligraficznym zastosowanym wobec osób skazanych za przestępstwa seksualne można by monitorować codzienną aktywność tych osób i zapobiegać ewentualnemu popełnieniu przestępstwa seksualnego w przyszłości. Jednak stosować te badania wobec ww. osób powinno się jedynie wtedy, gdy badania psychiatryczne wykazują możliwość powrotu na drogę przestępczą czy spalenie psychiczne byłego skazańca. (...) taka kontrola na etapie postpenitencjarnym wobec osoby resocjalizującej się może być zbyt daleko idącą ingerencją w jej prawa i wolności osobiste (prawo do prywatności).

Część ankietowanych zwróciła uwagę również na koszty.

Zwolennicy badań poligraficznych dostrzegają też możliwość pozyskiwania istotnych informacji w śledztwach, m.in.: *Jestem zwolenniczką stosowania badań poligraficznych, przede wszystkim w sądach. Jest dużo spraw dotyczących np. podrabiania podpisów, testamentów, anonimów itp. Po takim badaniu nie byłoby wątpliwości; czy: Badanie poligraficzne na etapie postępowania przygotowawczego już mogłoby nakierować organy ścigania na obranie odpowiedniego kierunku działań – dowód poszlakowy.* Za wykorzystaniem badań poligraficznych w procesie karnym opowiedziało się 76 proc. ankietowanych, a 24 proc. wyraziło swój sprzeciw. Zwolennicy uznali je za „wartościowy dowód”, widząc szczególną przydatność przy rozwiązywaniu zawiłych spraw albo w takich sprawach, w których występuje słowo przeciwko słowu. Dodawano także postulat ostrożnej interpretacji, np.: *Zapewne jest to metoda dająca pewien pogląd ma daną sytuację. Mimo wątpliwości co do 100 proc. wiarygodności, mogą być one bardzo przydatne, choć nie powinny być uznawane za pewnik, a ich rezultaty weryfikowane za pomocą innych metod.*

Jednocześnie postulowano potraktowanie badań poligraficznych jako metody pomocniczej, np.: *Mogą być użytecznym źródłem wiedzy, jeśli będą stosowane w połączeniu z innymi metodami, np. wywiadem bądź: Badanie tym narzędziem mogłoby*

¹⁰ Szerzej na ten temat zob. M. Gołaszewski, *Użyteczność badań poligraficznych w ograniczaniu recydywy wśród sprawców przestępstw przeciwko wolności seksualnej*, „Prokuratura i Prawo” 2016, nr 12, s. 5–22.

pomóc w doborze osób na ważne stanowiska państwowe albo w danej firmie. Nie chodzi tu o to, aby opierać się tylko na wynikach z badania poligrafem, ale traktować je jako wskazówkę bądź usprawnienie procesu rekrutacyjnego, mówiące o tym, co należałoby jeszcze sprawdzić albo na co zwrócić szczególną uwagę.

Natomiast przeciwnicy badań poligraficznych argumentowali swoje stanowisko tym, że rzekomo są one (...) *niemiarodajne*, a ich wyniki mogą być związane ze (...) *stanem zdrowia, przyjmowanymi lekami, wiekiem, stresem związanym z badaniem itp., wcześniejsze zaś przygotowanie do badania umożliwia oszukanie urzędnika*. Ta grupa ankietowanych uważa, że nie należy wykorzystywać badań poligraficznych w procesie karnym, ponieważ: (...) *trafność badania jest wątpliwa; (...) sytuacja emocjonalna związana z badaniem ma wpływ na otrzymany wynik; (...) ekspertyza jest kosztowna*.

3. Badania poligraficzne funkcjonariuszy w instytucjach państwowych

W odniesieniu do wykorzystania badań poligraficznych w służbach mundurowych 85 proc. badanych wskazało na ich przydatność, o czym świadczą m.in. takie wypowiedzi: *Jest to wyjątkowo odpowiedzialna i wymagająca praca, dlatego trzeba mieć pewność że kandydat nie ma powiązań np. z grupami handlującymi narkotykami. Praca jest też wybitnie obciążająca, dlatego warto badać w trakcie służby, czy ktoś nie pękł i nie przeszedł na ciemną stronę mocy oraz: Uważam, że w procesie rekrutacji do służb szczególnie ważnych dla obronności i bezpieczeństwa kraju badanie poligrafem jest znakomitym i adekwatnym (co prawda, wchodzi w sferę prywatną osoby rekrutowanej, ale jest to uzasadnione specyfiką sytuacji) sposobem na weryfikację kandydatów.*

Stosowania poligrafu w procesie rekrutacji do służb nie poparło 15 proc. ankietowanych. Pojawiały się wypowiedzi typu: *Moim zdaniem badania poligraficzne nie mogą być źródłem informacji o rekrucie, mają zbyt duży wskaźnik błędu czy: Uważam, że to dodatkowy, niepotrzebny stres dla kandydata, który i tak przechodzi skrupulatną weryfikację.*

Pierwszą polską służbą mundurową, która w latach 60. XX w. kupiła poligraf Keelera (model 6308), była Wojskowa Służba Wewnętrzna – formacja łącząca funkcje policji wojskowej i kontrwywiadu wojskowego. Później poligraf nabyło Ministerstwo Spraw Wewnętrznych, w którego strukturze były: wywiad cywilny (Departament I) i kontrwywiad cywilny (Departament II). W obydwu instytucjach poligrafy służyły przede wszystkim do celów szkoleniowych.

Prawdopodobnie z działaniem poligrafu zapoznawano także agentów wywiadu, zakładając, że mogą oni być w przyszłości poddani tego rodzaju badaniom (np. przez służby amerykańskie). W Wojskowej Służbie Wewnętrznej poligraf wykorzystywano w sprawach karnych – w śledztwach prowadzonych przez prokuratury wojskowe, szczególnie w sprawach kradzieży broni. Eksperci WSW byli też powoływani przez prokuratury powszechne do wykonywania badań poligraficznych w najpoważniejszych sprawach karnych, zwłaszcza w sprawach o zabójstwa.

W strukturach Milicji Obywatelskiej do 1989 r. nie było żadnej komórki badań poligraficznych, a w razie potrzeby korzystano z usług ekspertów WSW lub uniwersyteckich. W tamtym czasie nie wykonywano badań poligraficznych kandydatów ani do służb policyjnych, ani specjalnych.

Zmiana nastąpiła po 1989 r., po upadku komunizmu. Uniezależnienie się od ZSRR, reforma służb specjalnych i policyjnych oraz nawiązanie nieskrępowanej współpracy w różnych dziedzinach z państwami zachodnimi, w tym Stanami Zjednoczonymi, pozwoliło na szersze niż do tej pory stosowanie badań poligraficznych i wykorzystanie wzorów zachodnich. Policja, która zastąpiła Milicję Obywatelską, kupiła pierwsze poligrafy i zorganizowała centralny ośrodek badań poligraficznych w Warszawie oraz cztery ośrodki terenowe. Również Urząd Ochrony Państwa, utworzony w 1990 r., uruchomił swoją komórkę badań poligraficznych. Takie komórki powstały także w Straży Granicznej i Żandarmerii Wojskowej.

Obecnie badania poligraficzne znajdują zastosowanie w postępowaniach kwalifikacyjnych i kontrolnych (ang. *screening*) większości służb policyjnych i specjalnych. Procedury przyjęć (rekrutacyjne) do służby są określone ustawowo i przewidują obowiązkowe badania poligraficzne kandydatów. Wykorzystuje się je również do sprawdzania lojalności funkcjonariuszy służb oraz żołnierzy. Liczba badań przeprowadzonych na użytek wewnętrzny w służbach policyjnych i specjalnych nie jest znana, ale można szacować, że jest ich co najmniej kilkakrotnie więcej niż w sprawach karnych.

Lojalność wspomniana w wypowiedziach ankietowanych to postawa charakteryzująca się m.in. przestrzeganiem przepisów prawa, wiernością wobec siebie osób połączonych wzajemnym zaufaniem i uczciwością w kontaktach międzyludzkich¹¹. Objawia się dotrzymywaniem przyjętych zobowiązań oraz respektowaniem zasad honoru i prawości¹². Lojalność pracownicza jest postawą, przez którą rozumie się m.in. chęć pozostania pracownika w organizacji i wykonywanie z zaangażowaniem powierzonych mu obowiązków, bez względu na występujące problemy w miejscu zatrudnienia¹³. Lojalność w służbach mundurowych jest warunkowana z jednej strony względami pragmatycznymi wynikającymi z trwałego stosunku służbowego i dążeń do awansu w strukturach hierarchicznych. Z drugiej zaś ma podłoże w wartościach, postawach obywatelskich i patriotycznych oraz osobistej satysfakcji funkcjonariuszy ze służby. Z badań ankietowych i wywiadów przeprowadzonych w latach 2015–2016 wśród pracowników polskich przedsiębiorstw wynika, że lojalny pracownik jest opisywany jako osoba uczciwa, szczerą, sumiennie i rzetelnie wykonująca swoje obowiązki¹⁴. Konformistyczne

¹¹ M. Jarosz, *Słownik wyrazów obcych*, Wrocław 2001.

¹² M.S. Szczepański, *Lojalność*, w: *Fundamenty dobrego społeczeństwa. Wartości*, M. Bogunia-Borowska (red.), Kraków 2015.

¹³ A. Lipka, A. Winnicka-Wejs, J. Acedański, *Lojalność pracownicza. Od diagnozy typów pracowników do Zarządzania Relacjami z Pracownikami (Employee Relationship Management)*, Warszawa 2012.

¹⁴ E. Robak, *Lojalność pracowników a zarządzanie potencjałem społecznym współczesnych organizacji*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie” 2016, nr 24, s. 82–95.

podporządkowanie się organizacji nie wysuwa się tutaj na pierwszy plan, choć z pewnością ma większe znaczenie w służbach niż w sektorze prywatnym. Przed podjęciem służby w różnych instytucjach funkcjonariusze ślubują według roty, która uwzględnia takie przyrzeczenia związane z lojalnością, jak: służba Narodowi, wierność konstytucyjnym organom Rzeczypospolitej Polskiej, pilne przestrzeganie prawa i dyscypliny służbowej, wykonywanie rozkazów, strzeżenie honoru, godności oraz dobrego imienia danej służby.

Kandydaci do służby w: Policji, Centralnym Biurze Antykorupcyjnym, Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Żandarmerii Wojskowej, Służbie Wywiadu Wojskowego, Służbie Kontrwywiadu Wojskowego oraz Krajowej Administracji Skarbowej są poddawani badaniom poligraficznym przed ich zatrudnieniem. Celem tych badań jest sprawdzenie przydatności danego kandydata do służby na danym stanowisku lub w określonej komórce organizacyjnej i eliminacja tych spośród kandydatów, którzy z określonych powodów nie powinni pełnić służby lub pracować na określonym stanowisku. W przypadku ABW i AW, SKW i SWW¹⁵, CBA oraz Straży Granicznej¹⁶ badanie poligraficzne może być przeprowadzone w przypadku kandydatów na stanowiska, które wymagają szczególnych umiejętności lub predyspozycji (dotyczy to niemal wszystkich stanowisk).

Badaniom poligraficznym są poddawani także funkcjonariusze i pracownicy wymienionych instytucji. O skierowaniu funkcjonariusza na badanie poligraficzne w służbach specjalnych decydują szefowie tych służb. Nie muszą oni przy tym uzasadniać swojej decyzji. Jest to element kontroli funkcjonariusza. Ewentualna odmowa poddania się badaniu może być potraktowana jako niewykonanie polecenia służbowego, czyli delikt dyscyplinarny. Przeprowadzenie badania poligraficznego wobec funkcjonariusza zostało ściśle określone w Straży Granicznej i jest ono możliwe w przypadku skierowania funkcjonariusza na szkolenie oraz prowadzenia postępowania w sprawie o przestępstwo popełnione w związku z wykonywaniem czynności służbowych¹⁷.

W Krajowej Administracji Skarbowej badaniom poligraficznym są poddawani kandydaci przewidziani do służby w większości komórek organizacyjnych Służby

¹⁵ *Rozporządzenie Ministra Obrony Narodowej z dnia 26 lipca 2006 r. w sprawie postępowania kwalifikacyjnego wobec kandydatów do służby w Służbie Kontrwywiadu Wojskowego (Dz.U. z 2006 r. nr 137 poz. 978); Rozporządzenie Ministra Obrony Narodowej z dnia 26 lipca 2006 r. w sprawie postępowania kwalifikacyjnego wobec kandydatów do służby w Służbie Wywiadu Wojskowego (Dz.U. z 2006 r. nr 137 poz. 979).*

¹⁶ *Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j.: Dz.U. z 2017 r. poz. 2365).*

¹⁷ Zgodnie z art. 1 ust. 2a ustawy o Straży Granicznej Straż Graniczna prowadzi postępowania w sprawach rozpoznawania i wykrywania przestępstw określonych w art.: 228 (łapownictwo bierne), 229 (łapownictwo czynne) i 231 (nadużycie uprawnień, niedopełnienie obowiązków) kodeksu karnego, popełnionych przez funkcjonariuszy Straży Granicznej w związku z wykonywaniem czynności służbowych oraz zapobieganie im. W takim przypadku funkcjonariusza kieruje na badanie Komendant Główny Straży Granicznej.

Celno-Skarbowej¹⁸. W celu sprawdzenia przydatności do służby na danym stanowisku badaniom mogą być poddani także funkcjonariusze tego organu (szczególnie ci, którzy są uprawnieni do wykonywania czynności operacyjno-rozpoznawczych).

Warto przy tym zwrócić uwagę na obowiązujące w KAS kryteria, które powinna spełniać osoba przeprowadzająca badania poligraficzne. Zgodnie z § 7 rozporządzenia ministra rozwoju i finansów w sprawie przeprowadzania badania psychofizjologicznego, testu sprawności fizycznej oraz badania psychologicznego funkcjonariuszy Służby Celno-Skarbowej¹⁹ poligrafer

(...) posiada tytuł magistra oraz ukończył kurs specjalistyczny i uzyskał stosowny certyfikat autoryzowany lub uznany przez American Polygraph Association (APA) lub kurs z zakresu badań poligraficznych na poziomie co najmniej podstawowym, lub posiada odpowiednie, nabyte w innej drodze umiejętności prawidłowego przeprowadzania badania poligraficznego i interpretacji jego wyników poświadczone przez polskie organizacje z zakresu badań poligraficznych, w tym Polskie Towarzystwo Badań Poligraficznych.

Wymienione rozporządzenie jest najnowszym dokumentem tej rangi w Polsce, który reguluje kwalifikacje poligrafera.

W Policji badania poligraficzne mają służyć określeniu predyspozycji danego funkcjonariusza do pełnienia służby na określonych stanowiskach lub w określonych komórkach organizacyjnych, zwłaszcza ustaleniu: lojalności wobec służby, czy nie czerpie on nieuprawnionych korzyści w służbie, a także patologii i niepożądanych uzależnień w służbie. Podczas badania poligraficznego nie zadaje się pytań dotyczących wyznania oraz preferencji seksualnych i politycznych. Przebieg badania jest rejestrowany (obraz i dźwięk), a jeśli jego wynik jest niejednoznaczny, takie badanie można powtórzyć tylko jeden raz w ciągu 30 dni²⁰.

Badania kontrolne mają na celu głównie sprawdzenie, czy od ostatniego badania funkcjonariusze nie ujawnili informacji niejawnych, nie nawiązali niepożądanych kontaktów, nie popełnili przestępstw lub przewinień dyscyplinarnych itp.

Spośród wszystkich służb wykonujących zadania w zakresie bezpieczeństwa państwa jedynie w przypadku Biura Ochrony Rządu brakowało regulacji ustawowych, które wprowadzałyby obowiązek – i jednocześnie możliwość – przeprowadzenia badań poligraficznych zarówno wobec kandydatów do służby, jak i funkcjonariuszy.

¹⁸ Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. z 2016 r. poz. 1947, ze zm.).

¹⁹ Rozporządzenie Ministra Rozwoju i Finansów z dnia 10 kwietnia 2017 r. w sprawie przeprowadzania badania psychofizjologicznego, testu sprawności fizycznej oraz badania psychologicznego funkcjonariuszy Służby Celno-Skarbowej (Dz.U. z 2017 r. poz. 805).

²⁰ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 marca 2007 r. w sprawie trybu i warunków ustalania zdolności fizycznej i psychicznej policjantów do służby na określonych stanowiskach lub w określonych komórkach organizacyjnych jednostek Policji (Dz.U. z 2007 r. nr 62 poz. 423).

W Służbie Ochrony Państwa, która w 2018 r. zastąpiła BOR, przewidziano już obowiązkowe badania psychofizjologiczne dla kandydatów do służby i fakultatywne dla funkcjonariuszy, pracowników SOP lub funkcjonariuszy innych instytucji państwowych przenoszonych do służby w SOP.

Nie ulega wątpliwości, że skoro uprawnienie do wykonywania badań poligraficznych kandydatów do służby i funkcjonariuszy ma oparcie w przepisach rangi ustawowej, to znaczy, że żaden inny urzędnik państwowy nie może być poddawany takim badaniom, jeśli ustawa tego nie przewiduje.

Służby policyjne i specjalne, które realizują czynności operacyjno-rozpoznawcze, mogą ponadto wykonywać badania poligraficzne wobec osób udzielających pomocy przy takich czynnościach.

Badania poligraficzne są dopuszczalne także w postępowaniach dyscyplinarnych prokuratorów. Przepisy ustawy – Prawo o prokuraturze²¹ (w rozdziale dotyczącym odpowiedzialności karnej, dyscyplinarnej i służbowej prokuratorów), mówią o tym, że rzecznik dyscyplinarny podczas prowadzonego postępowania dyscyplinarnego może – w celu ograniczenia kręgu osób podejrzanych o popełnienie przewinienia dyscyplinarnego zawierającego znamiona przestępstwa ujawnienia informacji z postępowania karnego stanowiących informacje niejawne o klauzuli „tajne” lub „ściśle tajne” – powołać biegłego w celu zastosowania wobec prokuratora mającego dostęp do tych informacji, za jego zgodą, środków technicznych kontrolujących nieświadome reakcje organizmu. Wymagana jest też zgoda prokuratora generalnego²².

Wieloletnie doświadczenia pozostałych polskich służb mundurowych dowodzą wysokiej wartości badań psychofizjologicznych z wykorzystaniem poligrafu, ponieważ dzięki nim zdobywa się cenne informacje, trudne lub wręcz niemożliwe do uzyskania w ramach innych dostępnych procedur. Mimo to badania przeprowadzane w instytucjach państwowych wywołują niekiedy rozmaite kontrowersje, które występują na dwóch płaszczyznach. Pierwsza jest związana z dopuszczalnością takich badań w sensie formalno-prawnym i etycznym, a wątpliwości w tym zakresie są zgłaszane przez osoby spoza służb, z naciskiem na rzekomo wysoki poziom błędów badań poligraficznych. Druga płaszczyzna to zagadnienia standaryzacji badań i polityka zapewnienia jakości. Ta część dyskusji toczy się między resortami oraz w gronie funkcjonariuszy poszczególnych instytucji.

Dopuszczalność badań poligraficznych kandydatów do służby oraz funkcjonariuszy już zatrudnionych była w Polsce przedmiotem badań Trybunału Konstytucyjnego²³, który nie dopatrywał się niekonstytucyjności przepisów ustawy pozwalających na takie badania w Policji. Organom państwowym wolno czynić tylko to, co jest przez ustawę nakazane lub dozwolone. Zakres tych kompetencji został wyżej wskazany dla poszczególnych instytucji i nie powinien budzić wątpliwości.

²¹ Ustawa z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (t.j.: Dz.U. z 2017 r. poz. 1767).

²² Tamże, art. 154.

²³ Wyrok Trybunału Konstytucyjnego z dnia 23 lutego 2010 r. K. 1/2008 LexPolonica nr 2144497, OTK ZU 2010/2A, poz. 14.

W sektorze prywatnym natomiast obowiązuje zasada, że co nie jest przez prawo zabronione, należy uznać za dozwolone. Badania poligraficzne są w firmach wykonywane zwykle w ramach rekrutacji oraz w sytuacjach, gdy podejrzewa się, że pracownik może działać na niekorzyść pracodawcy. A. Drozd wskazuje na głosy przedstawicieli prawa pracy, którzy zwracają uwagę na związane z tym naruszanie dóbr osobistych, wolności, godności i sfery życia prywatnego jednostki²⁴. Według tego autora badania kadrowe z wykorzystaniem poligrafu mogą być dopuszczone jedynie wtedy, gdy zostaną ustanowione normy niebudzące wątpliwości oraz gdy kandydat lub pracownik wyraziłby dobrowolną zgodę na ich przeprowadzenie. Te warunki są zgodne z obowiązującymi standardami American Polygraph Association²⁵ i Polskiego Towarzystwa Badań Poligraficznych. J. Pietruszka i R. Rogalski konstatują, że badania poligraficzne są dla pracodawcy często nieocenionym źródłem wiedzy i pozwalają na zdobycie informacji, do których nie dotarłby w inny sposób²⁶.

Oponenti często przedstawiają pod adresem badań poligraficznych nierealny postulat bezwzględnej trafności, przytaczając jednocześnie zaniżone dane (np. 75 proc. dokładności)²⁷. Należy podkreślić, że badania poligraficzne mają bardzo wysoką i prawdopodobnie najlepiej zbadaną wartość diagnostyczną w stosunku do innych metod wykorzystywanych w kryminalistyce. Średnia dokładność wszystkich typów testów poligraficznych, potwierdzona badaniami naukowymi, wynosi 87,1 proc.²⁸ Dla testów diagnostycznych (jednoproblemowych) jest to 92,1 proc., a dla przesiewowych (wieloproblemowych) – 85 proc. Dane dotyczące dokładności technik badań poligraficznych wynikają z rozmaitych badań naukowych prowadzonych na przestrzeni XX i XXI wieku. Brane są pod uwagę te badania naukowe, które spełniają naukowe standardy i zostały opublikowane w czasopismach niezależnie recenzowanych i monografiach naukowych. W rezultacie metaanalizy danych pochodzących z wielu badań powstały m.in. dwa ważne raporty podsumowujące średnią dokładność badań poligraficznych ogółem, a także poszczególnych typów badań i technik badawczych. Jeden ze wspomnianych raportów wydała w 2003 r. amerykańska National Research Council. Potwierdzono wówczas wskaźnik dokładności badań poligraficznych prowadzonych w „konkretnych sprawach”, który wynosił ok. 90 proc. Drugi raport został opracowany przez APA w 2011 r. i obecnie uznaje się go za najlepszy punkt odniesienia. Jak w każdej innej dziedzinie nauki, dane opublikowane w raporcie należy uznać za obowiązujące dopóty, dopóki nowe wyniki dowodów naukowych nie zaowocują istotną zmianą.

²⁴ A. Drozd, *O dopuszczalności wykorzystywania wariografu w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne” 2003, nr 4, s. 9–14.

²⁵ *Code of Ethics*, [http://www.polygraph.org/assets/docs/Misc.Docs/2015 proc.20code proc.20of proc.20ethics.pdf](http://www.polygraph.org/assets/docs/Misc.Docs/2015%20proc.20code%20proc.20of%20ethics.pdf) [dostęp: 25 V 2017].

²⁶ J. Pietruszka, R. Rogalski, *Nie odbierać prawa do obrony – artykuł dyskusyjny o poligrafie*, „Praca i Zabezpieczenie Społeczne” 2004, nr 11, s. 15–21.

²⁷ Zob. m.in. P. Słowik, *Rekrutacja do Straży Granicznej: Wariograf wątpliwy, ale nie dla MSWiA*, „Gazeta Prawna” z 14 III 2017 r., <http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1026987,rekrutacja-do-strazy-granicznej-badanie-wariografem-w-sadzie.html> [dostęp: 26 III 2017].

²⁸ *Meta-Analytic Survey of Criterion Accuracy of Validated Techniques*, „Polygraph” 2011, nr 4.

W kontekście dokładności testów stosowanych w badaniach poligraficznych bardziej zasadny jest postulat minimalizacji ryzyka błędu, wyrażony w marcu 2017 r. m.in. przez przedstawiciela Helsińskiej Fundacji Praw Człowieka²⁹. Temu postulatu wychodzą naprzeciw standardy profesjonalne. Jeśli jakiś test, a tym bardziej całe badanie poligraficzne, jest na pewnym etapie nierozstrzygnięty, to należy wykonać dodatkowe testy (w ramach tego samego badania lub kolejnego – powtórnego). Z kolei podejście tzw. sukcesywnego pokonywania przeszkód wymaga, aby przy niekorzystnym dla badanego wyniku testu przesiewowego przeprowadzić test diagnostyczny w celu weryfikacji powstałych wątpliwości. Technicznie oznacza to, że po teście o mniejszej dokładności (średnio 85 proc.), powinien nastąpić test bardziej dokładny (średnio 92,1 proc.).

Należy też wyraźnie podkreślić, że nie wolno stawiać znaku równości między stanowiskami w instytucjach rządowych i organach egzekwowania prawa a miejscami pracy w zwykłych urzędach czy zakładach pracy. Nikomu nie trzeba chyba tłumaczyć, że z punktu widzenia bezpieczeństwa państwa lepiej odrzucić pewien procent kandydatów – być może nie do końca słusznie ocenionych – niż pozwolić na przejście przez rekrutacyjne sito jednostce, która może wyrządzić poważne szkody Rzeczypospolitej Polskiej. Interes związany z bezpieczeństwem państwa i ochroną informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami³⁰.

Zasady przeprowadzania badań poligraficznych określają ogólnodostępne standardy organizacji profesjonalnych i normalizacyjnych o zasięgu międzynarodowym (APA, ASTM International) oraz krajowym (m.in. Polskie Towarzystwo Badań Poligraficznych). Ponadto w różnych instytucjach państwowych, w których przeprowadza się badania poligraficzne, obowiązują wewnętrzne instrukcje i zarządzenia regulujące wykonywanie takich badań. Standardy zostały omówione w polskojęzycznych publikacjach naukowych³¹ i są powszechnie dostępne, zatem bariera językowa nie jest dostatecznym usprawiedliwieniem, aby je ignorować.

Do badań kadrowych typu *screening* rekomenduje się techniki, które są potwierdzone naukowo i mają poziom dokładności wyższy niż statystyczna szansa. Mogą być stosowane wraz z podejściem tzw. sukcesywnego pokonywania przeszkód.

Poszczególne testy, w powiązaniu z określonym systemem analizy danych testowych, różnią się między sobą nie tylko dokładnością, lecz także czułością na kłamstwo i swoistością. Optymalnym rozwiązaniem wydaje się dobór takiej techniki, która ma te parametry zrównoważone. Polityka danej instytucji może jednak przewidywać, że celem nadrzędnym jest jak najwyższa czułość na kłamstwo, nawet kosztem swoistości

²⁹ P. Słowik, *Rekrutacja do Straży Granicznej...*

³⁰ Zob. art. 24. ust. 4 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (t.j.: Dz.U. z 2016 r. poz. 1167, ze zm.).

³¹ *Współczesne standardy badań poligraficznych*, M. Gołaszewski (red.), seria: Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego, Warszawa 2013; M. Gołaszewski, M. Widacki, *Aktualny standard badań poligraficznych a praktyka polska*, w: *Badania poligraficzne w Polsce*, J. Widacki (red.), Kraków 2014.

testu (skutecznego potwierdzenia prawdomówności badanego). Regulacji mogą podlegać także progi decyzyjne przy ocenach numerycznych – w zależności od akceptowanej tolerancji błędu. Standardowo przyjmuje się tolerancję błędu przy wynikach korzystnych dla badanego na poziomie 10 proc. System można by jednak uszczelnić, obniżając tę tolerancję do 5 proc. (tak jak to jest w przypadku wyników wskazujących na nieszczerłość).

Możliwość wyboru testu spośród kilkunastu nie powinna jednak oznaczać zupełnej dowolności. Na uwagę zasługuje stosowanie testu R/I (tzw. klasycznego), który powoli odchodzi do historii, a mała dokładność (na poziomie ok. 75 proc.), w połączeniu z bardzo niską swoistością i wyłącznie jakościową (globalną) metodą ewaluacji wykresów, podają w wątpliwość sens jego stosowania w ogóle. W pewnych warunkach ten test bywa użyteczny, jednak w normalnej sytuacji trudno zrozumieć jakiegokolwiek argumenty za jego wyborem (poza prostotą techniki i wygodą badającego), skoro istnieją inne, o parametrach pod każdym względem korzystniejszych. Podobne zastrzeżenia może budzić także stosowanie testów szczytowego napięcia (ang. *Peak of Tension*, POT) z tego względu, że ich wyniki są podstawą wydania opinii o wiarygodności osoby badanej. Test typu POT w wersji z poszukiwanym rozwiązaniem ma charakter wyłącznie pomocniczy.

Na gruncie tego typu wątpliwości pojawia się temat tzw. kontroli jakości czy – delikatniej rzecz ujmując – „polityki zapewnienia jakości”. W Stanach Zjednoczonych takie procedury funkcjonują z powodzeniem. Z jednej strony pomagają eliminować patologie (np. wyniki „na zamówienie”), ograniczać subiektywizm badających, mobilizować do doskonalenia zawodowego, a z drugiej – samym badającym zapewniają ochronę przed naciskami zewnętrznymi i próbami podważania opinii. W Polsce, w różnych instytucjach i różnym zakresie, wprowadzono wewnętrzne procedury obejmujące między innymi tzw. ślepą ocenę poligramów, sprawdzania wybranych badań w całości („na żywo” lub z odtworzenia) i nadzór merytoryczny właściwych przełożonych. Brakuje natomiast organu kontrolnego, który koordynowałby programy badań poligraficznych na poziomie centralnym, międzyresortowym, i odpowiadałby równocześnie za proces szkolenia ekspertów i badania naukowe (na wzór National Center for Credibility Assessment w Stanach Zjednoczonych).

Podobny problem występuje przy badaniach poligraficznych w procesie karnym, w których, wobec braku procedur licencyjnych, działalność biegłych pozostaje jedynie pod formalną kontrolą sądową i, ewentualnie, naukową oraz środowiskową. Część biegłych działa poza strukturami stowarzyszeń zawodowych i nie jest zainteresowana utrzymaniem jakichkolwiek kontaktów z ekspertami.

Podsumowując, należy stwierdzić, że niezależnie od wskazanych kontrowersji i problemów badania poligraficzne w polskich instytucjach państwowych są stosowane w szerokim zakresie. Wydaje się, że poligraferzy zapracowali na ugruntowaną pozycję i renomę u osób kierujących służbami i tzw. resortami siłowymi. Tylko wysoka jakość systematycznie realizowanych ekspertyz (szczególnie na potrzeby procesu karnego) oraz aktywność w przestrzeni publicznej samego środowiska

ekspertów tej specjalności przyczynią się do postrzegania badań poligraficznych przez społeczeństwo jako spójne z obrazem tych badań w służbach i adekwatne do rzeczywistych możliwości diagnostycznych.

Bibliografia:

1. *Code of Ethics*, American Polygraph Association, [http://www.polygraph.org/assets/docs/Misc.Docs/2015 proc.20code proc.20of proc.20ethics.pdf](http://www.polygraph.org/assets/docs/Misc.Docs/2015%20proc.20code%20of%20ethics.pdf) [dostęp: 28 V 2017].
2. Drozd A., *O dopuszczalności wykorzystywania wariografu w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne” 2003, nr 4.
3. Ekman P., *Kłamstwo i jego wykrywanie w biznesie, polityce i małżeństwie*, Warszawa 2006, Wydawnictwo Naukowe PWN.
4. Gołaszewski M., *Użyteczność badań poligraficznych w ograniczaniu recydywy wśród sprawców przestępstw przeciwko wolności seksualnej*, „Prokuratura i Prawo” 2016, nr 12.
5. Herbowski P., *Wykrywcze wykorzystanie wyników badań poligraficznych*, „Problemy Kryminalistyki” 2010, nr 267.
6. Honts C.R. i in., *General acceptance of the polygraph by the scientific community: Two surveys of professional attitudes*, referat zaprezentowany podczas zjazdu APLS w Austin (Texas, USA) w 2002 r.
7. Jarosz M., *Słownik wyrazów obcych*, Wrocław 2001, Europa.
8. Lipka A., Winnicka-Wejs A., Acedański J., *Lojalność pracownicza. Od diagnozy typów pracowników do Zarządzania Relacjami z Pracownikami (Employee Relationship Management)*, Warszawa 2012, Difin.
9. *Meta-Analytic Survey of Criterion Accuracy of Validated Techniques*, „Polygraph” 2011, nr 4.
10. Moszczyński J., *Subiektywizm w badaniach kryminalistycznych*, Olsztyn 2011, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.
11. Niziołek K., *Ocena trafności badań psychofizjologicznych w odniesieniu do polskiego procesu karnego*, prezentacja z Ogólnopolskiej Konferencji Naukowej „Rola badań psychofizjologicznych w rozumieniu i korekcji funkcjonowania człowieka”, 18 V 2017, Uniwersytet Kardynała Stefana Wyszyńskiego, Warszawa.
12. Pietruszka J., Rogalski R., *Nie odbierać prawa do obrony – artykuł dyskusyjny o poligrafie*, „Praca i Zabezpieczenie Społeczne” 2004, nr 11.

13. Robak E., *Lojalność pracowników a zarządzanie potencjałem społecznym współczesnych organizacji*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie” 2016, nr 24.
14. Słowik P., *Rekrutacja do Straży Granicznej: wariograf wątpliwy, ale nie dla MSWiA*, „Gazeta Prawna” z 14 III 2017 r., <http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1026987,rekrutacja-do-strazy-granicznej-badanie-wariografem-w-sadzie.html> [dostęp: 26 III 2017].
15. Szczepański M.S., *Lojalność*, w: *Fundamenty dobrego społeczeństwa. Wartości*, Bogunia-Borowska M. (red.), Kraków 2015, Znak.
16. Widacki J., *Badania poligraficzne w Polsce*, Kraków 2014, Polskie Towarzystwo Badań Poligraficznych.
17. *Współczesne standardy badań poligraficznych*, M. Gołaszewski (red.), seria: Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego, Warszawa 2013.

Abstrakt

Problem badań psychofizjologicznych z wykorzystaniem poligrafu jest przyczyną wielu dyskusji na gruncie naukowym i społecznym. Zwykle ma to związek z ograniczonym dostępem do wiedzy w tym zakresie i w konsekwencji – z powszechnymi przekonaniami panującymi w polskiej opinii publicznej. W artykule zostały przedstawione wyniki przeprowadzonej ankiety, uwzględniającej takie zmienne, jak: znajomość istoty badań poligraficznych, doświadczenie w zakresie wykorzystania metody tego typu badań, opinie dotyczące praktycznego zastosowania badań poligraficznych (zarówno podczas rekrutacji, jak i na etapie zatrudnienia na określonych stanowiskach czy w postępowaniu karnym). Wyniki wskazują na skromny zakres wiedzy na temat tych badań w społeczeństwie, w dużej mierze oparty na nieprawidłowym lub niedostatecznym przedstawianiu metody w mediach, prasie i literaturze (również obejmującej zagadnienia specjalistyczne). Ten obraz zestawiono z użytecznością badań poligraficznych w różnych obszarach praktyki – szczególnie w instytucjach państwowych (służbach mundurowych i innych).

Słowa kluczowe: poligraf, badania psychofizjologiczne, detekcja nieuczciwości, użyteczność, funkcjonariusze, instytucje państwowe, lojalność, społeczeństwo, ankieta.

Marek Świerczek

Wewnętrzne źródła porażki Oddziału II Sztabu Generalnego Wojska Polskiego w starciu z Państwowym Zarządem Politycznym przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej podczas operacji dezinformacyjnej sowieckiego kontrwywiadu, znanej jako „afera MOCR-Trust”

Niełatwo znaleźć odpowiedź na pytanie, jak doszło do tego, że w 1921 r. Oddział II rozpoczął współpracę agenturalną z KRO GPU¹, która trwała niemal sześć lat. Gdy ten fakt wyszedł na jaw, zamiast podjąć kroki zaradcze, Oddział II SG WP zrezygnował z działalności na Wschodzie, zastępując ją pracą obserwacyjną, z której słabości świetnie zdawali sobie sprawę zwykli oficerowie². Wykorzystywano także mało skuteczną działalność w postaci nasłuchu radiowego i analizy sowieckich mediów, które były w pełni cenzurowane, a więc praktycznie bezwartościowe wywiadowczo, i wciąż oferowały Rosjanom możliwości prowadzenia dezinformacji.

Uwikłanie się polskiego wywiadu głębokiego w operację dezinformacyjną prowadzoną przez sowiecki kontrwywiad trzeba rozpatrywać w kategorii nie taktycznej porażki, ale strategicznej klęski. Przez pierwsze sześć lat funkcjonowania polskiego wywiadu na Wschodzie był on „przezroczysty” dla czekistów i oszukiwany przez sowieckich prowokatorów. Natomiast przez pozostałe lata istnienia II RP najpierw zrezygnowano z werbowania agentury za wschodnią granicą, aby uniknąć prowokacji, potem, gdy się okazało, że przyjęte metody obserwacyjne nie wystarczają – nie zdołano już odrobić zaległości. W ostatecznym rozrachunku polski wywiad był na terenach wschodnich „ślepy”, czego najtragiczniejszym dowodem był 17 września 1939 r., kiedy to Rzeczpospolita została napadnięta przez ZSRR. A według kierownictwa Oddziału II Rosja Sowiecka miała nie tylko zachować neutralność, lecz także udzielić Polsce materialnej pomocy w wojnie z Niemcami.

Po przeanalizowaniu rozmiaru strat polskiego wywiadu w latach 1921–1927 (oraz ich konsekwencji w latach późniejszych) nie wystarczy poprzestać na opisie prowadzonych przez niego operacji. Konieczne jest sformułowanie hipotez odpowiadających na podstawowe pytanie o **przyczyny**³ tak poważnej porażki, jaką poniósł. Aby wyjaśnić te z nich, które spowodowały klęskę wywiadowczą Oddziału II w starciu z sowieckimi służbami, trzeba przede wszystkim uświadomić sobie ich **wielorakość i złożoność**.

¹ Kontrrazwiedywiatel’nyj otdiel GPU, czyli sowiecki kontrwywiad GPU. Operacja „Trust” była realizowana przez sowiecki kontrwywiad mimo zmian organizacyjnych, tj. zarówno przez WCzK, GPU, jak i OGPU. Dla uproszczenia autor używa w tekście tylko jednej nazwy.

² Por. W. Michniewicz, *Wielki bluff sowiecki*, Chicago 1991, s. 268–269.

³ Wszystkie wyróżnienia w tekście pochodzą od autora (przyj. red.).

Brakuje jednego, najważniejszego, elementu czy wydarzenia, które można by było określić jako kamień węgielny procesu poddania się sowieckiej dezinformacji przez polski wywiad. Formalnie początkiem współpracy z podziemną organizacją o nazwie MOCR⁴-Trust (zwaną też organizacją „M”), a zarazem inicjacją wielkiej operacji dezinformacyjnej, było nawiązanie kontaktu z emisariuszami Trustu przez kpt. Wiktora Tomira Drymmera kierującego placówką wywiadowczą w Rewlu. Nie można jednak zapominać, że było to tylko pojedyncze zdarzenie, jakich wiele w pracy wywiadowczej. W innych okolicznościach i przy zastosowaniu innych rozwiązań kadrowo-organizacyjnych takie wydarzenie nie musiało doprowadzić do strat wywiadowczych na poziomie strategicznym, a mogło się zakończyć jedynie penetracją rewelskiego ataszatu.

Podjęcie kontaktu z organizacją przez kpt. W.T. Drymmera oraz późniejsze podtrzymywanie go przez Referat „Wschód” i wysłanie oficerów do łącznikowania Trustu w Moskwie – co w rezultacie doprowadziło do monopolizacji przez Trust polskiego rozpoznania na Wschodzie – były skutkiem splotu wielu czynników, które sprawiły, że Oddział II padł ofiarą sowieckiej dezinformacji.

Można jednak zaryzykować stwierdzenie, że biorąc pod uwagę kompleksowość oraz mnogość przyczyn stojących za współpracą z Trustem, Oddział II SG WP był idealnym obiektem takich działań. Nawet gdyby w Rewlu nie nawiązano kontaktu z tamtejszym ZJARMEM⁵, to z dużym prawdopodobieństwem można przyjąć, że prędzej czy później polski wywiad (a także wywiady państw limitrofowych) musiał się uwikłać w tego typu sytuację. Była to tylko kwestia czasu.

Starając się zrozumieć przyczyny tego zjawiska, można wyodrębnić główne czynniki stojące za wieloletnimi działaniami polskiego wywiadu, który od 1921 r. do 1927 r. konsekwentnie **ułatwiał** GPU pracę, gdyż ani nie podejmował żadnych prób weryfikowania informacji, ani nie prowadził działań ofensywnych, które mogły określić charakter operacji zaczepnych prowadzonych przez sowiecki kontrwywiad. Zastrzegając, że lista nie musi być kompletna, poniżej wyodrębniono grupy czynników, które wpłynęły na poziom gotowości do samooszukiwania się przez polskie struktury wywiadowcze.

I. Czynniki wewnętrzne

1. Czynniki psychologiczne, ogólnoludzkie, występujące powszechnie – kłamstwo współuczestniczące; zjawisko dysonansu poznawczego, które utrudnia bądź uniemożliwia rozpoznanie kłamstwa, zwłaszcza w jego wersji współuczestniczącej; syndrom myślenia grupowego, zwykle opartego na bezkrytycznym powielaniu zdania zwierzchników⁶.

2. Czynniki kreowane przez organizację Oddziału II SG WP (strukturalne) – autorytaryzm instytucji wojskowej opartej na rozkazie i przekazie informacji

⁴ Monarchiczieskoje Objedinenije Central’noj Rossii (przyp. red.)

⁵ Zagranicznaja Jaczejka Rossijskoj Monarchiczieskoj Organizacyi MOCR – przedstawicielstwo organizacji MOCR w stolicach tzw. limitrofów oraz państw zachodnich (przyp. red.).

⁶ Por. T.H. Bagley, *Wojny szpiegów*, Poznań 2014, s. 281.

w strukturze „góra–dół”, wykluczającej przepływ informacji zwrotnych (obiektywnych, a zwłaszcza krytycznych), którego skutkiem był konformizm pracowników; interesy grupowe dużej instytucji o charakterze biurokracji wojskowej sprzyjające powstawaniu mechanizmów zacierania kłamstwa współuczestniczącego; brak pracy zespołowej, awans uzależniony od osobistego sukcesu, od woluntarystycznych⁷ decyzji przełożonych, których przychyłność – zdobywana na różne sposoby – odgrywała najważniejszą rolę w karierze zawodowej oficerów wywiadu; związek między sukcesem wywiadowczym, mierzonym liczbą i jakością informacji pozyskiwanych przez agenturę a karierą oficerów prowadzących⁸; stopień identyfikacji oficerów ze służbą (czyli upraszczając – dysonans między etosem a karierowiczostwem⁹; splot czynników organizacyjnych i psychospołecznych powodujących niedostatki profesjonalizmu przynajmniej części kadry oficerskiej¹⁰; przyjęty model organizacyjny, charakter relacji międzyludzkich, przepustowość kanałów awansowych itp¹¹; poziom odpowiedzialności i odwagi cywilnej kadry kierowniczej, która w sytuacji pojawiania się symptomów świadczących o infiltracji i dezinformacji musi wybierać między zdecydowanymi działaniami wywołującymi poważne reperkusje ze strony społeczeństwa i rządu (w tym wpływającymi na kariery kierownictwa podejmującego takie decyzje) a wyciszaniem skandalu i ukrywaniem niewygodnych faktów.

II. Czynniki zewnętrzne

Do czynników zewnętrznych zalicza się: **politykę rządów przedmajowych wobec armii**, której skutkiem było drastyczne zwiększenie (na skutek cięć finansowych i pauperyzacji kadry oficerskiej) poziomu ryzyka kontrwywiadowczego w Wojsku Polskim oraz w Oddziale II, a także **ścisły związek między operacją dezinformacyjną a infiltracją aparatu wywiadowczego oszukiwanej służby** (agentura wpływu, „krety”)¹².

Ad I. 1. Czynniki psychologiczne

- **Zjawisko kłamstwa współuczestniczącego** – występuje ono powszechnie i jest znane ludzkości od stuleci. Ofiara kłamstwa (...) *nie zwraca uwagi na błędy*

⁷ Woluntaryzm – kierowanie się tylko własną wolą i nieliczenie się z opiniami innych ludzi w podejmowaniu decyzji, za: <https://pl.wikipedia.org/wiki/Woluntaryzm> [dostęp: 5 II 2019] (przyp. red.).

⁸ Por. J. Masterman, *Brytyjski system podwójnych agentów 1939–1945*, Warszawa 1973, s. 42.

⁹ Por. T.H. Bagley, *Wojny szpiegów...*, s. 139.

¹⁰ Płk M. Romeyko nazwał to zjawisko „kultem niekompetencji”. Zob. M. Romeyko, *Przed i po maju*, Warszawa 1985, s. 512.

¹¹ Można powiedzieć, że dobrze opłacane, zarządzane, kontrolowane instytucje, zachowujące otwarte ścieżki awansu dla zdolnych i oddanych oficerów, są zwykle znacznie mniej podatne na infiltrację, niż organizacje źle kierowane i wynagradzane. W tych ostatnich grupy „z dojciami” skutecznie blokują drogi awansu, posuwając się do prześladowania wszystkich, którzy mogą zagrażać karierze wybrańców.

¹² Por. M. Romeyko, *Przed i po maju...*, s. 160.

popelniane przez okłamującego, interpretując wieloznaczne zachowanie tak korzystnie dla kłamcy, jak tylko to możliwe¹³. Takie działania są podejmowane we wszystkich obszarach życia społecznego. Ludzie chcą wierzyć w nieprawdziwe informacje, gdy mają w tym własny, zwykle ukryty interes, a wykrycie kłamstwa mogłoby mieć negatywne konsekwencje (głównie w wymiarze psychologicznym) dla osoby okłamywanej. W życiu codziennym mamy do czynienia z tego typu współuczestnictwem np. wtedy, gdy akceptujemy czyjeś usprawiedliwienia, nie chcąc zrywać znajomości z powodów mniej lub bardziej błahych, gdy zdradzany mąż woli nie dostrzegać ewidentnych symptomów zdrady małżonki¹⁴ lub wtedy, gdy czyjeś kłamstwa odpowiadają wcześniej przyjętym założeniom.

W działaniach służb specjalnych zjawisko kłamstwa współuczestniczącego występuje wyjątkowo często: niejednoznaczność uzyskiwanych informacji, wielość często sprzecznych danych i utrudniony proces ich weryfikowania sprzyjają sytuacji, w której oficer (lub cała organizacja) w rzeczywistości ułatwia stronie oszukującej ukrywanie prawdziwego celu, ponieważ leży to w jego własnym interesie lub w interesie grupy, do której przynależy, a także pozwala na wywiązywanie się ze stawianych mu zadań oraz gwarantuje karierę.

To zjawisko starannie przeanalizował współtwórca brytyjskiego systemu podwójnych agentów J. Masterman¹⁵. Najbardziej syntetyczną charakterystyką kłamstwa współuczestniczącego jest zaś cytowane przez T.H. Bagleya zeznanie oficera Abwehry Hermana Bauna¹⁶, który przesłuchującym go po wojnie Amerykanom wyjawiał, że:

(...) był świadomy tego, że każdy z jego informatorów na sowieckich tyłach jest kontrolowany przez sowiecki kontrwywiad. Ponieważ nie był w stanie uzyskać lepszych wyników i ponieważ niemieckiemu najwyższemu dowództwu (OKH) podobały się jego raporty, kwestionowanie ich byłoby dla niego politycznym samobójstwem. Dlatego wciąż udawał przed zwierzchnikami, że wszystko jest w porządku¹⁷.

W służbach specjalnych łatwo może wytworzyć się sytuacja, w której znacznie korzystniej jest wierzyć kłamiącemu agentowi, niż go zdekonspirować i podważyć jego oświadczenia. Przyjmowanie dezinformacji (zwłaszcza w obszarach źle do tej pory rozpoznanych) gwarantuje nagrody, szybki awans i uznanie kierownictwa, które z kolei samo jest zainteresowane szybkim sukcesem wywiadowczym, a nie żmudnymi procedurami sprawdzającymi lojalność agentury i wiarygodność informacji.

¹³ P. Ekman, *Kłamstwo i jego wykrywanie w biznesie, polityce i małżeństwie*, Warszawa 1997, s. 22.

¹⁴ Tamże.

¹⁵ Zob. J. Masterman, *Brytyjski system podwójnych...*

¹⁶ Szerzej na temat wywiadowczej działalności Oberstleutnanta H. Bauna patrz odtajniony materiał CIA: http://www.foia.cia.gov/sites/default/files/document_conversions/1705143/CIA%20AND%20NAZI%20WAR%20CRIM.%20AND%20COL.%20CHAP.%201-10,%20DRAFT%20WORKING%20PAPER_0010.pdf [dostęp: 7 VII 2016].

¹⁷ T.H. Bagley, *Wojny szpiegów...*, s. 139.

W każdej instytucji o charakterze wywiadowczym, w której sukces jednostki jest powiązany z jej osobistym „wkładem informacyjnym” (czyli: im więcej agentów oraz informacji, tym więcej pochwał i awansów), a ta jednostka jest oderwana od interesów zespołu bądź całej służby, istnieje ogromne pole do wystąpienia kłamstwa współuczestniczącego.

Z zachowanych dokumentów Oddziału II niezbiecie wynika, że oficerowie uwikłani w większym lub mniejszym stopniu w aferę Trustu unikali przeprowadzania jakichkolwiek czynności, które mogły zachwiać ich zaufaniem do monarchistów i przynoszonych przez nich informacji. Przez lata pobytu w Warszawie sowieckiego agenta Jurija Artamonowa, który niemal codziennie bywał w siedzibie Oddziału II na ul. Brackiej i świadczył usługi na rzecz polskiego wywiadu, nikt w całym Oddziale II nie wpadł na pomysł, aby – choćby pobieżnie – sprawdzić, czym naprawdę zajmuje się ten młody Rosjanin i skąd czerpie środki na wystawne życie.

Z wyjaśnień kpt. W.T. Drymmera oraz z raportów Edwarda Czyżewskiego wynika, że Oddział II zdawał sobie sprawę z tego, że w Zarządzie Trustu działa Polak przedstawiający się jako Kijakowski (w rzeczywistości Wiktor Steckiewicz), ale w zachowanych materiałach brakuje jakichkolwiek informacji o tym, aby usiłowano zidentyfikować tę postać i zebrać informacje na jej temat. I to mimo to, że Steckiewicz (działający wówczas także jako Kosiński), nadzorował sowiecki wywiad na obszarze szeroko rozumianej Pribałtyki i często przebywał w Helsingfors (Helsinki)¹⁸, gdzie działał polski ataszat wojskowy. Nawet po nieudanym werbunku kmdr. Bohdana Jarocińskiego przez Steckiewicza nikt w Warszawie nie próbował ustalić, kim naprawdę był, co robił wcześniej, gdzie przebywał i z kim z Polaków się spotykał (lub mógł się spotkać) werbownik GPU, choć przecież porównanie opisu wyglądu Kijakowskiego i Steckiewicza mogłoby polskim analitykom nasunąć myśl, że to ta sama osoba¹⁹.

Z wyjaśnień rtm. Aleksandra Niedzińskiego wynika, że kiedy był w Moskwie – a więc miał możliwość osobistej weryfikacji części członków Trustu – w całości polegał na ich ustnych zapewnieniach i nawet nie zadał sobie trudu, aby chociaż zobaczyć, gdzie znajdują się firmy, o których Rosjanie mu opowiadali.

Podczas trwających latami spotkań polskich oficerów z agentem sowieckiego kontrwywiadu Eduardem Opperputem nikt nawet nie próbował zdobyć jakichkolwiek informacji na jego temat, mimo że materiały dotyczące jego osoby musiały być przechowywane w archiwum Oddziału II, gdyż E. Opperput jako Paweł Seljeninow podjął kontakt z polskim wywiadem w 1921 r. podczas operacji wymierzonej przeciwko Borisowi Sawinkowowi. W tym samym roku E. Opperput kontaktował z Józefem Beckiem i płk. Stanisławem Dowoyno-Sołohubem (w towarzystwie tego

¹⁸ List E. Opperputa do gazety „Siegodnia” opublikowany 17 V 1927 r.

¹⁹ Co gorsza, przedstawił się kmdr. B. Jarocińskiemu swoim prawdziwym nazwiskiem, demaskując swoją przeszłość, a mimo to nikt nie uznał za stosowne przeprowadzić szerszych ustaleń, które mogłyby ujawnić jego udział w organizacji „M”.

ostatniego uczestniczył w rozmowach z brytyjską misją wojskową)²⁰. Oddział II wystawił mu paszport na nazwisko Paweł Iwanowicz Spektorskij, co oznacza, że jego rzeczywiste nazwisko (w kontaktach z Sawinkowem miał wyjawic, jak się naprawdę nazywa) i wygląd²¹ powinny być znane oficerom polskiego wywiadu. Warto dodać, że rozpoznanie E. Opperputa nie było trudne. Zrobił to w 1927 r. w Finlandii – natychmiast po ucieczce E. Opperputa z ZSRR – były współpracownik Sawinkowa, niejaki Aleksandr K. Rudin, który pod pseudonimem A. Karin opublikował artykuł na ten temat w ryskiej gazecie „Siegodnia”²².

Oficerowie Oddziału II skutecznie **unikali** przeprowadzania jakichkolwiek działań, które potencjalnie mogły zagrozić wiarygodności ich informatorów. Nie prowadzili nawet najbardziej podstawowych czynności polegających na szczegółowych sprawdzeniach w kartotekach, co należało do ich obowiązków służbowych. Warto też pamiętać, że legenda tworzona przez GPU dla agentury wcale nie była perfekcyjna i powinna wywoływać pytania, na które nie było dobrych odpowiedzi – na przykład pytanie zadane przez gen. Jewgenija Klimowicza podczas spotkania z przedstawicielem Zarządu Trustu gen. Nikolajem Potapowem: jak udaje mu się podróżować tak długo po Europie, będąc oficerem służby czynnej Armii Czerwonej?²³ Problem polegał na tym, że niemal nikt po stronie polskiej takich pytań nie stawiał.

• **Dysonans poznawczy** – (...) *stan napięcia, który występuje wtedy, gdy dana osoba posiada jednocześnie dwa elementy poznawcze (idee, postawy, przekonania, opinie), które są psychologicznie niezgodne ze sobą*²⁴. Jeżeli między wspomnianymi wyżej elementami poznawczymi powstaje dysonans, czyli jeżeli są one niezgodne ze sobą, pojawia się poczucie dyskomfortu, który motywuje jednostkę do jego redukcji, gdyż jedną z podstawowych cech ludzkich jest wiara, że życie ma sens, akceptowanie zaś dwóch sprzecznych ze sobą idei przekreśla tę logikę istnienia zakładaną a priori²⁵. Im bardziej ktoś jest zaangażowany w jakieś działanie wynikające z akceptowanego przekonania, tym większy stawia opór wobec informacji zagrażających temu

²⁰ P. Seljaninow, *Narodnyj sojuz zaszczyt Rodiny i swobody. Wspominanija*, Berlin 1922, s. 66.

²¹ Po I wojnie światowej, w latach 20. XX w., przy podróżowaniu za granicę wymagano dowodu osobistego. Pomimo nazwy „dowód osobisty” znajdującej się na wewnętrznej okładce, był on powszechnie nazywany paszportem. Dowód miał formę arkusza złożonego na pół i zawierał dane osobowe, fotografie, zawód, informację o wyznaniu, alfabetyzmie oraz rysopis, za: A. Baczyńska, *Historia dowodu osobistego w Polsce*, <http://wiadomosci.onet.pl/kraj/historia-dowodu-osobistego-w-polsce/sd95s> [dostęp: 6 XI 2015].

²² Centralne Archiwum Wojskowe (dalej: CAW), Oddział II, sygn. I.303.4.2090, pismo placówki „NORD” dotyczące artykułu w „Siegodnia” z 10 VI 1927 r. Rudin, publikując swoje oskarżenia wobec E. Opperputa, pozostawał pod kontrolą GPU, gdyż jego bliskim przyjacielem był mąż Mariny Cwietajewej Siergiej Efron – kolejny oprócz Arapowa *jewrazijec* – agent GPU.

²³ Potapow odpowiedział, że kierownictwo RKKA jest przekonane, że na urlopie poluje w tajdze, co zostało – z niepojętych przyczyn – przyjęte do wiadomości. Ta sprawa wyraźnie pokazuje, że legendy agentów GPU miały „dziury”, które stosunkowo łatwo było dostrzec i, korzystając z możliwości organizacji wywiadowczej, zweryfikować podejrzenia.

²⁴ E. Aronson, *Człowiek – istota społeczna*, Warszawa 1987, s. 134.

²⁵ Tamże.

poglądowi²⁶. Redukcja dysonansu następuje pod wpływem procesu zniekształcania, dyskredytowania i selektywnego doboru informacji, dzięki którym chroni się własne przekonania. Jest to proces, który był sprawdzany zarówno w warunkach laboratoryjnych²⁷, jak i na przykładach historycznych. Najbardziej znanym są analizy zachowań Żydów podczas *Shoah* (Holocaustu), którzy pomimo coraz większej ilości informacji na temat mającego miejsce ludobójstwa, konsekwentnie starali się dyskredytować zagrożenie²⁸.

Działanie Oddziału II już po nawiązaniu kontaktu z Trustem i podpisaniu porozumień z monarchistami (najpierw przez placówkę w Rewlu, a potem przez centralę w Warszawie) miało wszystkie cechy klasycznej redukcji dysonansu poznawczego. Od 1921 r. do 1927 r. – nie licząc tzw. raportu por. Władysława Michniewicza – w archiwach brakuje jakichkolwiek śladów wskazujących na to, że ktokolwiek z Oddziału II na poważnie rozpatrywał prawdopodobieństwo, że przedstawiciele MOCR-Trust mogą być agentami GPU.

Jak już wspomniano, przez cały okres pobytu J. Artamonowa w Warszawie nie objęto go choćby wyrywkową kontrolą operacyjną. Nikt nigdy nie zastanowił się, skąd czerpie on środki na dostatnie życie, choć jest to pytanie, na które odpowiedź jest najistotniejsza w przypadku osoby pozostającej w stałym kontakcie z wywiadem. Zwłaszcza jeśli jest to cudzoziemiec z kraju traktowanego jako główny przeciwnik własnego państwa. Identyczna sytuacja miała miejsce w placówce Oddziału II w Moskwie. Nikogo nie zastanawiało, że E. Opperput regularnie bywał w polskich placówkach dyplomatycznych i – mimo to – nie stał się obiektem zainteresowania GPU, choć implikacje tego były tak oczywiste, że informator W. Michniewicza, płk Wiktor Drobyszewski, automatycznie uznał to za dowód na prowokację GPU. Sam W. Michniewicz po rozmowie z płk. W. Drobyszewskim odkrył tę prawdę i był pod takim jej wrażeniem, że nie mając żadnych dowodów poza poczuciem oczywistości kłamstwa w obliczu realiów sowieckich, pojechał z raportem na ten temat do Warszawy. Pomimo niezachowania się dokumentu, napisanie raportu w sprawie Trustu przez W. Michniewicza należy uznać za wysoce prawdopodobne z czterech powodów:

- 1) w 1923 r. W. Michniewicza rzeczywiście spotkały szykany ze strony kierownictwa Oddziału II, wskutek których trafił do służby liniowej w pułku w Równem, choć w jego wcześniejszej karierze brakowało przesłanek do takiej kary;
- 2) istniało przywoływane przez niego źródło informacji (tj. płk W. Drobyszewski);
- 3) o jego raporcie z 1923 r. pisał w liście zastępca kierownika Referatu „Wschód” w latach 1922–1923 por. Władysław Kowalewski²⁹;

²⁶ Tamże, s. 137.

²⁷ Omówienie badań (D. Ehrlich, E. Jones, R. Kohler, J. Freedman, S. Fraser, J. Mills, L. Festinger, J. Merrill Carlsmith, A.R. Cohen, K. Davis, R. Nisbett, E. Aronson) zob. tamże, s. 134–190.

²⁸ Przypadek wymordowania żydowskiej ludności węgierskiego miasta Sighet zob. tamże, s. 147–148.

²⁹ W. Michniewicz, *Wielki bluff sowiecki...*, s. 135–136.

- 4) potwierdzeniem, choć nie bezpośrednim, jest artykuł W.T. Drymmera z 1965 r.³⁰ Podany przez niego przebieg zdarzenia odpowiada w większości wersji przedstawionej przez W. Michniewicza. Wiadomo również, że W.T. Drymmer nie meldował o swoich podejrzeniach wobec Trustu w 1923 r. W swoich pisemnych wyjaśnieniach na temat afery organizacji „M” z 1927 r. nie wspomniał on ani słowem o takim zdarzeniu, choć działał pod presją jako oficer służby zewnętrznej oskarżony przez E. Opperputa o współpracę z GPU. Może to świadczyć o przypisywaniu sobie po latach przez W.T. Drymmera cudzych zasług, co odpowiadało jego profilowi psychologicznemu. Oznacza to prawdopodobnie, że sprawa raportu była mu znana, a więc można założyć, że raport istniał i mógł być omawiany w środowisku oficerów Oddziału II, a W. Michniewicz nie kłamał w swoich wspomnieniach.

Podany przez W. Michniewicza przebieg omówienia treści raportu z bezpośrednim przełożonym, kpt. Michałem Talikowskim, w pełni odpowiada założeniom teorii dysonansu poznawczego:

(...) Drobyszewski straszy nas GPU, pewnie ze strachu, sam siedzi jak mysz pod miotłą. W Warszawie zaś – perorował Talikowski – mamy wszechstronne źródła i szerokie możliwości ich kontroli. Mamy kontakty z generałem Klimowiczem i Kutiepowem, dysponującymi w Sowietach własną siatką agencyjną. Mamy tu delegata MOCR, rotmistrza Artamonowa, nie tylko błyskotliwego oficera gwardii, którego znasz z Rewla, ale wyrobionego i inteligentnego sztabowca. Jest o Truście najlepszej opinii i zapowiada rychły przyjazd do Warszawy specjalnej misji z Moskwy do pertraktacji polityczno-wojskowych na najwyższym szczeblu! Szczeblu, do którego nie dorastasz, stale komunikując się z Kasatkinem, obaj w roli listonoszy³¹.

Ze wspomnień W. Michniewicza wynika, że kierownik Referatu „Wschód” stosował wszystkie znane strategie redukcji dysonansu poznawczego: ośmieszał i bagatelizował tezy płk. W. Drobyszewskiego oraz powoływał się na (nieistniejące w rzeczywistości) możliwości weryfikowania informacji przekazanych przez Trust u niezależnych źródeł. Gdy W. Michniewicz, który podczas służby miał kłopoty z dyscypliną, nie przestawał mówić o sprawie, Talikowski pozbył się go z wywiadu. W ten sposób zlikwidował źródło nieprzyjemnych dla siebie informacji i zapewnił sobie komfort psychiczny. Zachowanie kpt. M. Talikowskiego³² także wskazuje na redukcję dysonansu w sytuacji zaangażowania emocjonalnego, czyli na zdecydowane usunięcie

³⁰ W.T. Drymmer, *Trust*, „Kultura” 1965, nr 2.

³¹ W. Michniewicz, *Wielki bluff sowiecki...*, s. 132.

³² Który w stosunkowo drobnej sprawie różnicy w ocenach sytuacji operacyjnej, łatwej do obalenia z powodu nieposiadania przez podwładnego zweryfikowanych informacji, sięgnął po środki represji, wysyłając W. Michniewicza na Ukrainę, choć ten miał rodzinę w Warszawie i tutaj też rozpoczął studia.

źródła informacji sprzecznych z przyjmowanym stanowiskiem. Kpt. M. Talikowski, jak się wydaje, był ofiarą, która prawdopodobnie aktywnie uczestniczyła w sowieckim kłamstwie. Przyjmowanie sowieckiej dezinformacji było dla niego korzystne: sprzyjało karierze (pomimo złych opinii kierownictwa o jego inteligencji i zdolnościach), zapewniało pieniądze potrzebne na dokończenie budowy willi na Sadybie, a także pozwalało odgrywać rolę „czarodzieja od wywiadu”, brylującego m.in. wśród snobistycznych arystokratów z MSZ, którzy w nadziei na odzyskanie majątków na Kresach, chętnie wysłuchiwali informacji o zbliżającym się rozpadzie państwa sowieckiego³³.

Innym przykładem ilustrującym działanie dysonansu poznawczego u oficerów Oddziału II uwikłanych we współpracę z Trustem są wyjaśnienia rtm. A. Niedzińskiego, np. opisana przez niego ewidentna wpadka GPU, które na jesieni 1925 r. dostarczyło Polakom fałszywą informację o rzekomych manewrach wojsk sowieckich:

Szczęśliwie się jednak stało, że wywiad nasz zauważył tę inspirację; zażądałem zatem kategorycznego wyjaśnienia i gruntownego zbadania tej sprawy. Dokładnie przypominam sobie ową rozmowę z członkami „M” – Fiodorowem, Potapowem, Denisowem i Kasatkinem, na których oświadczenie moje, iż w dokumentach wym. są inspirowani przez GPU, zrobiło silne wrażenie. Wyjaśnieniem zajął się Kasatkin, który twierdził, że dokument od nich mógł zginąć w naszym sztabie i następnie został przekazany z ramienia GPU przez jakiś inny kontakt naszego wywiadu celem dezorientacji. Nietrudno było obalić to przypuszczenie, gdyż wywiad nasz otrzymał ten dok. jednocześnie z 3 źródeł: z R7/I., z plac. „Bałt” i o ile się nie mylę, z placówki „Szperacz” (...) Zaznaczyć należy, że placówka „Szperacz” otrzymała ów dokument świadomie od agenta GPU jako inspirowany. Po tem oświadczeniu mojem, organizacji nie pozostawało nic innego, jak oświadczyć po pewnym czasie, iż rzeczywiście ich człowiek w Kijowie natknął się na agenta GPU, od którego nabył ów dokument. Oświadczone mi zatem, że z tego tytułu wpadło u nich jedno ogniwo organizacyjne, a ów niefortunny wywiadowca został rozstrzelany. O powyższem meldowałem we właściwym czasie, będąc zdania, że taki wypadek jest możliwy w warunkach pracy konspiracyjnej³⁴.

Nietrudno dostrzec, że strona polska zignorowała niezwykle czytelną wskazówkę świadcząca o byciu ofiarą dezinformacji. Niejasne są motywy, dla których GPU przekazało ten sam dokument jednocześnie trzem placówkom wywiadowczym Oddziału II, przy czym – jakby upewniając się, że strona polska na pewno zrozumie – dodało w jednym przypadku informację, że Oddział jest inspirowany. Prawdopodobnie Sowietci mieli poczucie pełnej kontroli informacyjnej nad Oddziałem II i być może chcieli sprawdzić procedury weryfikacyjne stosowane przez Polaków w przypadku oczywistej dezinformacji. Jeśli ta hipoteza jest poprawna, to trzeba podkreślić, że Oddział II

³³ W. Michniewicz, *Wielki bluff sowiecki...*, s. 100.

³⁴ CAW, Oddział II, sygn. I.303.4.1781, załącznik nr 130 do *Arkusza obserwacyjnego org. „M”*.

nie zastosował żadnych metod weryfikacji poza przekazaniem agentom GPU nie tylko sugestii o tym, że dokument jest fałszywy, lecz także wiedzy o tym, w jaki sposób polski wywiad doszedł do takiego przekonania (sic!).

Identyczna sytuacja miała miejsce w przypadku wspomnianego dokumentu mobilizacyjnego dostarczonego przez Trust, który został zakwestionowany przez Wydział Ewidencji (zwany Ewidencją). Rtm. A. Niedziński w sposób następujący opisywał tę sprawę:

Rozmawiając w tej sprawie z organizacją [MOCR – dop. aut.] wypowiedziałem im zarzuty, jakie zostały postawione powyższemu dokumentowi oraz zaznaczyłem, że bezwzględnie są oni inspirowani przez źródło, które dostarczyło im powyższy dokument. Ze swej strony nie mogłem się jednak pogodzić z myślą, że organizacja „M” była zdekonspirowana wobec GPU, dochodząc do tego na podstawie znanych mi systemów pracy GPU oraz całego szeregu danych przemawiających za niemożliwością podobnej supozycji³⁵.

Wyjaśniając, dlaczego nie przekonywały go argumenty Ewidencji, dodawał: (...) *placówka nie miała i nie mogła mieć sprawdzianu, operując li tylko logicznymi wywodami wypływającymi ze znajomości terenu i na podstawie moralnego przeświadczenia.*

Żeby w pełni pojąć nielogiczność powyższego zdania, wystarczy dodać, że sowiecki dokument był sfalszowany wyjątkowo nieudolnie. Sugerowano w nim, że w planach mobilizacyjnych stworzonych na wypadek wojny z Polską przewidywano atak od strony południowej, z terytorium Ukrainy. Było to niezgodne ze wszystkimi dotychczasowymi planami sztabowymi, w których zakładano dyslokację wojsk przez Bramę Smoleńską³⁶. Atak z terenów Ukrainy byłby rozwiązaniem absolutnie nierealnym z uwagi na brak odpowiednio gęstej sieci połączeń kolejowo-drogowych³⁷. „Moralne przeświadczenie” przywołane przez rtm. A. Niedzińskiego było w istocie żelazną logiką sztabową, która wykluczała taki kierunek dyslokacji.

Symptomy ciągłej redukcji dysonansu można zauważyć w zachowaniu oficerów Oddziału II zarówno w początkowych stadiach operacji, jak i już po samodekonspiracji Trustu, gdy nie dało się dłużej utrzymywać iluzji, że polski wywiad ma na Wschodzie potężną i wpływową organizację dostarczającą wiele informacji wywiadowczych. Widać je w reakcji ppłk. Ludwika Bocińskiego na rewelacje E. Opperputa przekazywane w liście attaché wojskowego RP w Finlandii do kpt. M. Talikowskiego³⁸, oraz

³⁵ Tamże.

³⁶ Brama Smoleńska – historyczne i geostrategiczne pojęcie określające obszar pomiędzy górną Dźwiną i górnym Dnieprem. Przez ten obszar przechodzi najkrótszy i najłatwiejszy do przebycia szlak Wschód–Zachód łączący centralną Europę z Moskwą i resztą Rosji (przyp. red.).

³⁷ W. Michniewicz, *Wielki bluff sowiecki...*, s. 248.

³⁸ CAW, Oddział II, sygn. I.303.4.2090, list bez nagłówka z 25 V 1927 r. z dopiskiem „zał. 150”. Najprawdopodobniej adresatem był kpt. Michał Talikowski. Autorem listu był przypuszczalnie por. Stanisław Łaniewski – wówczas p.o. attaché wojskowego w Helsingfors i kierownika Placówki Wywiadowczej „Fin”.

w przebiegu tzw. komisji Bocińskiego, w której motywy strictly polityczne nałożyły się na zaprzeczenia powstające w wyniku redukcji dysonansu poznawczego.

• **Syndrom grupowego myślenia** – (...) *myślenie grupowe odnosi się do upadku psychicznej efektywności, realizmu i osądu moralnego spowodowanych wewnątrzgrupowymi naciskami*³⁹. W momencie wystąpienia takiego zjawiska ujawniają się następujące defekty obiegu informacji w grupie: ograniczanie dyskusji do rozważenia zmniejszonej liczby alternatyw, unikanie powtórnej analizy przyjętych już rozwiązań, lekceważenie rozwiązań odrzuconych na początku, rezygnacja z ekspertyz zewnętrznych, które mogłyby ocenić alternatywne sposoby działania, przyjmowanie jedynie faktów i ocen potwierdzających obrany kierunek oraz ignorowanie wpływu czynników negatywnych na spodziewane rezultaty⁴⁰. Istotnymi czynnikami wystąpienia syndromu grupowego myślenia są: spójność grupowa (*esprit de corps*), izolacja od wykwalifikowanych współpracowników i ekspertów, a także preferowanie przez kierownictwo (lidera danej grupy) konkretnego rozwiązania⁴¹.

Opierając się na badaniach Irvinga L. Janisa poświęconych temu zagadnieniu, można wyodrębnić następujące symptomy grupowego myślenia⁴² zaobserwowane w działaniach Oddziału II podczas operacji Trust:

1. **Iluzja wszechmocności i niezwyciężoności rodząca optymistyczne przekonanie o sukcesie i ośmielająca do podejmowania ryzyka.** Ten symptom można dostrzec w zachowaniu niemal wszystkich oficerów Oddziału II, i to zarówno z centrali, która formułowała śmiałe oczekiwania uzysku operacyjnego wobec placówek wywiadowczych na Wschodzie, ignorując istniejące realia, jak i oficerów służby zewnętrznej notorycznie łamiących podstawowe zasady konspiracji pracy wywiadowczej⁴³.
2. **Kolektywna racjonalizacja przyjętych rozwiązań,** czyli omawiany już proces dysonansu poznawczego dzielonego przez grupę uwiklaną w obronę przyjętych założeń.
3. **Stereotypowy wizerunek przeciwnika jako zbyt złego, aby z nim wchodzić w układy, lub zbyt głupiego, aby mógł pokrzyżować jakiegokolwiek, nawet ryzykowne, plany.** Ten symptom koresponduje z iluzją wszechmocności. Polscy oficerowie, co wykazano na przykładach, z zadziwiającą konsekwencją niedoceniali przeciwnika. Skutkowało to nonszalancją w zachowaniu, m.in.: robieniem nielegalnych interesów z agenturą GPU, ignorowaniem oczywistych

³⁹ W. Domachowski, S. Kowalik, J. Miluska, *Z zagadnień psychologii społecznej*, Warszawa 1984, s. 123.

⁴⁰ Tamże, s. 121.

⁴¹ Por. tamże, s. 123–124.

⁴² Tamże.

⁴³ Między innymi ignorowanie ryzyka penetracji przez oficerów polskiej misji wojskowej, przechowywanie przez W. Michniewicza kompromitujących listów w tekturowej walizce pod łóżkiem (w budynku zajmowanym przez Komisję Repatriacyjną), zabawa „w kotka i myszkę” z członkami zespołów obserwacyjnych GPU itp. Często wynikało to jednak z braku funduszy i złego wyekwipowania polskich wywiadowców.

- sugestii, że istnieją związki pomiędzy pozyskiwanymi źródłami a sowieckim kontrwywiadem oraz brakiem jakichkolwiek zabezpieczeń polskiej placówki.
4. **Bezpośredni nacisk na każdego członka grupy, który przedstawia mocne argumenty przeciwko któremuś z grupowych stereotypów czy iluzji.** Najlepszą tego ilustracją była sprawa W. Michniewicza, który po napisaniu raportu na temat Trustu, stawiającego organizację w nie najlepszym świetle (choć pozbawionego bazy faktograficznej, która mogłaby realnie grozić dekonspiracją monarchistów), został ukarany dyscyplinarnie i usunięty z Oddziału II.
 5. **Niekwestionowana wiara we wrodzoną moralność własnej grupy.** Uwidaczniało się to najsilniej w raporcie ppłk. L. Bociańskiego, który – bez badania wiarygodności zeznań E. Opperputa oskarżającego oficerów Oddziału II o zdradę – już na wstępie rozmów z fińskimi oficerami zadeklarował pełne zaufanie do swoich oficerów. Z całą pewnością miało to wpływ na późniejsze ustalenia komisji, która nie znalazła winnych i zablokowała działania mogące oczyścić polski wywiad na Wschód z sowieckiej agenty.
 6. **Blokowanie oceny i weryfikacji przyjętych założeń skutkujące autocenzurą odstępstw od rozwiązań grupowych.** Jak już wspomniano, z artykułu W.T. Drymmera oraz ze wspomnianego listu por. W. Kowalewskiego do W. Michniewicza wynika, że część kadry Oddziału II znała prawdopodobnie raport W. Michniewicza, jednak brakowało jakichkolwiek śladów w dokumentach świadczących o tym, że któryś z oficerów formułował na piśmie wątpliwości wobec Trustu. Zachowana dokumentacja potwierdzała, że do 1927 r. Oddział II nie miał żadnych podejrzeń wobec monarchistów. Nawet jeśli oficerowie powtarzali sobie w formie plotek historię raportu W. Michniewicza, to na zewnątrz prezentowali linię zgodną z oczekiwaniami kierownictwa przekonanego o posiadaniu znakomitego źródła na najwyższych szczeblach władzy sowieckiej.
 7. **Iluzja jedności płynąca z autocenzury.** Jeżeli przyjmie się, że polscy oficerowie cenzurowali własne wnioski umieszczane w materiałach sprawy, to każda osoba mająca do nich dostęp utwierdzała się w przekonaniu, że **wszyscy** mający do czynienia ze sprawą oceniali ją pozytywnie. Takie konkluzje były potem przekazywane kolejnym prowadzącym sprawę, którzy tę iluzję pełnej jedności ocen przyjmowali jako podstawę dalszych kontaktów z Trustem (wynika to jednoznacznie np. z cytowanych już wyjaśnień rtm. A. Niedzińskiego).
 8. **Obecność stróżów poprawnego myślenia,** czyli osób wyłonionych z grupy chroniących daną grupę przed dopływem informacji, które mogłyby zniszczyć samozadowolenie tej grupy z powodu podjętych decyzji. W ocenie autora tę rolę odgrywał najprawdopodobniej kpt. M. Talikowski, który, jeśli wierzyć W. Michniewiczowi, posunął się do zniszczenia lub zagubienia jego raportu⁴⁴.

⁴⁴ W. Michniewicz twierdzi, że tego raportu bezskutecznie szukał Jerzy Niezbrzycki po objęciu stanowiska kierownika Referatu „Wschód”, z czego wyciągał wniosek, że raport musiał być zniszczony przez M. Talikowskiego. Zob. W. Michniewicz, *Wielki bluff sowiecki...*, s. 132, 137.

Ad I.2. Czynniki strukturalne

- Organizacja wojskowa z jej sztywną hierarchią stopni wojskowych i podległości służbowej, w której obowiązuje bezdyskusyjne wykonywanie rozkazów, przyciąga osoby z predyspozycją do postaw autorytarnych, wzmacnianych jeszcze podczas pełnienia służby. Przez osobowość autorytarną⁴⁵ rozumie się zespół ukształtowanych cech, do których zalicza się przede wszystkim: uznanie konwencjonalnych wartości, nietolerowanie słabości u siebie i u innych, silną skłonność do karania, podejrzliwość, ale przede wszystkim niezwykły respekt dla władzy oraz „sztywność poznawczą”, czyli małą podatność na zmianę raz ukształtowanych poglądów⁴⁶. Ten typ osobowości łączy w sobie dwa rodzaje konformizmu, tj. **uleganie** (zachowanie jednostki jest motywowane pragnieniem uzyskania nagrody lub uniknięcia kary) oraz **identyfikację** (zachowanie i poglądy są kształtowane przez pragnienie jednostki, aby upodobnić się do jednostki uznanej za wzór)⁴⁷. W kreowaniu postawy młodego oficera ogromną rolę odgrywa zarówno wymuszanie konkretnych zachowań i poglądów (przynajmniej prezentowanych publicznie), jak i naśladowanie przełożonych. Opiszana wyżej tendencja znajdowała odbicie, przynajmniej do pewnego stopnia, także w Oddziale II. Wpływało to na wszystkie aspekty jego funkcjonowania, w tym na działalność operacyjną.

Jako przykład konformistycznego ulegania m.in. w sytuacjach ekstremalnych można przytoczyć wspomnienia oficerów uwikłanych we współpracę z Trustem, którzy w zetknięciu z najbardziej absurdalnymi decyzjami przełożonych ulegali ich rozkazom nawet wtedy, gdy mieli **niezachwiane** przekonanie, że to oni mają rację. W swoich wspomnieniach W. Michniewicz pisze otwarcie, że po odrzuceniu jego raportu przez kpt. M. Talikowskiego oraz rozpoczęciu prześladowania go, nie podjął żadnych kroków, aby powiadomić o tym wyższych przełożonych. Po latach swoje zachowanie tłumaczył w następujący sposób: (...) *nie było sensu iść na skargę do wyższego szczebla – bo do kogo? Do oślepionego przez sejmową politykę Bajera, ignoranta wywiadowczego?*⁴⁸ W. Michniewicz nie zrobił nic, gdyż najprawdopodobniej bał się dalszych szykan (które i tak nastąpiły) i zdawał sobie sprawę z tego, że przełożeni byli wyjątkowo solidarni w niszczeniu krnąbrnych podwładnych⁴⁹.

Abstrahując od prawdziwości jego relacji, wspomnienia W.T. Drymmera na temat rzekomego zdekonspirowania przez niego Trustu ujawniają ten sam stopień bezsilności wobec samowoli przełożonych:

Po powrocie do Warszawy raz jeszcze meldowałem moim przełożonym, że jesteśmy ślepych narzędziem w rękach sowieciarzy. Popierali mnie dwaj oficerowie:

⁴⁵ Omówienie cech osobowości autorytarnej patrz: E. Aronson, *Człowiek – istota społeczna...*, s. 248–251. Szerzej zob. też: T.W. Adorno, *Osobowość autorytarna*, Warszawa 2010.

⁴⁶ E. Aronson, *Człowiek – istota społeczna...*, s. 249.

⁴⁷ Tamże, s. 57.

⁴⁸ W. Michniewicz, *Wielki bluff sowiecki...*, s. 132.

⁴⁹ Por. F. Kusiak, *Życie codzienne oficerów Drugiej Rzeczypospolitej*, Warszawa 1992, s. 258.

pplk (Józef – dop. red.) Englicht i mjr (Czesław – dop. red.) Pawłowicz z tzw. Ewidencji O.II, której zadaniem było badanie jakości i prawdziwości otrzymywanych przez nasz wywiad wiadomości. W rezultacie tych naszych zastrzeżeń – odebrano mi łączność z M.O.R. (Trustem – dop. aut.), odwołano mego utalentowanego oficera por. (Tadeusza – dop. red.) Wernera i wysłano na jego miejsce innego, zresztą również dzielnego, oficera, tylko niestety niedoświadczonego, mjra Niedzińskiego⁵⁰.

Relacja kpt. W.T. Drymmera, podobnie jak wspomnienia W. Michniewicza, ukazuje konformistyczną uległość wobec przełożonych wielu osób, które deklarowały, że **wiedziały o odbywającej się na ich oczach operacji sowieckich służb wymierzonej w polskie interesy**. Ważnym szczegółem jest to, że nikt z im współczesnych nie kwestionował ich zachowania. Wykonywanie poleceń przełożonych, jak z tego wynika, stało wyżej w hierarchii wartości polskiego oficerstwa niż interes służby i państwa.

Z identyczną sytuacją można się spotkać, czytając kolejny dokument dotyczący współpracy z Trustem, tym razem sporządzony przez por. T. Wernera, któremu pplk Ignacy Boerner nakazał, aby umożliwił on skontaktowanie się por. J. Szczepkowskemu – jego adiutantowi – z agenturą obsługiwaną przez T. Wernera, czyli w tym wypadku z E. Opperputem.

Ponieważ rozkaz ten uznałem za niezgodny z instrukcjami i dyrektywami OII Referatu Centralnej Agencji SG (...) zwlekałem z wykonaniem go. Po upływie dłuższego czasu zostałem wezwany do Pułkownika, który w zupełnie konkretnej formie polecił mi w przeciągu 2-ch dni skomunikować por. Szczepkowskiego z organizacją „M”. Nie mogąc przeciwstawić się tak wyraźnemu rozkazowi, zaproponowałem umożliwienie wymienionemu rozmowy z panem „z bródką” (...). Następnego dnia udałem się z por. Szczepkowskim autem w umówione miejsce, gdzie czekał na nas i wsiadł do samochodu „Magik”. W aucie por. Szczepkowski oświadczył mi, że w myśl dyrektyw „swysze” ma on z nim odbyć dłuższą konferencję i zażądał, aby „bródka” przyjechał w najbliższych dniach do lokalu Attachatu. Początkowo starałem się sprzeciwić (...) *nolens volens* zgodziłem się. Miało to miejsce w sobotę 2 lutego. „Magik” prosił, aby spotkać się z nim w celu udania się do Attachatu 5.02.1924, lecz na schadzki nie stawiał się. Przypuszczałem więc, że będzie starał się uniknąć wycieczki do Attachatu. Tegoż dnia wieczorem, gdy byłem w Poselstwie, Pułkownik zapytał, czy rozkaz jego został wykonany, zameldowałem mu że agent nie stawiał się, na co Pułkownik oświadczył, iż widzi w tym jedynie moją złą wolę i żąda kategorycznie doprowadzenia do skutku schadzki. Następnego dnia skomunikowałem się z „Magikiem” i umówiliśmy się, że pojedzie on do Attachatu wraz ze mną 8.2., co też zostało doprowadzone do skutku. W Attachacie rozmawiał on z por. Szczepkowskim ok. 4 godzin prawie wyłącznie o sytuacji wewnętrznej politycznej Rosji. Tegoż dnia wieczorem udałem się do Poselstwa, gdyż chciałem być obecnym przy

⁵⁰ W.T. Drymmer, *Trust...*, s. 99.

zdawaniu przez por. Szczepkowskiego Pułkownikowi sprawozdania z odbytej konferencji. Po wysłuchaniu takowego, Płk Boerner polecił por. Szczepkowskiemu napisać na podstawie informacji uzyskanych od „bródki” polityczny meldunek sytuacyjny. (...) Ponieważ uważam za bezwzględnie niewskazane ze względów konspiracyjnych spotkanie się mych ludzi z kimkolwiek z placówek polskich, zwłaszcza zaś z adiutantem Pułkownika i bywania ich w lokalu tak skompromitowanym i obserwowanym, jakim jest budynek Attachatu (...) i biorąc pod uwagę usługi, które nam oddaje org. „M” jako źródło wywiadowcze, uważam wszelkie spotkania Szczepkowskiego z ich ludźmi, zwłaszcza w czasie obecnych politycznych represyj, za nadzwyczaj niepożądane – zwiększające szanse dekonspiracji, proszę o instrukcje w tym względzie na przyszłość⁵¹.

Przytoczony fragment jednoznacznie określa poziom zależności służbowej od wyższych szarż – i to w sytuacji niejasnej podległości służbowej. Por. T. Werner, choć zdawał sobie sprawę z tego, że polecenie ppłk. I. Boenera było wydane wbrew najbardziej elementarnym zasadom pracy wywiadowczej i mogło doprowadzić do dekonspiracji całej organizacji „M” efektywnie współpracującej (jak sądził) z polskim wywiadem, to po krótkiej zwłoce wykonał je. Dopiero po tym zdobył się na zażądanie od swojego bezpośredniego przełożonego wskazówek, co ma robić w przypadku takich sytuacji w przyszłości.

Autorytaryzm wojskowej organizacji polskiego wywiadu był także przyczyną bezrefleksyjnego przyjmowania ocen przełożonych przez oficerów wywiadowczych. Przykładem może być fragment wyjaśnień rtm. A. Niedzińskiego z 1927 r.:

W tem miejscu muszę podkreślić, że zarówno w instrukcjach otrzymywanych przeze mnie z Wydziału Wywiadowczego, jako też od kierownictwa R7 niebyły zupełnie wysuwany moment jakiegokolwiek nieufności co do samego faktu istnienia organizacji (sic!), przy czem, jako człowiek nowy w wywiadzie, wyniosłem najzupełniejsze przeświadczenie, że organizacja owa jest oparta na podłożu wybitnie ideowym. Zresztą, opierano się najwidoczniej na zasadzie dotychczasowych rezultatów pracy wywiadowczej w postaci dokumentów i informacji oraz na rezultacie obserwacji wynikającej z kontroli korespondencji org. „M”⁵².

Wynika z nich, że rtm. A. Niedziński, przyjeżdżając do Moskwy, **miał już ukształtowaną opinię na temat Trustu, przy czym czerpał ją w całości od swoich przełożonych**, bo któż inny z Wydziału Wywiadowczego oraz placówki R7 mógł go wprowadzić w sekrety wyznaczanego mu zadania? Nic dziwnego, że w dalszej części swoich wyjaśnień opisywał jedynie profesjonalizm Trustu i oddanie sprawie jego członków. Oficer, wysłany do Moskwy bez jakiegokolwiek doświadczenia

⁵¹ CAW, Oddział II, sygn. I.303.4.1781, odpis pisma L.dz. 015/24 z 14 II 1924 r.

⁵² CAW, Oddział II, sygn. I.303.4.1781, załącznik nr 130 do *Arkusza obserwacyjnego org. „M”*.

i mający ograniczone kompetencje służbowe, przyjął za pewnik to, co mu opowiadali przełożeni, potem zaś, działając na podstawie tych ocen, stał się gorliwym, choć pewnie nieświadomym, współnikiem GPU.

Z powyższych przesłanek wynika oczywisty wniosek: **podobnie jak we wszystkich instytucjach o charakterze autorytarnym, tak i w Oddziale II SG WP informacje i opinie szły „z góry w dół”, wszelkie zaś próby przekazywania przez szeregowych pracowników wywiadu opinii sprzecznych z już ukształtowanymi opiniami kierownictwa spotykały się z odrzuceniem, ośmieszaniem i prześladowaniem autorów.**

- Hierarchicznie zbudowana organizacja wywiadowcza, w której najważniejszym motorem ludzkich zachowań jest pragnienie awansu pionowego (gdyż w instytucjach o ściśle przestrzeganej hierarchii dopiero taki awans daje wysokie zarobki i prestiż), powodowała uporczywe niedostrzeganie problemu w chwili, gdy już trwała operacja dezinformacyjna, a zwłaszcza w sytuacji, gdy należało się spodziewać, że towarzyszy jej infiltracja ze strony przeciwnika. Jak pisze J. Masterman na podstawie własnych doświadczeń z oszukiwania Abwehry podczas II wojny światowej:

Sam fakt, że dokonywaliśmy stale przeglądu tak wielu różnych, szczegółowych informacji, powodował, że nam wydawało się oczywiste, że wysłanie pewnej wiadomości musi spalić agenta. W rzeczywistości jednak sprawa ta wyglądała inaczej i to z wielu powodów. Przede wszystkim pierwszą instancją, do której agent wysyłał informacje, był jego bezpośredni przełożony, a ten z kolei przekazywał je wyższemu przełożonemu, bardzo często bez szczegółowego ich zbadania. Jeżeli nawet zawarte w informacji błędy lub świadoma dezinformacja polegały na wzajemnych sprzecznościach, jest mało prawdopodobne, że ci wyżsi przełożeni będą w posiadaniu tak dokładnych informacji, aby te błędy i sprzeczności zauważyli. Może się nawet zdarzyć, że właściwe źródło informacji nie zostanie wymienione, gdyż bezpośredni mocodawca agenta będzie chciał zachować swój prestiż, zwłaszcza jeżeli oprócz prawdziwych agentów ma jeszcze swoich agentów fikcyjnych. Jeżeli nawet wyższe władze powezmą jakieś podejrzenia, to właśnie ten bezpośredni przełożony agenta zrobi wszystko ze względu na swój prestiż i osobiste korzyści, aby obronić swojego informatora⁵³.

Mówiąc prościej, w hierarchicznej instytucji wywiadowczej z pozyskiwania informacji korzysta cały łańcuch osób nadzorujących agenta: jego oficer prowadzący, bezpośredni i wyższy przełożony oficera, a jeśli informacje odpowiadają założeniom polityków rządzących, podpierając ich tezy, to i kierownictwo danej służby. Odkrycie, że informacja była błędna lub fałszywa (zwłaszcza gdy została już przekazana „wyższemu czynnikom”) kompromituje ten sam łańcuch pośredników, stawiając

⁵³ J. Masterman, *Brytyjski system podwójnych...*, s. 56–57.

w złym świetle ich profesjonalizm i zdrowy rozsądek. To zaś może przekreślić główny cel ich działań w instytucji hierarchicznej, czyli karierę.

Dodatkowym elementem wspomnianym przez J. Mastermana jest naturalna tendencja instytucji wywiadowczych do unikania za wszelką cenę skandalu, który spowodowałby przeprowadzenie audytu przez osoby z zewnątrz, co mogłoby prowadzić do odkrycia pozorowania pracy i wyłudzenia pieniędzy z budżetu operacyjnego na fikcyjne źródła. Rejestrowanie fikcyjnych źródeł występowało we wszystkich służbach, choć w różnym nasileniu. Trudno określić, jaki był procent „martwych dusz” w Oddziale II, ale – dla porównania – gen. Franciszek Szlachcic określał ich liczbę w Służbie Bezpieczeństwa PRL na 30 proc. Pisał, że powstał cały przemysł wyłudzenia pieniędzy, w który wciągano kolegów i członków rodzin⁵⁴. W Oddziale II SG WP takie zjawisko występowało z całą pewnością. Dowodem tego był akt oskarżenia mjr. Jerzego Sosnowskiego, z którego jednoznacznie wynikało, że posługiwał się on fikcyjną agenturą, aby zwiększyć pulę pieniędzy otrzymywanych z centrali⁵⁵. Warto też pamiętać o finansowo-przemysłowych praktykach oficerów na placówkach, w których uczestniczyli lub które przynajmniej tolerowali ich przełożeni.

Wszystko to powodowało, że niemal na żadnym poziomie tej struktury nie chciało dopuścić do skandalu, który mógłby doprowadzić do dogłębnej, prokuratorskiej kontroli działań wywiadu i w rezultacie – do złamania wielu karier⁵⁶. Brakowało też motywacji, aby rzetelnie weryfikować informacje uzyskiwane od Trustu. Nawet w przypadku ewidentnie sfałszowanego dokumentu mobilizacyjnego Ewidencja, mimo oczywistych symptomów dezinformacji, nie odrzucała go. Żądała natomiast dodatkowych danych, choć przecież sama udawadniała, że założenia logistyczne w nim zawarte były niezgodne z logiką.

Gdy w kwietniu 1927 r. prawda o Truście została ujawniona, Oddział II najpierw długo się łudził, że to jedynie częściowa dekonspiracja realnie istniejącej organizacji „M”, potem zaczął dezawuować informacje E. Opperputa, ale jedynie w części odnoszącej się do agentury działającej w polskim Sztapie Generalnym⁵⁷. Jednocześnie próbowano się zorientować, czy dwuznaczna rola Oddziału II będzie zauważona na Zachodzie⁵⁸. Na końcowym etapie zaś – przy pomocy tzw. komisji Bocińskiego –

⁵⁴ J.S. Mac, *Przesłuchanie supergliny*, Warszawa 1990, s. 33.

⁵⁵ Archiwum Instytutu Pamięci Narodowej w Warszawie (dalej: AIPN), sygn. BU 01480/331, K. Graczyk, *Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych*, Katowice 2015, niepublikowana praca magisterska, UŚI, s. 239–250. Szerzej zob. H. Ćwiek, *Rotmistrz Sosnkowski. As wywiadu Drugiej Rzeczypospolitej*, Kraków 2011; Ł. Ulatowski, *Berlińska placówka wywiadowcza „In.3” (1926–1934). Oddział II i działalność majora Jerzego Sosnowskiego w Niemczech*, Warszawa 2016; P. Kołakowski, A. Krzak, *Sprawa majora Jerzego Sosnowskiego w świetle dokumentów analitycznych Oddziału II SG WP i zeznań Franza Heinricha Pfeifera*, Warszawa 2015.

⁵⁶ Taka sytuacja występuje powszechnie. T.H. Bagley opisał niepojęte działania kierownictwa CIA po sporządzeniu tzw. raportu niezgodności z przesłuchaniem defektora z KGB Jurija Nosenki.

⁵⁷ Był to zabieg karkołomny z punktu widzenia logiki formalnej, lecz w pełni zrozumiały na gruncie psychologii dysonansu poznawczego.

⁵⁸ Ta obawa wyziera z odpowiedzi nadesłanej do centrali z ataszatu w Londynie: „Na tutejszym

zatuszowano sprawę, rozmywając odpowiedzialność i blokując możliwość sanacji wywiadu na Wschód.

• J. Masterman za najważniejszy element powodzenia operacji dezinformacyjnych prowadzonych przez MI5 wobec Abwehry uznał **pobudki osobiste, które dominowały nad pełną integracją zespołów wchodzących w skład niemieckiego wywiadu**. Ujął tę myśl następująco:

Prawie zawsze bowiem, gdy Niemcy popełniali zasadniczy błąd, okazywało się, że było to wynikiem kierowania się o s o b i s t y m i pobudkami jakiegoś pracownika Abwehry. Robił on pieniądze i zyskiwał prestiż dzięki swojemu agentowi, wystarczyło też, aby dzięki niemu mógł się bezpiecznie uplasować w jakimś neutralnym porcie, to wówczas nie potrafił i nie chciał obiektywnie i uczciwie oceniać agenta i jego pracy⁵⁹.

Obserwacja J. Mastermana odnosi się również do Oddziału II. Centrala wysyłała oficerów do Rosji Sowieckiej, mając zupełnie oderwane od realiów wyobrażenia na temat możliwości prowadzenia tam działalności wywiadowczej. Oficerowie na placówkach działali w warunkach skrajnie niesprzyjających: poddani 24-godzinnej obserwacji i otoczeni donosicielami GPU ulokowanymi w poselstwie i konsulatach RP mieli wykonywać nierealistyczne zadania zlecane przez centralę. Byli stale podsłuchiwani i najczęściej pozbawieni nawet tak oczywistych narzędzi pracy, jak wystarczająca ilość pieniędzy. Kontrola kontrwywiadowcza prowadzona przez KRO GPU przypominała kontrolę prowadzoną zwykle wobec państw, z którymi jest się w stanie wojny. To sprawiało, że skuteczność polskich oficerów musiała być niezwykle niska⁶⁰. Polscy wywiadowcy znajdowali się w skrajnie trudnej sytuacji: z jednej strony nikłe były realne możliwości prowadzenia przez nich działalności wywiadowczej, z drugiej zaś byli bombardowani żądaniami Warszawy, których niespełnienie mogło mieć tragiczne skutki dla ich karier. Było to o tyle istotne, że oficerowie, podejmując służbę w wywiadzie, byli tak naprawdę w mniej korzystnej sytuacji awansowej niż oficerowie liniowi. Mieli utrudniony awans w stopniach, a ponadto rezygnowali ze względnej stabilizacji, jaką mieli np. w garnizonie stołecznym.

Należy powiedzieć wprost, że **interes służby stał w sprzeczności z interesami oficerów placówkowych**. Zamiast pełnej współpracy centrali z placówkami, widoczna była ewidentna rozbieżność ich interesów. Centrala żądała spełniania nierealnych oczekiwań, wzbraniając się przy tym przed ponoszeniem kosztów. Natomiast oficerowie,

gruncie nie grozi żadne niebezpieczeństwo opublikowania tej sprawy ani fałszywa jej interpretacja w stosunku do nas”. Zob. CAW, Oddział II, sygn. I.303.4.2090, pismo attaché wojskowego w Londynie, l.dz. 518/I/C z 26 V 1927 r. (prawdopodobnie do szefa Oddziału II Tadeusza Schaetzla lub – co mniej prawdopodobne – szefa Wydziału Ewidencyjnego Tadeusza Pełczyńskiego).

⁵⁹ J. Masterman, *Brytyjski system podwójnych...*, s. 262.

⁶⁰ Por. analizę nieskuteczności wywiadu w warunkach wojny, tamże, s. 236–264.

którzy wyjechali z Polski, robili wszystko, aby na placówkach jednak pozostać. Chcieli odnieść sukces lub choćby uniknąć kompromitacji. Warto też pamiętać o tym, że wyjazd na kilka lat z RP oznaczał nie tylko przerwanie kariery w wojsku, lecz także konieczność uregulowania w kraju spraw majątkowych. Powrót zaś oznaczał zarówno utratę diet dyplomatycznych, jak i problemy z ponowną adaptacją w ojczyźnie.

Prowokatorzy podsyłani przez KRO GPU trafiali na podatny grunt. Zła organizacja pracy oficerów na placówkach wywiadowczych stwarzała sytuację, w której dokładna analiza wiarygodności pojawiającego się agenta **nie leżała w interesie polskiego wywiadowcy**, który jednocześnie – jak można się spodziewać – uaktywniał opisany wyżej proces redukcji dysonansu i przekonywał sam siebie, że jeśli nawet agent wydaje się podejrzany, to z pewnością ma uczciwe intencje, albo, w najgorszym wypadku, da się go kontrolować przy pomocy innych źródeł. Polscy wywiadowcy, aby wykazać się przed centralą, musieli pozyskiwać agenturę, choć pełna kontrola ze strony sowieckiego kontrwywiadu skutecznie im to utrudniała. Byli więc narażeni na ryzyko zatrzymania, pobicia bądź odesłania do kraju. To powodowało, że istniała psychologiczna gotowość do wykorzystywania nadarzających się okazji, a także przyjmowania każdego podszywanego agenta, którego informacje stanowiły dla centrali dowód, że oficer działa i jest skuteczny. Taka ukryta motywacja jest widoczna np. w charakterystyce agenta W. Nałęcz-Wojciechowskiego sporządzonej przez płk. Romualda Wolikowskiego: (...) *komunista, mason, okultysta, typ o bardzo niewyraźnej fizjonomii*. Nawet przy najlepszej woli nie dałoby się takiego agenta uznać za mającego odpowiednie *bona fides*. Mimo to figurował on wśród członków siatki prowadzonej przez polskiego attaché wojskowego.

Oddział II SG WP nie wytworzył żadnych mechanizmów, za których pomocą można by było obiektywnie opiniować agenturę oficerów placówkowych, poza ocenami dostarczanych przez nich informacji dokonywanymi przez Ewidencję. Ta zaś na jednym z kolejnych etapów operacji dezinformacyjnej prowadzonej przez GPU musiała osiągnąć taki poziom nasycenia „fałszywkami”, że porównując nowo uzyskane produkty „kriwego zierkała”⁶¹ do już posiadanych zasobów (przy założeniu, że GPU potrafiło kontrolować wewnętrzną spójność produktów dezinformacji równie skutecznie, jak robiło to MI5 podczas II wojny światowej), nie była w stanie wychwycić dezinformacji. Porównywała informacje spreparowane, które pasowały do wcześniej przekazanych, również fałszywych⁶².

Jedynym sposobem wychwycenia dezinformacji było znalezienie nielogiczności założeń przyjętych przez Sowieców, bez zwracania uwagi na to, czy dana informacja wpasowuje się w już posiadany zasób wiedzy. I dokładnie tak zrobiła Ewidencja w przypadku opisanego wcześniej dokumentu mobilizacyjnego. Wskazano na jego sprzeczność z istniejącym zapleczem logistycznym niezbędnym dla transportu

⁶¹ Żartobliwa nazwa międzyresortowego Biura Dezinformacji.

⁶² G. Bailey pisze o sytuacjach jeszcze groźniejszych, kiedy to odrzucano informacje z innych źródeł, jeśli nie były zgodne z informacjami pozyskiwanymi od zaufanego Trustu. Zob. G. Bailey, *The Conspirators*, London 1961, s. 12–13.

wojsk. Tak więc polscy analitycy potrafili wyciągać poprawne wnioski, jednak – zgodnie z zasadami dedukcji – mając fałszywe przesłanki, musieli uzyskiwać fałszywe rezultaty.

Z zachowanych materiałów wynika, że w Oddziale II SG WP w czasie prowadzenia operacji „Trust” dochodziło do ciągłych tarć na tle ambicjonalnym⁶³, a oficerowie byli tak skupieni na sobie, że woleli kompromitować służbę niż siebie. Wynika to jednoznacznie m.in. z korespondencji nawet tak dobrego oficera, jak por. T. Werner, który pisał:

Melduję, że jeden z przedstawicieli organizacji „M” wyraził zdziwienie, że nie napisałem do Warszawy w sprawie wyrobienia paszportu dla Denisowa, żeby wykręcić się z głupiej sytuacji, w której bez swej winy się znalazłem, oświadczyłem, że pismo w sprawie paszportu wysłałem szyfrem i że zostało ono prawdopodobnie niedokładnie odszyfrowane⁶⁴.

Można przyjąć za J. Mastermanem, że **Oddział II na skutek braku pracy zespołowej i ścisłego powiązania sukcesu oficera z pracą pozyskanej przez niego agentury, bez wprowadzania starannych procedur sprawdzeniowych i ciągłej weryfikacji wiarygodności obsługiwanych agentów, stworzył ramy dla sukcesu sowieckiej dezinformacji.**

- Warunkiem koniecznym wymienionych czynników jest niski poziom profesjonalizmu oficerów Oddziału II, który wpłynął na wystąpienie opisanych wcześniej negatywnych zjawisk. Na początku lat 20. XX w. jego powody były oczywiste: polski wywiad był tworzony przez amatorów wywodzących się z młodzieży peowiackiej oraz oficerów legionowych. Działalność dywersyjno-wywiadowcza tych pierwszych była pozbawiona jakiegokolwiek zaplecza logistycznego i szkoleniowego⁶⁵, oficerowie legionowi zaś sprowadzali swoją działalność wywiadowczą do prowadzenia rozpoznania wojskowego, a kontrwywiadowczą – do wyłapywania dezertersów i „elementów podejrzanych”⁶⁶.

O stanie przygotowania kadry służby informacyjnej można wywnioskować ze wspomnień W.T. Drymmera. Wynikało z nich, że polska służba informacyjna była organizowana ad hoc, a rolę kierownika Oddziału IV Informacyjnego, i jednocześnie wychowawcy nowych kadr, powierzono byłemu oficerowi skompromitowanej

⁶³ Por. opisany już przypadek wymuszenia przez I. Boenera dotyczący zapoznania jego adiutanta z agenturą prowadzoną przez oficerów placówkowych.

⁶⁴ CAW, Oddział II, sygn. I.03.4.1781, pismo l. dz. 019/24 z 1 II 1924 r.

⁶⁵ Dla ilustracji: W. Michniewicz opisuje działalność komórki POW w Humaniu, która – nie mając żadnej broni ani środków wybuchowych – „prowadziła sabotaż”, przecinając nożycami krawieckimi linie telefoniczne ukraińskiego garnizonu. Zob. W. Michniewicz, *Wielki bluff sowiecki...*, s. 12–13.

⁶⁶ Jak wyglądała praktyka takich działań, opisał gen. Józefa Rybak w swoich wspomnieniach. Psychozie nakazującej w każdym cywilu widzieć szpiega nadał nazwę „spioninitis”. Zob. J. Rybak, *Pamiętniki generała Rybaka*, Warszawa 1954, s. 102.

c. i. k. armii, której organizacja, modus operandi i aktywa operacyjne były dokładnie znane Rosjanom dzięki zdradzie płk. Alfreda Redla. Gen. Józef Rybak, który prowadził szkolenie, **nigdy sam nie był przeszkolony wywiadowczo**, a tajniki pracy w HK Stelle poznawał intuicyjnie; jego działalność rozpoznawcza przeciwko Rosji była znana rosyjskiemu agentowi – płk. A. Redlowi⁶⁷. Jeśli wierzyć opisowi kpt. W.T. Drymmera⁶⁸, samo szkolenie odbyło się w sposób urągający elementarnemu profesjonalizmowi:

Gen. Rybak w jakimś narzeczu, czy gwarze polsko-austriackiej, w której mieszały mu się słowa polskie z czeskimi i niemieckimi, dawał nam fachowe rady i tłumaczył rolę oficera informacyjnego, bo tym słowem kamuflowano właściwe nasze przeznaczenie: wywiad. Mnie z odprawy tej pozostał w głowie chaos, pamiętałem tylko słowa: „szyf, Dancyg, zaś-ale”. Wszystko to raczej śmieszyło, niż interesowało⁶⁹.

Ta sytuacja nie powinna oczywiście dziwić, gdyż Oddział II był budowany od podstaw, ad hoc, bez oparcia się na jakimkolwiek poważnym dorobku i kadrze. Problem polegał jednak nie na tym, że pierwsze pokolenie oficerów wywiadowczych było niedokształcone i dobrane z klucza koleżeńskigo, lecz na tym, że później to pokolenie, wspierające się w ramach opisanej przez kpt. W.T. Drymmera „sitwy”, już jako kierownictwo Oddziału II nadało ton całemu wywiadowi i narzuciło swoje wyobrażenia o tym, jak powinno się prowadzić wywiad, oraz decydowało o doborze ludzi, ich szkoleniu zawodowym czy awansach. Stąd prawdopodobnie brały się takie kurioza biurokracji wojskowej, jak np. wystawianie pozyskanym agentom legitymacji współpracownika, wręczanie im drugiego egzemplarza kontraktu dotyczącego współpracy z wywiadem⁷⁰ i zbioru *Przepisów o prowadzeniu służby wywiadowczej*⁷¹, a także nacisk na wywiad dokumentarny, dzięki któremu niezwykle łatwo było GPU manipulować polskimi oficerami przez podsuwanie im bezwartościowych fałszywek. Problemem były też kwestionariusze wykorzystywane podczas przesłuchań⁷² uciekinierów i oferentów sprowadzające indagację wywiadowczą do urzędniczego rozpytywania oraz stosunkowo niskie uplasowanie

⁶⁷ Tamże, s. 15–17.

⁶⁸ Trzeba brać pod uwagę niechęć W.T. Drymmera jako przedstawiciela „piłsudczyków” do J. Rybaka, jednakże sam J. Rybak we wspomnieniach pisał otwarcie o braku własnego przygotowania oraz o tym, że oficerów nowo przyjętych do WP z c. i. k. armii przywitał mową powitalną... w języku niemieckim (!).

⁶⁹ W.T. Drymmer, *W służbie Polsce*, Warszawa–Kraków 2014, s. 84.

⁷⁰ Warto zadać sobie pytanie: gdzie pozyskani współpracownicy mieli – zdaniem oficerów Oddziału II – przechowywać te dokumenty, zwłaszcza w sytuacji, gdy po wojnie mieszkali po kilku w wynajmowanych pokojach, K. Danielewicz, *Formy i metody pracy operacyjnej wywiadu polskiego w latach 1921–1939 na przykładzie Lwowskiej Ekspozytury nr 5 Oddziału II Sztabu Generalnego (Głównego)*, w: *Wywiad wojskowy II Rzeczypospolitej*, P. Kołakowski, A. Peplowski (red.), Kraków 2011, s. 305.

⁷¹ Tamże, s. 308.

⁷² Tamże, s. 292.

rezydentów polskiego wywiadu w placówkach dyplomatycznych, utrudniające współpracę z często niechętną wywiadowi kadrami dyplomatyczną. Co gorsza, do powyższych elementów należało też dodać ogólnie niski poziom wiedzy wojskowej personelu wywiadowczego⁷³.

Za błędami Oddziału II stał nie tylko brak fachowości kadry oficerskiej, lecz także rażący brak rozpoznania rzeczywistej sytuacji panującej w Rosji Sowieckiej. To powodowało, że naciskano na stosowanie takich form prowadzenia działalności szpiegowskiej, jak np. na biały wywiad⁷⁴, który polegał na czasochłonnym czytaniu sowieckiej prasy i wydawnictw specjalistycznych. W związku z powszechną w Rosji Sowieckiej cenzurą i wykorzystaniem przez GPU prasy do dezinformacji nie mogło to jednak dawać rezultatów adekwatnych do nakładów organizacyjnych niezbędnych do zdobycia i przeanalizowania materiałów. Niewykluczone jednak, że pozwalało na wyciąganie pewnych wniosków⁷⁵. Wykorzystywanie w łączności wywiadowczej listów pisanych atramentem sympatycznym wynikało z niewiedzy o tym, że w Rosji Sowieckiej otwierano i sprawdzano **wszystkie** listy wysyłane za granicę i stamtąd przychodzące⁷⁶. Niefortunne były także pomysły dotyczące wykorzystywania agentów manewrowych, którzy po przekroczeniu granicy mieli zbierać informacje na temat stosunków panujących w Rosji, a wręcz kuriozalnym wymysłem było np. werbowanie w szaletach dworcowych agentów, którzy mieli podsłuchiwać rozmowy sowieckich kolejarzy⁷⁷.

Z punktu widzenia systemowego Oddział II charakteryzował się trzema głównymi defektami, które musiały odbić się na jego funkcjonowaniu. Należały do nich:

- 1) tworzenie wywiadu od zera, bez zaplecza know how, z przypadkowych ludzi, którzy dzięki szybkim awansom wojennym zajmowali kierownicze stanowiska w służbie informacyjnej;
- 2) uplasowanie wywiadu, które sprzyjało selekcji negatywnej oficerów trafiających do tej służby; było to spowodowane przepisami wewnątrzarmijnymi preferującymi oficerów liniowych z tzw. cenzusem dowodzenia, oficerowie informacyjni zaś byli zwykle pomijani w awansach i odznaczeniach; szef Oddziału II nie miał swobody doboru pracowników, a jego potrzeby kadrowe były zaspokajane w drugiej kolejności⁷⁸;

⁷³ Tamże, s. 283.

⁷⁴ Tamże, s. 288.

⁷⁵ Na podstawie identycznej metodologii rozpoznania ani CIA (ani żaden ośrodek sowietologiczny w USA) nie potrafiła ocenić rzeczywistej sytuacji społeczno-gospodarczej w ZSRR i przewidzieć – co wydaje się niezwykle – rozpadu państwa związkowego.

⁷⁶ W okresie 1945–1990 ta praktyka była powszechnie stosowana przez wzorującą się na służbach sowieckich polską Służbę Bezpieczeństwa. Dzięki monitorowaniu tego kanału łączności, chętnie wykorzystywanego przez służby zachodnie, SB uzyskiwała najwięcej naprowadzeń na agenturę w PRL.

⁷⁷ K. Danielewicz, *Formy i metody pracy operacyjnej...*, s. 288.

⁷⁸ CAW, Oddział II, sygn. I.303.4.1144, sprawozdanie pplk. Głabisza z kontroli finansowej z 16 II 1932 r.

- 3) stałe niedofinansowanie wywiadu⁷⁹ spowodowane szukaniem oszczędności, i to pomimo małej liczebności kadr tej struktury, zwłaszcza w porównaniu z liczebnością służb sowieckich.

W rezultacie, jak pisze K. Danielewicz, wywiad stałe cierpiał na niedostatek zdolnych, inteligentnych i oddanych służbie oficerów⁸⁰, którzy borykali się na placówkach w Rosji z problemami finansowymi, lokalowymi i stałą inwigilacją ze strony sowieckiego kontrwywiadu.

Podczas trwania operacji „Trust” nie zaobserwowano nawet elementarnego profesjonalizmu w działaniach polskich służb wywiadowczych. Najbardziej dobitnym dowodem na kompletny brak wiedzy dotyczącej realiów sowieckich są wspomnienia W. Michniewicza, w których całkowicie się dyskredytował jako oficer wywiadu, z czego należy wnosić, że pisał prawdę. Nawet kilkadziesiąt lat po opisywanych zdarzeniach nie pojmował, że się kompromituje. Zarówno Michniewicz, jak i inni oficerowie Oddziału II nie widzieli nic złego w tym, aby wysyłać polskim szyfrem informacje Trustu, przez co sowiecki dekryptaż nie miał najmniejszych problemów z ich łamaniem⁸¹. Ponadto W. Michniewicz przechowywał listy polecające do generałów Akademii Sztabu Generalnego Armii Czerwonej w walizce... trzymanej pod łóżkiem.

To jednak nie wyczerpuje listy błędów popełnionych przez niego. Wystarczy się wczytać w przytoczoną po latach treść jego raportu na temat Trustu z 1923 r., aby pojąć ogrom ignorancji polskich oficerów. Cytując rozmowę ze swoim informatorem płk. W. Drobyszewskim, Michniewicz nie podał żadnej informacji źródłowej, która mogłaby dekonspirować Trust. Cała zawartość raportu składała się jedynie z **opinii** rozmówcy, które jednak „oślśniły” polskiego oficera:

Zamachowcy pozostają w stałej łączności z zagranicą, a w Moskwie i na prowincji werbują masowo członków? Są na stanowiskach rządowych i dostarczają materiałów szpiegowskich? Sami jeżdżą za granicę i spokojnie wracają, jak z majówki w podmiejskich Sokolnikach? Przy dzisiejszym terrorze? (...) Tylko bałwani mogą w to wierzyć! To jawna prowokacja ze strony GPU (...) To straszna blaga, to wielka głupota z waszej strony, iść na lep takich bzdur! Każdy byle ex-carski oficer, cóż dopiero

⁷⁹ Dobitnym przykładem notorycznego oszczędzania na wywiadzie w okresie operacji Trust może być pismo por. T. Wenera z 29 II 1924 r., który prosząc o zwiększenie gaży, pisał: „Raport w sprawie wynagrodzenia, które wskutek wzrostu cen w Moskwie stało się niewystarczającym (do norm. gaży 30 funtów): Pomijając fakt, iż misja, którą mi powierzono, jest daleko trudniejsza i bardziej ryzykowna niż praca oficjalnego adjutanta Attache Wojskowego, muszę nadmienić, że będąc fikcyjnym urzędnikiem Wydziału Konsularnego Przy Poselstwie RP w Moskwie, wykonuję normalną pracę urzędnika konsularnego i od godz. 10 rano do 5 pp. siedzę w biurze, załatwiając sprawy nie mające nic wspólnego z wywiadem. Dopiero godziny pozabiurowe mogę poświęcić właściwej pracy, której zazwyczaj nie jestem w stanie ukończyć przed godz. 2 w nocy (...)”; CAW, Oddział II, sygn. I.303.4.1781, pismo bez nazwy l.dz. 024/24 z 18 III 1924 r.

⁸⁰ K. Danielewicz, *Formy i metody pracy operacyjnej...*, s. 318.

⁸¹ Sam szyfr nie był szczególnie trudny do złamania, gdyż polegał na przyporządkowaniu każdej głosce, grupie głosek, cyfrze lub znakowi pisarskiemu pary cyfr, zob.: K. Danielewicz, *Formy i metody pracy operacyjnej...*, s. 295.

nasi generałowie na stanowiskach w Akademii, jak ściśle muszą być inwigilowani (...). A materiały wywiadowcze są na pewno fałszowane, przynęta dla frajerów! W najdurniejszy sposób dajecie się nabierać tyle czasu (...). Kasatkin chodzi do polskiego konsulatu, jak do baru publicznego? A Jakuszew – konspirator afiszuje się niczym czeladnik Cziczerina? Tylko ślepi nic nie widzą, że cała „organizacja” jest narzędziem GPU!⁸²

Wystarczy się chwilę zastanowić nad tym zdaniem, aby pojąć, że oficer polskiego wywiadu wystawia jednoznaczną ocenę skuteczności własnemu przygotowaniu zawodowemu. Z tekstu bowiem wynika, że nie rozumiał, że stałą inwigilacją byli objęci zarówno polscy oficerowie, jak i użytkowane przez nich placówki przykrycia, nie pojmował, że każdy Rosjanin trafiający do polskiego poselstwa lub konsulatu stawał się obiektem zainteresowania operacyjnego GPU, nie zdawał sobie także najwyraźniej sprawy ze skali nieustannej inwigilacji i terroru, które skutecznie blokowały nawiązywanie kontaktów przez obywateli sowieckich z pracownikami obcych przedstawicielstw dyplomatycznych⁸³. Może to oznaczać, że polski wywiad na początku lat 20. XX w. miał ograniczone rozpoznanie sowieckich realiów lub że te realia całkowicie lekceważył.

Przegląd materiałów archiwalnych Oddziału II dotyczących współpracy z Trustem jest niestety ilustracją powyższych tez. Warto przypomnieć co ciekawsze wydarzenia pokazujące rzeczywisty poziom profesjonalizmu polskich oficerów i stopień lekceważenia przez nich podstawowych zasad konspiracji – zarówno na placówkach, jak i w centrali.

Ze wspomnień kpt. Michniewicza oraz S. Wojciechowskiego wiadomo, że spotkania z delegacjami rzekomych monarchistów przyjeżdżających do Warszawy w celu prowadzenia rozmów z kierownictwem Oddziału II odbywały się w modnych warszawskich restauracjach. Według S. Wojciechowskiego na tego typu wywiadowcze rendez-vous kpt. M. Talikowski przychodził ubrany w regulaminowy mundur⁸⁴. Tenże sam Talikowski, chcąc poinformować J. Artamonowa o terminie przetrzutu agentury Trustu, nie zastawszy go w domu, zostawił jego rosyjskiej żonie podpisany przez siebie otwarty liścik dotyczący tej sprawy.

Jak wspomniano, działalność J. Artamonowa w Warszawie nie wzbudziła żadnego zainteresowania Oddziału II, pomimo że młody arystokrata dysponował dość wysoką sumą pieniędzy, nie mając żadnej stałej pracy. Nie zainteresowano się nim nawet wtedy, gdy zaczął werbować polskich urzędników ministerialnych do warszawskiego ZJARMA⁸⁵. Kiedy w 1927 r. – najprawdopodobniej w ramach zwiększania

⁸² W. Michniewicz, *Wielki bluff sowiecki...*, s. 128–130.

⁸³ Cytowany już raport por. T. Wernera na temat kontaktowania się przedstawiciela Trustu z por. J. Szczepkowskim wskazuje na to, że akurat ten oficer w pełni pojmował skalę problemu.

⁸⁴ S. Wojciechowski, *Triest. Wspominanija*, London (Kanada) 1974, s. 34. Można założyć, że S. Wojciechowski, gardzący kpt. M. Talikowskim, był złośliwy w opisie, jednak pasuje to do sknerstwa M. Talikowskiego opisanego w książce W. Michniewicza, który znał osobiście Talikowskiego.

⁸⁵ W. Michniewicz, *Wielki bluff sowiecki...*, s. 114.

chaosu informacyjnego strony polskiej – S. Wojciechowski oraz niejaki Andro przekazali informację, że J. Artamonow mógł być w 1918 r. na usługach CzeKi, odbierający tę informację por. M. Freyman z rozbijającą szczerością napisał w raporcie, że nie sporządził z tego protokołu, gdyż obaj rozmówcy zastrzegli sobie dyskrecję⁸⁶. W aktach brakowało także śladów prób zweryfikowania tej informacji przez polski wywiad.

Innym przykładem niepojętej naiwności kierownictwa Oddziału II są dwa dokumenty z 1927 r.:

Aleksandrowicz (czyli J. Artamonow – przyp. aut.) podał, że w Poselstwie Afgańskim w Moskwie pracuje jedna z sióstr Straszkiwicz, przez którą w 1921 r. otrzymał kontakt i poznał Fiodorowa i Kolesnikowa. Chcąc się przekonać, czy ostatecznie areszty dot. Straszkiwiczów, i zbadać, czy są one na usługach GPU, Aleksandrowicz dołączył list do Warwary Nikołajewny Straszkiwicz z prośbą o dyskretne doręczenie i otrzymanie na miejscu odpowiedzi.

Przesłanie tego listu do Moskwy pozwoli na ustalenie:

- 1) czy W. S. do chwili obecnej jest na posadzie w Poselstwie Afgańskim,
- 2) czy w ogóle będzie chciała dać odpowiedź na załączony list względnie udzielić ustnych informacji okazielowi,
- 3) w razie odmowy zorientowanie naszego attache wojskowego o pracy agentów GPU w Poselstwie Afgańskim⁸⁷.

W załączeniu list pisany przez łącznika Organizacji „M” P. Artamonowa do W.N. Straszkiwicz rzekomo urzędniczki Poselstwa Afgańskiego. „Siostra Warwary N. S. jest tą osobą, która w r. 1921 dała listy polecające do Artamonowa najważniejszym psuedocłonkom Organizacji „M”. Chcąc się obecnie przekonać czy wym. Straszkiwicz jest nadal względnie była agentką GPU Artamonow złożył w tut. Oddziale list z prośbą o dowiedzenie się, czy W. Straszkiwicz w Poselstwie Afgańskim pracuje (...). Proszę o doręczenie go. W każdym razie oczekuję odpowiedzi, czy Straszkiwiczówna pracuje w Poselstwie, jeżeli nie, to kiedy była zwolniona i przy jakich okolicznościach⁸⁸.

Powyższa notatka z rozmowy oraz będący jej skutkiem szyfrogram do Moskwy są przykładami niezwykle wręcz naiwności ppłk. Tadeusza Schaetzla. Aby zrozumieć sytuację, wystarczy przeczytać polecenia wydane przez niego podwładnym. Szef polskiego wywiadu po otrzymaniu od Rosjanina podejrzanego o związki z GPU informacji, która miała jedynie podbudować zaufanie Polaków do J. Artamonowa

⁸⁶ CAW, Oddział II, sygn. I.303.4.2090, raport kierownika Referatu „B-1” do kierownika Referatu „C” mjr. J. Grudzińskiego z 1 VII 1927 r. (zał. 183).

⁸⁷ CAW, Oddział II, sygn. I.303.4.2090, dokument zatytułowany PRO DOMO, bez daty i liczby dziennika.

⁸⁸ CAW, Oddział II, sygn. I.303.4.2090, pismo do Attachatu Wojskowego w Moskwie (brak opisu kancelaryjnego), z (b.d.d.) VI 1927 r.

(bo przecież wciąż przekazywał informacje operacyjne), każe przekazać jego liścik do ciotki będącej rzekomo agentem GPU w Moskwie. Szef Oddziału II nie dostrzegając najwyraźniej absurdalności wydanego polecenia, zgodnie z którym oficer polskiego wywiadu miał dostarczyć informatorce GPU list od krewnego, niewidzianego od 10 lat, zawierający prośbę o udzielenie informacji, czy rzeczywiście pracuje ona na rzecz GPU. Pomijając niedorzeczność pomysłu, aby aktywny agent GPU miał się przyznać nigdy niewidzianemu człowiekowi przedstawiającemu się jako polski dyplomata, że rzeczywiście wypełnia polecenia sowieckiego kontrwywiadu, należy zauważyć, że ppłk T. Schaetzel wysyłał swojego oficera z poleceniem nie dość, że głupim, to w dodatku absolutnie nieistotnym z punktu widzenia polskiego wywiadu. Zamiast sprawdzić, czy J. Artamonow jest agentem GPU działającym w Warszawie, oficer miał wykonywać karkołomną operację nawiązania kontaktu z ciotką J. Artamonowa zamieszkałą w Moskwie, aby ustalić, czy nie szpieguje ona tamtejszego Poselstwa Afgańskiego. W dodatku nikt nie zauważył, że informacje J. Artamonowa o ciotce są uwiarygodnieniem wersji lansowanej od początku przez agenturę GPU, zgodnie z którą operacja tej struktury w Rewlu była przypadkowym zbiegiem okoliczności wykorzystanym sprytnie przez W. Steckiewicza, a nie spektaklem zaplanowanym dla emigrantów i zachodnich wywiadów, dzięki czemu oddalano podejrzenia wobec pierwszych aktorów afery, tj. Jurija Artamonowa i Wsiewołoda Szczełgaczewa.

Wysłanie do Finlandii ppłk. L. Bocińskiego, nieznającego ani języka rosyjskiego, ani realiów sowieckich, w celu przesłuchania E. Opperputa, a także dołączenie kpt. M. Talikowskiego do ppłk. L. Bocińskiego odpowiedzialnego za afere i zainteresowanego zamieceniem sprawy pod dywan, nie wyczerpuje listy błędów popełnianych przez kierownictwo Oddziału II. Jak wynika z materiałów archiwalnych, kpt. M. Talikowski, wysyłając do Rosji Sowieckiej agenturę niezależną od Trustu, prosił tę organizację o pomoc w przetruciu agentów, znalezieniu im dokumentów i załatwieniu kredytu potrzebnego do rozpoczęcia działalności⁸⁹. Oznacza to, że kierownik Referatu „Wschód” łamał podstawową zasadę prowadzenia działalności wywiadowczej zakazując udzielania informacji agenturze na temat innych agentów działających na jej terenie.

Z tego samego źródła można wywnioskować, że Oddział II pod kierownictwem kpt. M. Talikowskiego zaangażował się we współpracę gospodarczą z Trustem, prowadząc rozmowy z którymś z polskich ministerstw, nazywanych w piśmie *Ministerstwom Gosudarstwiennym Imuszczestw*⁹⁰. Tym sposobem doprowadzono do kolejnego błędu, jakim było uwikłanie oficerów w niejasne powiązania biznesowe z agenturą (jak się okazało po czasie – podwójną), co zawsze stwarza ryzyko zdobycia materiałów nacisku na kadre oficerską.

⁸⁹ CAW, Oddział II, sygn. I.303.4.1781, tekst maszynowy bez opisu, pisany w języku rosyjskim dorewolucyjną ortografią z dopiskiem po polsku: „kto pisze?”.

⁹⁰ Tamże. Ta sprawa nie była nigdy i przez nikogo poruszona, z czego można wnosić, że musiała istnieć dość duża grupa ludzi zainteresowanych jej wyciszeniem.

Nie tylko centrala zachowywała się w tak skandalicznie nieprofesjonalny sposób. Wileńska Ekspozytura nr 1 gościła u siebie z honorami rzekomego delegata Eurazji z ramienia Trustu A. Denisowa, który podczas pijackich ekscesów z W. Sekundą⁹¹ zdołał nie tylko przeprowadzić rozpoznanie polskiej placówki, lecz także nawiązać z tą placówką relacje niejako poza kontrolą Warszawy⁹².

W Moskwie, pomijając opisane już wcześniej całkowite „zanurzenie” polskiego wywiadu w agenturze GPU skutkujące całkowitą kontrolą nad nim Sowieców, dochodziło do tak kuriozalnych przypadków, jak np. zniszczenia listów przekazywanych przez Trust polską pocztą dyplomatyczną z powodu użycia złych odczynników chemicznych, za pomocą których chciano wyjawiać ukrytą treść⁹³. Smaczku sprawie dodaje informacja, że zniszczenie listów (które bezspornie dowiodło Sowiecom, że Polacy perlustrują ich korespondencję) odbyło się podczas pobytu por. T. Wernera na ul. Brackiej. Kpt. T. Rybotycki nakazał mu otworzyć korespondencję Trustu, aby zademonstrować innym oficerom, jak robi się to właściwie⁹⁴. Por. T. Werner nie miał narzędzia (w postaci kości) używanego zwykle do wygładzenia papieru pomarszczonego przez chemikalia⁹⁵. Mówi to, niestety, wiele o przygotowaniu technicznym polskiego wywiadu oraz o lekkomyślności jego kierownictwa.

Innym przykładem o niemal komediowym charakterze było podanie agentowi przez polskiego wywiadowcę określanego jako „Cz” (prawdopodobnie Edwarda Czyżewskiego) numeru kontaktowego z błędem w cyfrze, wskutek czego zadzwonił on do... prywatnego mieszkania w Moskwie, podając umówione hasło. Ponieważ, co oczywiste, ta informacja nie dotarła do polskiego oficera, agent czekał bezskutecznie na pojawienie się tego oficera w miejscu i czasie podanych mu jako zapasowe, gdyby nie nawiązano łączności telefonicznej. Nikt się nie pojawił, zrozpaczony Rosjanin więc, nie mogąc inaczej wywołać spotkania z Polakami, po prostu poszedł do Poselstwa RP⁹⁶.

Powyższe przykłady można traktować jako anegdotyczne, ale świadczą one o poważnych błędach systemowych popełnianych przy tworzeniu, a następnie kierowaniu polskim wywiadem. Większość oficerów, przynajmniej na początku lat 20. XX w., nie miała żadnej wiedzy teoretycznej, mieli też niewielką praktykę. Doświadczenie zdobywali albo podczas działań wojennych (w warunkach, które różniły się od czasu pokoju, czyli normalnej pracy wywiadu), albo na bieżąco, podczas tworzenia placówek wywiadowczych na Wschodzie.

Polski wywiad na Wschodzie od samego początku był kontrolowany przez kontrwywiad przeciwnika za pomocą podwójnej agentury. Polscy oficerowie zamiast poznawać rzemiosło wywiadowcze w praktyce i przekształcać doświadczenia

⁹¹ W. Michniewicz, *Wielki bluff sowiecki...*, s. 165.

⁹² CAW, Oddział II, sygn. I.303.4.1781, tekst maszynowy bez opisu, pisany po rosyjsku dorewolucyjną ortografią z dopiskiem po polsku: „kto pisze?”.

⁹³ CAW, Oddział II, sygn. I.303.4.1781, pismo Placówki „R.7/I” do Referatu Centralnej Agentury, l. dz. 013/24 z 6 II 1924 r.

⁹⁴ Tamże.

⁹⁵ Tamże.

⁹⁶ CAW, Oddział II, sygn. I.303.4.1781, meldunek napisany w języku rosyjskim (b.d.), z adnotacją po polsku: „do kogo i od kogo?”.

w wywiadowcze know how, od początku byli systematycznie oszukiwani. W takich warunkach nie dało się stworzyć sprawnych struktur wywiadowczych, brakowało bowiem realnych osiągnięć, które mogły stać się podstawą do opracowania skutecznych instrukcji działań operacyjnych. Można obrazowo powiedzieć, że Oddział II w swoich działaniach na Wschodzie od początku budował swoją wiedzę i doświadczenie na iluzjach. Uniemożliwiało to zdobycie umiejętności w rozpoznawaniu przeciwnika⁹⁷. Co więcej, ani w latach operacji, ani w 1927 r., kiedy już nawet dla Oddziału II stało się jasne, że – jak pisał S. Mayer – (...) *nie ma nic tajnego w polskiej służbie specjalnej*⁹⁸, nie podjęto systemowych działań sanacyjnych mających na celu zmianę kadr i przyjętych rozwiązań operacyjnych.

Brak profesjonalizmu polskiej kadry był wynikiem błędnych rozwiązań systemowych. Polski wywiad, choć wyjątkowo nieliczny, był na początku lat 20. XX w. słabo finansowany, źle wyszkolony i rządzony z jednej strony przez upolitycznione kierownictwo, z drugiej zaś przez grupy o charakterze wspólnotowym, czyli, mówiąc dosadnie, przez nieformalną sieć układów, zwanych przez W.T. Drymmera „sitwami”. Układy te opierały się na znajomościach bądź koleżeństwie, które wpływały na jakość doboru kadr wywiadu.

W opisanych działaniach Oddziału II wyraźnie widać wpływ tych czynników. Raport W. Michniewicza został skompromitowany nie tylko przez wskazanie na jego nieadekwatność, lecz także uczyniono to na użytek kierownictwa Oddziału II wyznaczonego przez Chjeno-Piasta. Raport W. Michniewicza przedstawiono jako możliwą intrygę oficerów będących zwolennikami Józefa Piłsudskiego⁹⁹. Z kolei wybór oficerów wysyłanych na placówki wschodnie był znakomitą ilustracją tezy o braku jakichkolwiek obiektywnych procedur ocennych stosowanych przy typowaniu kandydatów na takie stanowiska. Od samego początku łącznikami z Trustem zostawali ludzie niezwykle młodzi, bez jakiegokolwiek doświadczenia. Część z nich (jak np. rtm. A. Niedziński) ze względu na braki intelektualne i osobowość z góry była zdyskwalifikowana jako oficerowie wywiadowczy. Jedynym kryterium wyboru była znajomość z osobami decydującymi o wyznaczeniu kandydata na to stanowisko. W. Michniewicz pojechał na placówkę w Moskwie, gdyż znał się (i zapewne przyjaźnił) z kpt. W.T. Drymmerem, który również wysłał swojego kolegę z Legionów (Czyżewskiego) jako zastępcę chorego W. Michniewicza¹⁰⁰. Jego następcy na stanowisku łącznika z MOCR zawdzięczali to stanowisko personalnym decyzjom kpt. M. Talikowskiego, przy czym, jeśli wierzyć pozostawionym przez nich dokumentom, „ulegali prośbom” kierownika Referatu „Wschód”¹⁰¹. Wynika z tego,

⁹⁷ Por. opinię kpt. W.T. Drymmera: „Ponieważ nasz Oddział II nie składał się z zawodowców, wyszkolenie szwankowało. Uczono się od kolegów, na własnych błędach i na krótkoterminowych kursach”; W.T. Drymmer, *W służbie Polsce...*, s. 124–125.

⁹⁸ A. Krzak, „Czerwoni Azefowie”. *Afera „MOCR-TRUST” 1922–1927*, Warszawa 2010, s. 157.

⁹⁹ W. Michniewicz, *Wielki bluff sowiecki...*, s. 132.

¹⁰⁰ W.T. Drymmer, *W służbie Polsce...*, s. 107.

¹⁰¹ CAW, Oddział II, sygn. I. 303.4.1781, pismo T. Wernera do W.T. Drymmera, l.dz. 08/24 z 24 I 1924 r.

że przynajmniej w odniesieniu do tej operacji prowadzonej przez Oddział II nie stosowano w polskim wywiadzie żadnych procedur – poza osobistymi znajomościami – które mogły wyłonić odpowiedniego kandydata na jakiegokolwiek stanowisko merytoryczne. Na tej samej zasadzie pomocnikiem attaché wojskowego w Rewlu został kpt. W.T. Drymmer, choć dopiero co odszedł z wojska i deklarował niechęć do panujących tam stosunków. Poza tym nie miał pojęcia o wywiadzie.

Do przesłuchania E. Opperputa w 1927 r. wyznaczono ppłk. L. Bocińskiego, który, jak już wspomniano, nie znał ani słowa po rosyjsku¹⁰². Oddział II podejmował więc decyzje personalne nie tylko na podstawie woluntaryzmu decydentów, lecz także w oderwaniu od najbardziej, wydawałoby się, oczywistych wymagań wobec powierzonego zadania. Nikt chyba nie sądził, że ppłk L. Bociński, nie mówiąc po rosyjsku¹⁰³ i nie mając pojęcia o stosunkach panujących na Wschodzie, jest w stanie przeprowadzić przesłuchanie postaci najważniejszej w sprawie. Mówi to wiele o rzeczywistych mechanizmach decyzyjnych w Oddziale II oraz o tak ważnym elemencie dobrego zarządzania i motywowania personelu, jak otwartość ścieżek awansu dla zdolnych i pracowitych oficerów.

Z analizy materiału źródłowego dotyczącego operacji „Trust” wyłania się obraz polskiego wywiadu rządzonego przez ludzi połączonych nieformalnymi zależnościami, które potrafiły przeważyć nad elementarnym zdrowym rozsądkiem. Przykładem tego jest mianowanie rtm. A. Niedzińskiego na kierownika Referatu „Wschód”, pomimo że był on świetnie znany Rosjanom, przez lata dawał im się wodzić za nos i dał im do ręki „kompromaty”¹⁰⁴ dotyczące jego osoby (w Moskwie utrzymywał rosyjską kochankę). Woluntaryzm, opisana przez kpt. W.T. Drymmera „sitwa”, niejasne kryteria awansów, które w sytuacji niskich wynagrodzeń kadry oficerskiej były jedynym sposobem na stabilizację finansową, oraz ignorowanie obiektywnych wymagań wobec osób zajmujących kierownicze stanowiska nie tylko dezorganizowały funkcjonowanie wywiadu, lecz także ułatwiały penetrację wywiadowczą. Panujące stosunki stwarzały napięcia interpersonalne i dzieliły oficerów na wybrańców o szybkich ścieżkach karier (jak np. kpt. W.T. Drymmer) oraz resztę, która pełniąc służbę informacyjną, była pomijana nie tylko w awansach na stanowiskach, lecz także w stopniach¹⁰⁵. Musiało się to negatywnie odbijać na postawach oficerów wobec przełożonych i pełnionej przez nich

¹⁰² Przy przesłuchaniu był obecny por. S. Łaniewski, który doskonale znał język rosyjski. Można więc przyjąć, że to on mógł przesłuchiwać, a ppłk L. Bociński i kpt. M. Talikowski tylko formułowali pytania. Istnieje jeszcze jedna możliwość, i to zdecydowanie najbardziej prawdopodobna, że przesłuchanie prowadzili Finowie, a nasi oficerowie tylko zgłaszali pytania. Finowie bowiem wierzyli E. Opperputowi i byli przekonani o pełnej infiltracji Oddziału II SG WP.

¹⁰³ Nie miał natomiast problemów w porozumiewaniu się z Finami, którzy biegłe posługiwali się językiem niemieckim.

¹⁰⁴ Skrót od „kompromietirujuszczij matieriał” – termin określający kompromitujące materiały na temat polityka lub innej osoby publicznej, za <https://pl.wikipedia.org/wiki/Kompromat> [dostęp: 5 II 2018] – przyp. red.

¹⁰⁵ Por. A. Wszendyrówny, *System doboru kadr do Oddziału II Sztabu Głównego Wojska Polskiego w latach 1929–1939*, „Rocznik Archiwalno-Historyczny Centralnego Archiwum Wojskowego” 2009, nr 2, s. 129.

służby, a także najprawdopodobniej miało wpływ na nabór. Młodzi oficerowie zdawali sobie sprawę, że w jednostkach liniowych mają większą szansę na bycie zauważonymi i docenionymi, niż w rządzonej niejasnymi zasadami służbie informacyjnej.

O problemach dotyczących poziomu odpowiedzialności za służbę oraz odwagi cywilnej kierownictwa Oddziału II świadczy działalność tzw. komisji Bociańskiego. Nie doprowadziła ona w 1927 r. do czystki w Referacie „Wschód”, co powinno być oczywiste w sytuacji tak głębokiej infiltracji sowieckiej. Pomimo cytowanych już wyżej wypowiedzi osób kierujących tym wywiadem, sugerujących, że zdawały sobie one sprawę z powagi sytuacji, nie dokonano chociażby wymiany kadrowej, przez co, jak należy przypuszczać, nie udało się przerwać opisanego przez rtm. A. Niedzińskiego „zazębień” się polskiego wywiadu z sowieckim kontrwywiadem. Oddział II, którego kadra, metody i formy pracy operacyjnej, instytucje przykrycia, a także mentalność zostały przez GPU dokładnie rozpoznane, w 1927 r. nie zrobił nic, aby tę sytuację zmienić. Jedynie ułatwił GPU zadanie, dobrowolnie dokonując samoograniczenia własnej aktywności.

Motywacje oficerów podejmujących wówczas decyzje były prawdopodobnie wynikiem ich emocji i przekonań – szlachetnych i zapewne dających się zrozumieć¹⁰⁶. Zarazem były wyjątkowo szkodliwe i w sytuacji zagrożenia tak naprawdę małostkowe. Gdyby komisja Bociańskiego zdecydowała się na czystkę wraz z jej ewentualnymi konsekwencjami – prawdopodobną kompromitacją Oddziału II – mogłaby choć częściowo zachować polski wywiad na ZSRR¹⁰⁷. Natomiast ostatecznie przekreśliłaby ich własne kariery.

Zakończenie

Podsumowując dotychczasowe rozważania, trzeba raz jeszcze podkreślić, że opisane przyczyny porażki Oddziału II SG WPw starciu z GPU miały charakter złożony i oddziaływały synergicznie, wzajemnie się wzmacniając. Syndrom grupowego myślenia, kłamstwo powodowane osobistym interesem skutkujące uruchomieniem procesów redukcji dysonansu poznawczego, były zarówno rezultatem, jak i przyczyną błędów systemowych polskiego wywiadu. Trzeba też podkreślić, że przyczyny wewnętrzne, które autor skrótowo przedstawił, jedynie ułatwiały działania czynników zewnętrznych. W sytuacji gdy Oddział II był obiektem nieustannego zainteresowania ze strony wschodniego sąsiada, niedopuszczalnym błędem było doprowadzenie do tego, aby wywiad stawał się ofiarą procesów psychospołecznych. Te zaś procesy skutecznie utrudniały funkcjonowanie wywiadu i umożliwiły agresywne działania Sowietów. Czynniki wewnętrzne były jak osłabienie organizmu, który zwykle pada ofiarą choroby, choć w zwykłych warunkach potrafi się przed nią bronić.

¹⁰⁶ Na tę decyzję wpłynęło prawdopodobnie wiele dodatkowych czynników (wcześniej podkreślane: niewielka liczebność kadr, pewność, że E. Opperputt kłamie, celowo obciążając oficerów, i wreszcie – brak choćby elementarnego rozpoznania sowieckiego modus operandi).

¹⁰⁷ Wkrótce prowadzenie wywiadu dokumentalnego na ZSRR i tak stało się praktycznie niemożliwe ze względu na specyficzne warunki.

Sztab Generalny¹⁰⁸ WP pomylił się co do przewidywanego terminu wybuchu II wojny światowej raptem o jeden rok. Od 1925 r. podstawą polskiej myśli strategicznej było założenie, że wojna na dwa fronty jest nieuchronna, a jedyną receptą jest sprawny wywiad oraz szybko manewrujące wojska o dużej sile ognia¹⁰⁹. Kierujący II RP postąpili wbrew jakże słusznym założeniom: armia była zapóźniona technologicznie, a przez to mało mobilna. Siedemnasty września 1939 r. był zaskoczeniem, gdyż rząd był przekonany, że ZSRR w najgorszym wypadku zachowa neutralność. Wywiad zaś – mający być podstawą sprawnej armii i polityki – ugrzązł w opisanych problemach, które skutecznie zablokowały mu możliwość działania na Wschodzie. Jak mawiał Stanisław Mackiewicz, dwudziestolecie międzywojenne było czasem przygotowywania się do następnej, nieuniknionej wojny. Niestety, podobnie jak wielokrotnie w dziejach Rzeczypospolitej, tego czasu nie zdołaliśmy dobrze wykorzystać.

Bibliografia:

1. Adorno T.W., *Osobowość autorytarna*, Warszawa 2010, Wydawnictwo Naukowe PWN.
2. Aronson E., *Człowiek – istota społeczna*, Warszawa 1987, Wydawnictwo Naukowe PWN.
3. Baczyńska A., *Historia dowodu osobistego w Polsce*, <http://wiadomosci.onet.pl/kraj/historia-dowodu-osobistego-w-polsce/sd95s> [dostęp: 6 XI 2015].
4. Bagley T.H., *Wojny szpiegów*, Poznań 2014, Zysk i S-ka.
5. Bailey G., *The Conspirators*, London 1961, b.w.
6. Ćwiąk H., *Rotmistrz Sosnkowski. As wywiadu Drugiej Rzeczypospolitej*, Kraków 2011, Wydawnictwo Literackie.
7. Danielewicz K., *Formy i metody pracy operacyjnej wywiadu polskiego w latach 1921–1939 na przykładzie Lwowskiej Ekspozytury nr 5 Oddziału II Sztabu Generalnego (Głównego)*, w: *Wywiad wojskowy II Rzeczypospolitej*, P. Kołakowski, A. Peplowski (red.), Kraków 2011, Avalon.
8. Domachowski W., Kowalik S., Miluska J., *Z zagadnień psychologii społecznej*, Warszawa 1984, Wydawnictwo Naukowe PWN.
9. Drymmer W.T., *Trust*, „Kultura” 1965, nr 2.
10. Drymmer W.T., *W służbie Polsce*, Warszawa–Kraków 2014, Wingert.

¹⁰⁸ Od 1928 r. – Sztab Główny (przyp. red.).

¹⁰⁹ Por. P. Stawecki, *Polityka wojskowa Polski 1921–1926*, Warszawa 1981, s. 82–93.

11. Ekman P., *Kłamstwo i jego wykrywanie w biznesie, polityce, małżeństwie*, Warszawa 1997, Wydawnictwo Naukowe PWN.
12. Graczyk K., *Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych*, Katowice 2015, niepublikowana praca magisterska, UŚl.
13. Kołakowski P., Krzak A., *Sprawa majora Jerzego Sosnowskiego w świetle dokumentów analitycznych Oddziału II SG WP i zeznań Franza Heinricha Pfeifera*, Warszawa 2015, Dematr.
14. Krzak A., „Czerwoni Azefowie”. *Afera „MOCR-TRUST” 1922–1927*, Warszawa 2010, Wojskowe Centrum Edukacji Obywatelskiej.
15. Kusiak F., *Życie codzienne oficerów Drugiej Rzeczypospolitej*, Warszawa 1992, PIW.
16. Mac J.S., *Przesłuchanie supergliny*, Warszawa 1990, FAKT.
17. Masterman J., *Brytyjski system podwójnych agentów 1939–1945*, Warszawa 1973, Wydawnictwo MON.
18. Michniewicz W., *Wielki bluff sowiecki*, Chicago 1991, WICI.
19. Opperput E., list do gazety „Siegodnia” opublikowany 17 V 1927 r.
20. Romeyko M., *Przed i po maju*, Warszawa 1985, Wydawnictwo MON.
21. Rybak J., *Pamiętniki generała Rybaka*, Warszawa 1954, Czytelnik.
22. Seljaninow P., *Narodnyj sojuz zaszczuty Rodiny i swobody. Wspominanija*, Berlin 1922, b.w.
23. Wojciechowski S., *Triest. Wspominanija*, London (Kanada) 1974, b.w.
24. Wszendyrówny A., *System doboru kadr do Oddziału II Sztabu Głównego Wojska Polskiego w latach 1929–1939*, „Rocznik Archiwalno-Historyczny Centralnego Archiwum Wojskowego” 2009, nr 2.

Abstrakt

W artykule omówiono przyczyny uwikłania się Oddziału II SG WP we współpracę z MOCR-Trustem – prowokacyjną organizacją kierowaną przez sowiecki kontrwywiad. Autor stawia tezę, że brakowało jednej, możliwej do wyabstrahowania przyczyny tego, a za wywiadowczą klęską stał z kolei konglomerat przyczyn działających synergicznie. Do przyczyn zewnętrznych wobec Oddziału II, autor zalicza uwarunkowania polityczne oraz działalność sowieckiej agentury w Wojsku Polskim. Przyczyny wewnętrzne – to przyczyny psychospołeczne, wynikające z procesów poznawczych

i ludzkich interakcji, oraz strukturalne, związane z funkcjonowaniem Oddziału II jako organizacji hierarchicznej. Omawiając i wyjaśniając tę drugą grupę przyczyn, autor sięgnął do dorobku psychologii społecznej i psychologii organizacji, które łączy z badaniami historycznymi.

Słowa kluczowe: Oddział II SG WP, operacja dezinformacyjna, Trust, OGPU, psychologia społeczna i poznawcza, psychologia organizacji, historia służb specjalnych, teoria dezinformacji.

III

RECENZJE

Krzysztof Izak

Charles Townshend, *Terroryzm*¹

W 2017 r. Wydawnictwo Uniwersytetu Łódzkiego rozpoczęło publikację serii „Krótkie Wprowadzenie”, na którą składają się (...) *książki zmieniające sposób myślenia*, jak informuje na okładce wydawca. Są to niewielkie rozmiarowo pozycje (21×13 cm), liczące od stu kilkudziesięciu do około dwustu stron tekstu. W ramach serii są prezentowane pozycje z różnych dziedzin wiedzy, a ich autorami są naukowcy z Oxfordu, którzy w sposób przystępny wprowadzają czytelnika w świat rozmaitych dyscyplin naukowych. Cykl *A Very Short Introduction (VSI)*, wydawany od 1995 r. przez Oxford University Press, liczy już ponad 500 tytułów, które cieszą się popularnością na całym świecie. Dotychczas przetłumaczono je na 25 języków. Teraz przyszedł czas na polskie tłumaczenie, chociaż już w drugiej połowie lat 90. XX w. i w 2000 r. Wydawnictwo Prószyński i S-ka podjęło się wydawania książek z tej serii. Ukazało się wówczas kilkanaście opracowań, które były poświęcone religioznawstwu i wybranym dziedzinom humanistyki.

Opiekę merytoryczną nad obecną polską edycją serii sprawują naukowcy z Uniwersytetu Łódzkiego. Szczególnie polecam piąty tomik napisany przez brytyjskiego historyka Charlesa Townshenda, zatytułowany *Terroryzm*. Profesor Charles Townshend jest specjalistą z dziedziny historii i politycznych następstw brytyjskiego imperializmu w Irlandii i na Bliskim Wschodzie, a więc na terenach, gdzie brytyjskiej obecności towarzyszyła duża aktywność organizacji, dla których terroryzm był metodą działań politycznych. Te organizacje pozostały aktywne również po opuszczeniu tych terenów przez Brytyjczyków. Przekładu publikacji na język polski dokonał Ryszard M. Machnikowski, znany politolog Uniwersytetu Łódzkiego, zajmujący się problematyką terroryzmu, współczesnych konfliktów zbrojnych i bezpieczeństwa międzynarodowego. On też zapatrzył książkę we wstęp pt. *Współczesne oblicza terroryzmu*.

Przed omówieniem zawartości tej wartościowej publikacji warto zacytować słowa tłumacza:

Townshend obala na kartach swej książki szereg niepotrzebnych, a wciąż potykających w świadomości, i to nie tylko laików, mitów na temat terroryzmu. Są one często, co należy z przykrością stwierdzić, rozpowszechniane przez licznych komentatorów przesiadujących w studiach telewizyjnych. Jego praca pozwala przyjrzeć się zjawisku niejako „od podszewki”, mimo iż pierwsze wydanie znalazło się na półkach księgarskich w 2002 r., a czytelnik wersji polskiej ma do czynienia z wydaniem drugim, poprawionym i uzupełnionym, które ujrzało światło dzienne w 2011 r., a więc ponad 5 lat temu (s. 9–10).

¹ Łódź 2017, Wydawnictwo Uniwersytetu Łódzkiego, 202 s.

Książka składa się z siedmiu rozdziałów poświęconych różnym zagadnieniom związanym z terroryzmem, z których każdy jest opatrzony mottem lub sentencją autorstwa wybitnych osób znanych z historii lub obecnie żyjących.

W rozdziale pierwszym – *Problem z terroryzmem* – autor porusza takie kwestie, jak: spory o definicję terroryzmu, terroryzm a wojna, powstanie i przebieg tego zjawiska, strategie terroru, terror i polityka, kobiety a terroryzm. Zauważa, że terroryzm jest odrębną formą działalności politycznej, która ma na celu podważenie zdolności państwa do zapewnienia bezpieczeństwa swoim obywatelom, stąd wynika uzasadnienie takich działań. Istnieje ponad 200 definicji terroryzmu. W latach 80. XX w. dwóch badaczy, Alex Schmid i Albert Jongman, porównało ponad 100 istniejących wówczas określeń terroryzmu pod kątem występowania w nich tzw. słów kluczowych². Najczęstszymi wyrazami były: siła i przemoc (ponad 83 proc.), polityczny charakter (65 proc.) i strach (51 proc.). Co ciekawe, zaledwie w pięciu procentach definicji znajdowały się takie pojęcia, jak: nieobliczalność i nieprzewidywalność, które powszechnie występują w objaśnieniach sformułowanych w ostatnich dwóch dekadach. Zameł pojęciowy dotyczący terroryzmu jest obecny zarówno w mediach, jak i w literaturze naukowej. Dotyczy nie tylko definicji, lecz także kwestii językowych. Co dla jednych jest terroryzmem, dla innych jest walką o wyzwolenie narodowe, czego przykładem jest konflikt palestyńsko-izraelski, w którym świat arabski, czy szerzej – muzułmański, traktuje organizacje palestyńskie nie jak terrorystów, lecz jak bojowników o wolność.

Terroryzm jest fenomenem politycznym, a nie psychologicznym. Słowa: t e r r o r y z m, t e r r o r y ś c i jednoznacznie wzbudzają negatywne skojarzenia, podczas gdy ci, którzy stosują terroryzm, kwestionują zasadność takiego rozumienia tego terminu. Sami siebie nazywają b o j o w n i k a m i, r e b e l i a n t a m i lub p a r t y z a n t a m i. To ostatnie pojęcie również wprowadza chaos, walka partyzancka bowiem kieruje się logiką militarną. Partyzanci angażują siły zbrojne państwa, niezależnie od skali swoich działań. Ich celem są przede wszystkim siły zbrojne przeciwnika. Procesem definiującym partyzantkę jest zatem wojna. Warto w tym miejscu zacytować Henry'ego Kissingera, sekretarza stanu USA w latach 1973–1977, który stwierdził przed laty: *Partyzantka wygrywa, jeśli nie przegrywa, regularna armia przegrywa, jeśli nie wygrywa*. To zdanie najlepiej oddaje różnicę między partyzantką a regularnym wojskiem własnego lub obcego państwa, z którym partyzanci znajdują się w konflikcie.

Istotą terroryzmu jest zaprzeczenie walki rozumianej jako pojęcie wojskowe. Jego celem są osoby niewalczące, często bezbronne, cywile. W przypadku terroryzmu mamy zatem do czynienia z walką podejmowaną przez słabych, którzy stosują przemoc, ze względu bowiem na swoją słabość nie mogą podjąć otwartej walki. Może dochodzić do eskalacji działań i wówczas taką ich formę nazywa się często w o j n ą a s y m e t r y c z n ą, prowadzoną przez strony dysponujące nierównymi siłami. Właśnie ta asymetryczność jest czynnikiem odróżniającym terroryzm od w o j e n

² A.P. Schmid, A. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concept, Data Bases, Theories and Literature*, New Brunswick 1988, s. 5–6.

symetrycznych, tj. takich, które są starciem w miarę równych sił. Termin wojny asymetryczne, który miał pomóc w zdefiniowaniu terroryzmu i rozwianiu wątpliwości, doprowadził jednak do dalszego zamieszania. Jest on nadużywany, ponieważ nie każdy konflikt asymetryczny jest tożsamy ze zjawiskiem terroryzmu. Ch. Townshend w swoich rozważaniach pominął koncepcję wojny asymetrycznej. Zabrakło również porównania terroryzmu z południowoamerykańskimi *guerillas*, którą to nazwą określano partyzantki walczące z reżimami autorytarnymi, a nie organizacje terrorystyczne.

Wprowadzając czytelnika w zagadnienie strategii terroryzmu, autor opisuje to zjawisko w ujęciu historycznym, choć wymyka się ono chronologii i zaciemnia przekaz. Nie można się też zgodzić z autorem, który, odnosząc się do logiki terroryzmu, stwierdza, że: *Została ona po raz pierwszy jasno i wyraźnie przedstawiona w „Filozofii Bomby” Jonathana* (poprawnie imię powinno brzmieć „Johann”, a nie „Jonathan” – dop. aut.) *Mosta, traktacie anarchistycznym z 1880 r.* (s. 33). To Michaił Bakunin, uznawany za twórcę anarchizmu, którego apologetą był niemiecki anarchista Most, stworzył ideę stosowania przemocy. Bakunin był autorem hasła: „Przyjemność niszczenia jest uczuciem twórczym” oraz „Podstawą działania anarchistów jest realizowanie rewolucyjnej ideologii w nierewolucyjnej sytuacji”. Jego rodak i kolega Siergiej Nieczajew był autorem słynnego *Katechizmu rewolucjonisty*, ideologicznego traktatu stanowiącego fundament działalności rewolucyjnej, którą dziś określa się mianem *terroryzmu anarchistycznego*. Trzeci z rosyjskich ideologów anarchizmu, Piotr Kropotkin, głosił m.in. że umiarkowanie nie przystoi przemocy.

Nie można też zapominać o innych XIX-wiecznych niemieckich prekursorach i teoretykach terroryzmu. Jeden z nich, Wilhelm Weitling, określił terroryzm jako połączenie rewolucyjnej świadomości i kryminalnych umiejętności, czyli: terrorysta = rewolucjonista + kryminalista³. Z kolei Karl Heinezn w opracowanej doktrynie terroryzmu uzasadniał potrzebę dokonywania masowych morderstw w imię słusznej sprawy⁴.

W rozdziale drugim – *Krzyżowcy i konspiratorzy* – Ch. Townshend porusza kilka interesujących zagadnień, wydawałoby się – odległych od siebie. Stara się odróżnić „dobrych terrorystów” od „złych terrorystów”. Określenie *dobry terrorysta* odnosi się do XIX-wiecznych terrorystów-rewolucjonistów walczących z opresyjnymi państwami. W przypadku bojowników o wolność autor stara się podać cechy odróżniające ich od terrorystów. Najważniejszą jest to, że niezwykle rzadko przeprowadzają oni ataki terrorystyczne, aby osiągnąć cele polityczne. Z historycznego punktu widzenia żadnej organizacji, która odwoływała się jedynie do terroryzmu, nie udało się dokonać dzieła wyzwolenia. Terroryzm sam w sobie jest zjawiskiem negatywnym i jego stosowanie wywołuje często niespodziewane dla terrorystów katastrofalne skutki. Przykładem tego mogą być działania „dobrych terrorystów” lat 70. XX w. członków do

³ Z tą definicją kojarzy się inna, sformułowana przez indyjskiego teologa muzułmańskiego, filozofa i poetę Muhammada Ikbala (1877–1938), dla którego bolszewizm + Bóg = prawie islam.

⁴ Osoby zainteresowane terroryzmem anarchistycznym odsyłam do książek: A. Pawłowski, *Terroryzm w Europie XIX i XX wieku*, Zielona Góra 1980 oraz W. Potkański, *Terroryzm na usługach grupowań lewicowych i anarchistycznych w Królestwie Polskim do 1914 roku*, Warszawa 2014.

organizacji Movimiento de Liberación Nacional-Tupamaros, MLN-T (Ruch Wyzwolenia Narodowego Tupamaros), które spowodowały zmierzch liberalnego Urugwaju. Mimo możliwości zaistnienia nieprzewidywalnych zdarzeń słuszną jest w wielu wypadkach teza Frantza Fanona (1925–1961) – uczestnika wojny narodowo-wyzwoleńczej w Algierii, podczas której obie strony konfliktu stosowały terror wobec przeciwnika i tzw. zdrajców unikających walki, sprzeciwiających się stosowaniu przemocy lub wspierających stronę przeciwną – że przemoc wyzwala uciśnionych z kompleksu niższości, desperacji i niemocy, czyni nieustraszoną i przywraca poczucie własnej wartości.

Przechodząc do omawiania terroryzmu międzynarodowego, autor książki nie definiuje tego zjawiska, stwierdza natomiast, że pojawiło się ono wraz z karierą Carlosa (s. 49). Ale podpis pod fotografią zamieszczoną na stronie 46 informuje: *Idea terroryzmu międzynarodowego narodziła się wraz z zamachem w Haymarket w Chicago 4 maja 1886 r., gdy policja rozpraszająca zebranie anarchistów (wielu z nich było niedawnymi emigrantami z Niemiec), została zaatakowana bombą. Z pewnością obecność niemieckich imigrantów w zdarzeniu nie może skłaniać do określenia tego zdarzenia mianem terroryzmu międzynarodowego, któremu nowy wymiar nadał Ilicz Ramirez Sanchez alias Carlos, czyli słynny Szkał. Wielu autorów za początek terroryzmu międzynarodowego uznaje porwanie samolotu izraelskich linii lotniczych El Al, lecącego z Rzymu do Tel Awiwu. Do tego zdarzenia doszło 23 lipca 1968 r., a porywaczami byli członkowie Ludowego Frontu Wyzwolenia Palestyny. Samolot został uprowadzony do Algieru. Warto w tym miejscu przytoczyć definicję terroryzmu międzynarodowego, sformułowaną w 1986 r. przez Komisję Prawa Międzynarodowego ONZ. *Terroryzm międzynarodowy to (...) podejmowanie, pomaganie i zachęcanie przez władze państwa do aktów terrorystycznych w innym państwie albo tolerowanie przez te władze działalności organizowanej w celu przeprowadzenia aktów terrorystycznych w innym państwie.* W okresie zimnej wojny organizacje terrorystyczne były wspierane przez różne kraje, w tym ZSRR i USA. Wydaje się jednak, że obecnie podział na terroryzm wewnętrzny i międzynarodowy traci sens ze względu na sieci powiązań – może poza USA, gdzie działają różne ugrupowania niemające żadnych istotnych powiązań międzynarodowych.*

Starając się odpowiedzieć na pytanie: czy w przyszłości terroryzm może być jeszcze gorszy?, autor książki wyraża opinię, że takie ryzyko będzie rosło w miarę rozwoju możliwości technologicznych terrorystów. W przeszłości stosowali oni już broń chemiczną i mogą uzyskać komponenty do jej produkcji. Jednak superterroryzm w postaci broni masowego rażenia, zwłaszcza nuklearnej, który wywołuje strach opinii publicznej, to raczej wymysł dziennikarzy niż realne zagrożenie. Niemniej jednak jej użycie przez niektóre państwa wydaje się możliwe.

W rozdziale trzecim – *Rządy terroru* – autor wprowadza czytelnika w interesującą problematykę siania strachu we Francji w okresie Wielkiej Rewolucji. W 1793 r. jakobini wprowadzili rządy terroru, aby obronić rewolucję przed arystokracją i rojalistami, choć większość ofiar stanowili zwykli ludzie. Krwawe stłumienie powstania w Wandei, które stało się dla jakobinów symbolem kontrrewolucji, i eksterminacja ludności cywilnej jest tego najlepszym przykładem. Niedługo później rewolucja francuska

„pożarła” własne dzieci. Na gilotynę posłano członków Konwentu: Maksymiliana Robespierre’a, Ludwika Saint Justa oraz Grzegorza Dantona. Okrucieństwo i użycie przemocy na masową skalę w czasie Rewolucji Francuskiej stworzyło model stosowania terroru zarówno przez tych, którzy chcieli utrzymać stary porządek (tzw. biały terror), jak i tych, którzy chcieli go obalić. W ten sposób ukształtował się „czerwony terror” (np. bolszewicki) i „czarny terror” (nacjonalistyczny, np. hitlerowski). Należy zatem rozróżnić pojęcia „terror” od „terroryzmu”. Terror to używanie przemocy silniejszych organów państwa wobec słabszych obywateli, natomiast terroryzm to stosowanie przemocy słabszych obywateli wobec silniejszych organów państwa, niekoniecznie tego samego pochodzenia terrorystów.

Ch. Townshend wyróżnia terroryzm swobodnego zasięgu, do którego zalicza działalność latynoamerykańskich szwadronów śmierci, wspierających kontrterrorystyczne działania organów państwa. Wymienia także ultraterrotyzm, który występuje (...) w sytuacji gdy niegdyś znacząca grupa postrzega się jako porzucona i zdradzona przez państwo. To poczucie zdrady pojawia się, gdy ludność lokalna staje w obliczu negocjacji między rebeliantami a państwem, tak jak to się zdarzyło we francuskiej Algierii pod koniec kampanii narodowyzwolenczej prowadzonej przez FLN (Front de Libération Nationale, Front Wyzwolenia Narodowego – dop. aut.), a w nieco mniejszym stopniu w Irlandii Północnej podczas „procesu pokojowego” (s. 72). Pod koniec walk prowadzonych z algierskim FLN aktywna była l’Organisation Armée Secrète, OAS (Organizacja Tajnej Armii), ugrupowanie, które powstało w marcu 1961 r. i było przeciwne niepodległości Algierii. Celem jego działań stała się miejscowa ludność. Stosując taktykę spalonej ziemi, OAS chciała wywołać rebelię francuskich osadników, czego nie udało się jej osiągnąć. Działania terrorystyczne przeniosła także do Francji, przygotowując m.in. kilka nieudanych zamachów na prezydenta Charles’a de Gaulle’a. W przypadku Irlandii Północnej organizacje lojalistyczne, np. Ulster Volunteer Force, UVF (Ochotnicze Siły Ulsteru), nie atakowały przedstawicieli brytyjskiego rządu czy celów brytyjskich, koncentrowały się natomiast na celach irlandzko-republikańskich (katolickich). Ich działalność została nazwana terroryzmem ochotniczym. Gdyby Ch. Townshend napisał swoją książkę po 2011 r., to tym mianem z pewnością nazwałby wiele ugrupowań powstałych w wyniku wydarzeń arabskiej wiosny.

Rozdział czwarty – *Terroryzm rewolucyjny* – został podzielony na cztery podrozdziały. Dwa pierwsze, zatytułowane: *Dwa wieki terroryzmu: wiek I* oraz *Dwa wieki terroryzmu: wiek II*, przedstawiają zjawisko terroryzmu w ujęciu historycznym, począwszy od rosyjskich anarchistów, zwanych terrorystami-rewolucjonistami. Należeli do nich m.in. członkowie organizacji Narodna Wola (Wola Ludu), zwani też narodnikami, którzy chcieli sprowokować wybuch rewolucji, aby obalić istniejący porządek i zbudować na jego miejscu społeczeństwo bezpaństwowe. Anarchiści określali swoją działalność mianem „propagandy poprzez czyny”. Można tu znaleźć również polski akcent: *Polski socjalista Józef Piłsudski nazywał takie działania „czynem zbrojnym”, a syndykaliści „akcją bezpośrednią” czy też reprise individuelle (indywidualnym*

odwetem)⁵ (s. 79). Jako cel ataków terroryści-rewolucjoniści wybierali głowy państw i wysokich urzędników. W latach 1881–1914 przeprowadzono skuteczne zamachy na siedmiu władców (w tym m.in. na cara Rosji, prezydentów USA i Francji, króla Włoch i austrowęgierskiego następcę tronu). Przy okazji omawiania terroryzmu rewolucyjnego można dodać dwa polskie akcenty. Pierwszy to zabójca cara Aleksandra II, którym był pochodzący z Podlasia polski student Ignacy Hryniewiecki. Zmarł on w wyniku ran odniesionych podczas eksplozji bomby rzuconej 13 marca 1881 r. pod nogi imperatora. Odciętą głowę Hryniewieckiego umieszczono w słoju ze spirytusem i wystawiono ku przestrodze innym w holu komendy policji w Petersburgu. Drugi akcent jest związany z Bronisławem Piłsudskim, starszym bratem Józefa, który brał udział w nieudanym spisku na życie cara Aleksandra III w 1887 r. Za ten czyn został zesłany na Sahalin. Tam prowadził badania Ajnów zamieszkujących południe wyspy, a potem badania etnograficzne innych ludów Japonii⁶.

Zdaniem autora omawianej książki terroryzm rewolucyjny odpowiada za odrodzenie się przemocy politycznej po drugiej wojnie światowej, gdy rodził się antykolonialny ruch narodowo-wyzwoleńczy. Terroryzm był istotnym jego elementem. Przykładem są organizacje Wiet Min i Wietkong, które są odpowiedzialne za śmierć ponad 20 tys. ludzi. Istotną rolę w terroryzmie rewolucyjnym odegrał czynnik latynoamerykański (taki jest też tytuł kolejnego podrozdziału). Trwałe miejsce zajęli w nim Ernesto Guevara „Che”, Abraham Guillen, który napisał *Strategię miejskiej partyzantki* (1966 r.), Regis Debray, autor traktatu *Rewolucja w Rewolucji* (1967 r.), i Carlos Marighella – *Minipodręcznik miejskiego partyzanta* (1969 r.). W przypadku Ameryki Łacińskiej źródłem terroryzmu rewolucyjnego były masowe ruchy społeczne prowadzące działalność partyzancką (*guerilla*). Ta aktywność została przeniesiona do miast, tworząc miejską partyzantkę (*guerilla urbana*). Najlepiej znana organizacja partyzancka działała w Urugwaju – w najwyższym stopniu demokratycznym państwie Ameryki Łacińskiej. Był to wspomniany już ruch Tupamaros. Ostatecznym rezultatem jego działalności było powstanie mniej liberalnego i sprawiedliwego państwa, co z kolei zmusiło członków Tupamaros do zejścia do podziemia i finansowania działalności ze środków uzyskiwanych z napadów rabunkowych na banki.

Partyzanci Tupamaros byli wzorem dla młodzieży zachodnioniemieckiej. Przyczyn tego szczególnego zainteresowania należy szukać w warunkach, w jakich walczyli urugwajscy bojownicy. Nie bez znaczenia były również sukcesy odnoszone przez *guerillas* w drugiej połowie lat 60. XX w., a więc w okresie działania w RFN młodzieżowej opozycji pozaparlamentarnej. Zwycięstwa Tupamaros okazały się mieć charakter doraźny i w końcowym rezultacie obróciły się nie tylko przeciw samej organizacji, lecz także przeciw demokracji urugwajskiej. Niemniej jednak latynoamerykańska

⁵ Od 1904 r. Józef Piłsudski kierował frakcją Organizacji Bojowej Polskiej Partii Socjalistycznej (OB PPS), która prowadziła ataki na rosyjskie cele na terenie Królestwa Polskiego. Szczegółowo na ten temat pisze W. Lada w książce *Polscy terroryści*, Kraków 2014.

⁶ W październiku 2013 r. odsłonięto pomnik Bronisława Piłsudskiego w Shiraoui na Hokkaido. W Jokohamie mieszka jego wnuk Kuzuyasu Kimura.

partyzantka była natchnieniem do działania dla wielu skrajnie lewicowych organizacji terrorystycznych w Europie. O tych organizacjach jest mowa w ostatnim podrozdziale – *Terroryzm frakcji*. Czytelnik znajdzie w nim krótkie opisy działalności włoskich Brigade Rosse, BR (Czerwonych Brygad) czy niemieckiej grupy Baader-Meinhof, czyli Rote Armee Fraction, RAF (Frakcji Czerwonej Armii). Ostatecznie lewacy terroryści w Europie zostali pokonani przez organy państwowe.

Inną motywacją grup terrorystycznych jest ideologia nacjonalistyczno-separatystyczna. O nich jest mowa w kolejnym, piątym, rozdziale – *Nacjonalizm i terror*. Ruchy nacjonalistyczne wykazywały się znacznie większą odpornością na działania kontrterrorystyczne i własną destrukcję. Autor wymienia działania lankijskiej Liberation Tigers of Tamil Elam, LTTE (Tygrysów Wyzwolenia Tamińskiego Ilamu) i armeńskich organizacji nacjonalistycznych, będących spadkobiercami XIX-wiecznego ruchu dasznaków⁷. Osobne podrozdziały autor poświęcił Irish Republican Army, IRA (Irlandzkiej Armii Republikańskiej), baskijskiej Euskadi ta Askatasuna, ETA (Krajowi Basków i Wolność) oraz syjonizmowi jako ideologii i polityce terroru, które przybliżyły Żydów do powstania suwerennego państwa Izrael. IRA i ETA, wykorzystując doświadczenia ruchów antykolonialnych i latynoskich, doceniały znaczenie mediów. Zdawały sobie sprawę, że bez relacji telewizyjnych, radiowych i artykułów prasowych nie uda im się osiągnąć zamierzonego celu. Gdyby ich aktywność miała miejsce współcześnie, niewątpliwie wykorzystywałyby do tego celu media społecznościowe. Cyberprzestrzeń stanowiłaby najszerze pole kontaktu z opinią publiczną.

W latach 70. i 80. XX w. w wielu regionach Europy powstawały separatystyczne ugrupowania terrorystyczne. Ich celem było uzyskanie autonomii dla jakiegoś regionu lub też oderwanie go od państwa. Wszystkie te grupy odwoływały się do ideologii lewicowych oraz podkreślały niechęć wobec Zachodu, szczególnie USA. Działalność terrorystyczna wielu ówczesnych grup była też rezultatem pojawienia się pewnego rodzaju politycznej mody naśladowania przemocy stosowanej przez istniejące już organizacje separatystyczne, których aktywność ograniczała się w zasadzie do przeprowadzenia jednego lub kilku zamachów. Należały do nich ugrupowania działające w należącej do Włoch Górnej Adydze, w Bretanii, na Korsyce, Wyspach Kanaryjskich, Molukach czy w szwajcarskim masywie Jury.

Porównując aktywność grup terrorystycznych motywowanych różną ideologią, okazuje się, że terroryzm stosowany przez organizacje o charakterze nacjonalistycznym może w niektórych przypadkach doprowadzić do osiągnięcia sukcesu. Wymusza on bowiem zawarcie porozumienia politycznego przez strony konfliktu. Między

⁷ Nazwa wywodzi się od miejscowości Dasznakcutiun. Pochodząca z niej grupa uzbrojonych członków Armeńskiego Sojuszu Rewolucyjnego opanowała w 1896 r. Bank Osmanski w Stambule. Terroryści złożyli ultimatum na ręce ambasadorów państw zachodnich w Turcji. Domagali się w nim międzynarodowej interwencji w Imperium Osmańskim w celu przywrócenia spokoju w tym kraju, a tym samym „przerwania zbrodniczej obojętności ludzkości”. W przeciwnym razie grozili wysadzeniem budynku banku wraz z jego personelem i aktywami finansowymi. Wśród innych operacji dasznaków były dwa zamachy na życie sułtana Abdulhamida II – nieudane, podobnie jak atak na bank w Stambule.

innymi aktywność izraelskiego Irgunu (Irgun Cwai Leumi, Ecel) w latach 40. XX w. zmusiła Brytyjczyków do wycofania się z Palestyny. To samo udało się Cypryjczykom z organizacji Ethniki Organosis Kiprijon Agoniston, EOKA (Narodowej Organizacji Bojowników Cypryjskich). Francuzi zostali zmuszeni przez FLN do opuszczenia Algierii, Wielka Brytania i IRA podpisały w 1998 r. tzw. porozumienie wielkopiątkowe, którego rezultatem było przeproszenie przez IRA za cywilne ofiary swej działalności i rozpoczęcie likwidacji swoich arsenałów. Nastąpił okres pokoju, który jednak nie trwał długo. Po podpisaniu porozumienia powstała nowa frakcja IRA o nazwie Real IRA, RIRA (Prawdziwa IRA), która w marcu 2009 r. przeprowadziła atak na brytyjską bazę wojskową w Massereene, w hrabstwie Antrim (24 km na północ od Belfastu). Zginęło w nim dwóch żołnierzy, a kilku innych zostało rannych. Później dochodziło do kolejnych zamachów. Okazało się, że rozpoczętą przed wielu laty kampanię terroryzmu niezwykle trudno jest zatrzymać.

Walka w obronie religii i wiary jest zadaniem wspólnoty, nie ma innego obowiązku, poza samą wiarą, ważniejszego niż walka przeciwko wrogowi, który niszczy nasz styl życia i naszą religię. Te słowa, zaczerpnięte z *Kitab al-Iman (Księgi wiary)* Takiego ad-Dina ibn Tajmijji (1263–1328), są mottem otwierającym rozdział szósty – *Terror religijny*. Ch. Townshend stwierdza, że ostatnia dekada XX wieku przyniosła przełom w postrzeganiu terroryzmu motywowanego religijnie. Zwrócono wówczas uwagę na działalność islamskich organizacji fundamentalistycznych stosujących przemoc. Dla nich terroryzm jest sposobem walki o wprowadzenie postulowanych zmian społecznych i zaprowadzenie panowania Allaha nad światem, czyli globalnej hegemonii islamu. Muzułmańscy radykałowie stosują przemoc wobec niewiernych i tych współwyznawców, którzy nie podzielają ich jedynie słusznych poglądów. Ci są uznawani za zdrajców.

Przemoc towarzyszyła religii od starożytności, choć w tamtych czasach najazdy obcych ludów czy wrogich cywilizacji nie były motywowane religijnie. Burzono świątynie, a posągi bogów niszczone lub wywożone jako łup wojenny, religie pogańskie bowiem miały zdolność włączania do swojego panteonu bóstw podbitych ludów. Dopiero religie monoteistyczne porzuciły tę tradycję, ostro zwalczając pogaństwo oraz idolatrię (bałwochwalstwo). Zmiany w podejściu ludzi różnych wyznań do przemocy na przestrzeni dziejów zostały doskonale przedstawione w książce pt. *Pola krwi*, do której przeczytania również zachęcam⁸. Na stronie 126 *Terroryzmu* Ch. Townshend przytacza pogląd Bruce'a Hoffmana, który (...) *wskazywał na to, że żadnej z jedenastu najbardziej znanych grup terrorystycznych, które działały w 1968 r., nie da się zakwalifikować jako „religijnej”*. Według niego (...) *pierwsza współczesna grupa o takim charakterze pojawiła się około 1980 r.* Nie można się jednak zgodzić z taką opinią, ponieważ w 1968 r. w USA została założona przez rabina Meira Davida Kahanego organizacja Jewish Defense League, JDL (Żydowska Liga Obrony), łącząca żydowską ortodoksję i rasistowskie przekonania o wyższości Żydów nad innymi nacjami. Rabin Kahane postrzegał siebie jako religijnego przewodnika narodu żydowskiego, któremu wskazywał

⁸ K. Armstrong, *Pola krwi. Religia i przemoc*, Warszawa 2017.

najlepszą drogę do zbawienia. Tą drogą miało być ściśle podporządkowanie się prawom boskim. Od momentu powstania do 1976 r. JDL przeprowadzała w USA zamachy (w tym na polski konsulat w Nowym Jorku), w których zginęło siedem osób, a 22 zostały ranne. Żydowska „czystość rasy” była jednym z głównych punktów programu rabina i jego zwolenników. Ich ugrupowanie nazwano „Kach”, co z języka hebrajskiego tłumaczy się: „Tylko w ten sposób”. Było to określenie odnoszące się do realizacji idei rabina, w jaki sposób powinno się postępować z Palestyńczykami, doprowadzając do oczyszczenia Ziemi Izraela (*Erec Izrael*) z nieżydowskich mieszkańców⁹. Należy też dodać, że po wojnie sześciodniowej w 1967 r., gdy Izraelczycy zdobyli wschodnią Jerozolimę, w Izraelu zaczęły szybko dochodzić do głosu różne skrajne organizacje religijne wywodzące się z ruchu haredim (bogobożnych).

W latach 60. XX w. w Indiach powstała najbardziej radykalna organizacja fundamentalistyczna wyznawców hinduizmu Sziv Sena (Armia Sziwy), która nie stroniła od przemocy. W tym samym czasie rozwijała się religijno-nacjonalistyczna koncepcja hindutwy (hinduskości), która święciła triumfy w latach 80. ubiegłego wieku. Od 1920 r. w Indiach była aktywna sikhijska organizacja Shiromani Akali Dal, SAD (Armia Czcieli Ponadczasowego), która wyznawców hinduizmu i islamu uznawała za wrogów. Dlatego też trudno zgodzić się z tezą, że w 1968 r. nie istniała jeszcze żadna organizacja terrorystyczna o charakterze religijnym. W tym czasie w Egipcie działał w podziemiu ruch Al-Ichwan al-Muslimin (Braci Muzułmanów), którego członkowie znaleźli schronienie w Arabii Saudyjskiej.

Polskiemu wydaniu należy przypisać błędnie sformułowane zdanie: *Najdłuższy rozdział pt. „Inside Terrorism” w znanej pracy Bruce’a Hoffmana „Rand Corporation”, szefa grupy studyjnej badań nad terroryzmem, jest właśnie poświęcony religii* (s. 126). Rand Corporation jest amerykańskim neokonserwatywnym think tankiem, z którym Hoffman jest związany, *Inside Terrorism* to tytuł książki jego autorstwa, jej najdłuższym zaś rozdziałem, liczącym 50 stron, jest *Religion and Terrorism*¹⁰.

Tytułem *Religia a przemoc* – podobnym do tytułu książki B. Hoffmana – został opatrzony jeden z podrozdziałów rozdziału szóstego. Ch. Townshend polemizuje w nim z Hoffmanem oraz innymi autorami, dla których terroryzm religijny ma wybitnie transcendentálny, a nie polityczny charakter. Rzeczywiście, nie można zgodzić się z taką tezą, ponieważ organizacjom terrorystycznym motywowanym religią przyświecają w gruncie rzeczy cele polityczne. Odwoływanie się do okresu starożytności (zeloci) czy średniowiecza (asasyni) również nie ma większego sensu, ponieważ organizacje religijne tamtych czasów kierowały się m.in. celami o charakterze politycznym (walka z rzymskim panowaniem na terenie Palestyny w przypadku zelotów oraz Sułtanatem Seldżuckim i krzyżowcami w przypadku asasynów).

⁹ A. Krawczyk, *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej połowie XX wieku*, Toruń 2007, s. 154–203.

¹⁰ B. Hoffman, *Inside Terrorism*, New York 2006. Zdanie poprawnie mogłoby brzmieć: „Najdłuższy rozdział pt. „Religion and Terrorism” w znanej pracy „Inside Terrorism” autorstwa Bruce’a Hoffmana, szefa grupy studyjnej badań nad terroryzmem w Rand Corporation, jest poświęcony właśnie religii”.

W kolejnych podrozdziałach autor krótko charakteryzuje implikacje obecności religii w polityce, porusza problematykę mesjanizmu i milenaryzmu, terroryzmu samobójczego oraz fundamentalizmu. Szkoda, że w części poświęconej temu ostatniemu zagadnieniu autor koncentruje się wyłącznie na islamskim fundamentalizmie, w paru słowach tylko odnosząc się do fundamentalizmu w judaizmie i do sekty Aum Shinrikyo (Najwyższa Prawda).

Fundamentalizm, jak już wspomniano, jest obecny we wszystkich religiach monoteistycznych oraz w hinduizmie i buddyzmie. Pojęcie to powstało w Stanach Zjednoczonych na przełomie wieków XIX i XX. Pod tą nazwą kryły się radykalne kierunki protestanckie, które wychodziły ze swoją ideologią poza ogólny nurt protestantyzmu. Za prekursora amerykańskiego fundamentalizmu uważa się Dwighta L. Moody'ego (1837–1899), założyciela Moody Bible Institute w Chicago (1886 r.), mającego przygotować kadry do walki o wiarę. Najważniejszym celem, który postawił sobie Moody, było zbawienie ludzkich dusz. Dlatego był on gotów do współpracy z każdym chrześcijaninem. Troszczył się również o reformy społeczne. Absolwenci jego instytutu mieli zostać misjonarzami biedaków. Uważał, że bezbożne ideologie doprowadzą do zniszczenia świata. Według niego sytuacja na świecie z dnia na dzień ulegała pogorszeniu, dlatego należało zwrócić się do Boga. W 1910 r. presbiterianie¹¹ z Princeton sformułowali naukę o nieomyślności *Pisma Świętego*¹² i ogłosili listę pięciu podstawowych dogmatów: 1) nieomyślność *Biblii*, 2) narodziny Jezusa z Dziewicy, 3) całkowita realność czynionych przez niego cudów, 4) odpokutowanie przez Chrystusa ludzkich grzechów na krzyżu, 5) cielesne zmartwychwstanie Chrystusa. W latach 1910–1915 bracia Lyman i Milton Stewartowie, naftowi milionerzy z Kalifornii, sfinansowali wydanie serii broszur (12) pod tytułem *The Fundamentals. The Testimony of the Truth*, w których zawarto ok. 90 artykułów. Ich autorzy, czołowi konserwatywni protestanci teologowie, w sposób dostępny tłumaczyli zasady wiary. Każda z 12 broszur została opublikowana w nakładzie blisko 3 mln egzemplarzy, które bezpłatnie przesyłano pastorom, kaznodziejom, dyrektorom szkółek niedzielnych, profesorom i studentom teologii w USA. Ten projekt miał symboliczne znaczenie, ponieważ został uznany za oficjalny początek ruchu fundamentalistycznego¹³.

W ostatnim rozdziale recenzowanej książki autor przedstawia możliwe reakcje państwa na zagrożenie terrorystyczne, cytując pytanie, które zadał Walter Laqueur¹⁴: *Czy demokratyczne społeczeństwo może zdławić terrorystyczną przemoc bez poświęcenia wartości kluczowych dla tego systemu?* (s. 147). Odpowiadając na nie, autor uważa,

¹¹ Presbiterianie, oprócz kwaków, metodystów, baptystów i innych, są zaliczani do wyznań dysenterskich, czyli odłamów protestantyzmu, które nie należą do kościoła anglikańskiego.

¹² Zasada „sola Scriptura” („tylko Księga”) głosi, że *Biblia* jest Księgą pierwszą i ostateczną, jedynie pewną i nieomylną. Z tą zasadą jest związany tzw. skrypturalizm biblijny odrzucający wszelkie dogmaty i poglądy niepoparte autorytetem *Biblii*.

¹³ K. Armstrong, *W imię Boga. Fundamentalizm w judaizmie, chrześcijaństwie i islamie*. Warszawa 2005, s. 249.

¹⁴ Amerykański historyk i publicysta, autor książek poświęconych m.in. problematyce terroryzmu oraz publikacji *Ostatnie dni Europy. Epitafium dla Starego Kontynentu*, Wrocław 2008.

że ofiarą terrorystów staje się nie tyle sama demokracja, której struktury nie uległy zasadniczej zmianie, ile jej liberalne wartości. Do czynników wpływających na słabość demokracji w obliczu zagrożenia terrorystycznego zalicza: swobodę poruszania się, zrzeszania, wielość potencjalnych celów ataku, ograniczenia wynikające z przyjętego systemu prawnego chroniącego prawa człowieka, wysoką wartość, jaką nadaje się ludzkiemu życiu, oraz wolność mediów. Warto w tym miejscu przytoczyć słowa wypowiedziane przez terrorystów w 2015 r.: *Wasze prawa człowieka są naszą bronią* oraz: *My kochamy śmierć tak, jak wy kochacie życie*. Zachodnie społeczeństwa zgodziły się na ograniczenie wolności obywatelskich w imię zapewnienia poczucia bezpieczeństwa. Jednak wraz z rozszerzaniem uprawnień instytucji państwowych odpowiedzialnych za bezpieczeństwo nie doszło do jego poprawy. Od zamachów z 11 września 2001 r. świat wcale nie jest bezpieczniejszy, a wprost przeciwnie – coraz bardziej zagraża mu terroryzm.

Ch. Townshend stwierdza, że najważniejszą metodą reakcji na „czysty” terroryzm, wykorzystywaną w istniejącym konflikcie, a nie jedną z taktyk wojennych, jest jego zignorowanie, ponieważ ryzyko śmierci w wyniku ataku terrorystycznego jest znacznie mniejsze niż w wypadku drogowym. Najlepszą publiczną odpowiedzią na terroryzm powinno być nieokazywanie strachu. Niestety, reakcje państw są często nieadekwatne do zagrożenia. Najlepszym tego przykładem było ogłoszenie przez USA w 2001 r. globalnej wojny z terroryzmem oraz atak USA i trzech jego sojuszników na Irak przeprowadzony 20 marca 2003 r. Jego konsekwencją była śmierć tysięcy ludzi i powstanie nowego demona terroryzmu w postaci Państwa Islamskiego. Również niewspółmierny do zagrożenia był atak USA na Afganistan, który zamiast doprowadzić do likwidacji Al-Kaidy, wywołał w świecie muzułmańskim antyzachodnią psychozę. Trwająca do tej pory obecność sił NATO w Afganistanie i tak nie doprowadziła do unormowania sytuacji w kraju, a talibowie sprawują kontrolę nad znaczną częścią terytorium. Dlatego reakcja na zagrożenie terrorystyczne powinna być proporcjonalna do jego skali. Prawdopodobnie najgorszą reakcją na terroryzm jest naśladowanie samych terrorystów. Takie działania od lat stosują służby specjalne Izraela, które w skrytobójczych zamachach starają się eliminować najgroźniejszych terrorystów, a armia niszczy domy rodzin zamachowców. Według premiera Izraela Benjamina Netanyahu odwet nie tylko zapobiega terroryzmowi, ale jest wręcz w stanie go pokonać. Zdarza się również, że same władze państwowe manipulują strachem wywołanym rzeczywistym lub urojonym zagrożeniem terrorystycznym, czego przykładem była polityka Stanów Zjednoczonych w okresie pomiędzy atakami z 11 września 2001 r. a wkroczeniem wojsk do Iraku w 2003 r. Obowiązujący wówczas *Patriot Act* miał szerokie poparcie społeczne, zgodnie z tezą Ronalda Crelinstena: *Większość ludzi poświęci swoją wolność w zamian za bezpieczeństwo, jeśli tylko będzie wystarczająco wystraszona* (s. 177).

Ch. Townshend wskazuje też na różnice między „antyterroryzmem” i „kontrterroryzmem”. Antyterroryzm wiąże się ze stosowaniem działań defensywnych polegających na rozpoznaniu zagrożeń terrorystycznych i im zapobieganiu, a więc dotyczy wszystkich przedsięwzięć prewencyjnych. Z kolei kontrterroryzm

obejmuje sferę ofensywnego zwalczania terroryzmu, a więc angażowanie sił zbrojnych i służb bezpieczeństwa państwa do likwidacji organizacji terrorystycznych i eliminowania poszczególnych jej członków. W praktyce oba terminy bywają dziś używane zamiennie, a niektórzy autorzy stosują pojęcie *anty/kontr/terroryzm*. Każde państwo zagrożone zjawiskiem terroryzmu ma własną strategię jego zwalczania. Temu celowi służą m.in. jednostki specjalne. Strategia UE jest oparta na: zapobieganiu (np. deradykalizacji, odcięciu od środków finansowych oraz od zaplecza logistycznego), ochronie (osób, mienia oraz infrastruktury), ściganiu (prowadzeniu śledztw, procesach sądowych) i reagowaniu (neutralizowaniu i minimalizowaniu skutków ataku terrorystycznego). Wszystkie te działania są prowadzone przy uwzględnieniu praw człowieka.

Operacje antyterrorystyczne państwa powinny być lepiej skalkulowane i bardziej precyzyjne niż akcje terrorystów. Podstawą walki z terroryzmem powinny być: strategia wyprzedzania, czyli działanie prewencyjne polegające na uderzeniu w komórki terrorystyczne zanim dokonają one zamachu, oraz strategia proporcjonalnego odwetu po przeprowadzeniu ataku terrorystycznego, któremu nie udało się zapobiec. Do skutecznego wdrażania strategii wyprzedzania niezbędne są odpowiednie środki i źródła operacyjne. Obie strategie perfekcyjnie realizują izraelskie służby specjalne.

Autor odniósł się też do drażliwych spraw międzynarodowych, które długo nie pozwalały zdefiniować pojęcia *akt terroryzmu*. W końcu udało się pokonać rozbieżności, ale unikając samego terminu *terroryzm*, dla ominięcia spornego problemu motywacji politycznej. Neutralna terminologia użyta w konwencji nie spełniła jednak swojego zadania, trudno bowiem jest określić, co jest aktem terroryzmu, pomijając ideologię, przynależność etniczną czy religijną jego sprawców i sympatyków. Na to nakłada się również sponsorowanie terrorystów przez państwa. Jest to przedmiotem stanowczej krytyki USA, które po ataku z 11 września 2001 r. do „państw bandyckich” zaliczyły Irak, Iran i Koreę Północną. Na liście państw wspomagających finansowo terroryzm znalazły się także Sudan, Syria i Libia. W okresie zimnej wojny sponsorowanie, wspieranie, a nawet szkolenie terrorystów zarzucano ZSRR.

Dodatkowym walorem książki Ch. Townshenda są fotografie oraz wykazy literatury powiązanej z poszczególnymi słowami kluczowymi, oddzielnie dla każdego rozdziału, a także bibliografia załącznikowa wybranych zagadnień związanych z terroryzmem. Na końcu umieszczono indeks zawierający nazwiska, nazwy organizacji, nazwy geograficzne i najważniejsze słowa kluczowe. Na podkreślenie zasługuje komunikatywny styl i narracja publikacji, które sprawiają, że czyta się ją z dużym zainteresowaniem i zrozumieniem. Jest to lektura, którą polecam szczególnie funkcjonariuszom rozpoczynającym służbę w pionach zwalczania terroryzmu. Krótkie wprowadzenie w zagadnienie problematyki, którą przyjdzie im się zajmować, z pewnością będzie nieocenionym wkładem poszerzającym ich wiedzę. Warto zatem poświęcić jeden weekend na przeczytanie recenzowanej książki, przy czym zostanie jeszcze czas na własną nad nią refleksję.

Marek Świerczek

**Konrad Paduszek, *Zajrzeć do mózgu Lenina.*
*Wywiad II Rzeczypospolitej a postrewolucyjna Rosja*¹**

W nocy 17 września 1939 r. wiceminister spraw zagranicznych ZSRR Władimir Potiomkin przekazał ambasadorowi Rzeczypospolitej Polskiej w Moskwie Wacławowi Grzybowskiemu notę podpisaną przez Wiaczesława Mołotowa, która zawierała m.in. takie oto zdanie:

Wojna polsko-niemiecka ujawniła wewnętrzne bankructwo państwa polskiego. W ciągu dziesięciu dni operacji wojennych Polska utraciła wszystkie swoje regiony przemysłowe i ośrodki kulturalne. Warszawa przestała istnieć jako stolica Polski. Rząd polski rozpadł się i nie przejawia żadnych oznak życia. Oznacza to, iż państwo polskie i jego rząd faktycznie przestały istnieć. Wskutek tego traktaty zawarte między ZSRR a Polską utraciły swą moc².

Niemal równocześnie jednostki Armii Czerwonej przekroczyły wschodnie granice RP i rozpoczęły zdradziecką agresję, nazwaną – zgodnie z sowiecką praktyką przeniecanego świata – „wyzwolielskim pochodem”. Polska po dwudziestu latach niepodległości przestała istnieć. Wehrmacht spotkał się z Armią Czerwoną, aby świętować przymierze broni na trupie Rzeczypospolitej.

Jednak historycy w opisie tego złowieszczonego wydarzenia robią błąd, sądząc, że sowiecka napaść rozpoczęła się od wręczenia noty o trzeciej w nocy niczego nierozumiejącemu ambasadorowi Grzybowskiemu. Ta pomyłka czasowa wynosi – bagatela! – niemal osiemnaście lat. Podstępne wbicie Polsce sowieckiego „szytyka” w plecy było bowiem konsekwencją procesu, który zaczął się banalnie – od wizyty polskiego renegata, Wiktora Steckiwicka, w Rewlu na pierwszy śnieg 1921 r. To wtedy polski wywiad został wciągnięty w nieprawdopodobnie rozgałęzioną grę dezinformacyjną prowadzoną przez sowiecki kontrwywiad, który dzięki temu do kwietnia 1927 r. ogłupiał Sztab Główny Wojska Polskiego. Hurtowo podsuwał mu dokumenty produkowane przez fałszerzy pracujących w międzyresortowym Biurze Dezinformacji, zwanym dowcipnie „krywym zwierkiem”. Nastąpił wówczas niemal całkowity rozkład polskiego aparatu wywiadowczego. Polscy oficerowie zamiast z agenturą spotykali się z sowieckimi prowokatorami, zamiast tajnych dokumentów dostarczali do Warszawy makulaturę zawierającą kłamstwa albo półprawdy. Co gorsza, będąc stale pod kontrolą operacyjną przeciwnika, stanowili dla niego łatwy cel werbunkowy. Wpadali w ręce Sowietów, próbując dorobić na czarnym rynku do skąpych oficerskich pensji,

¹ Łomianki 2016, LTW, 608 s.

² *Zmowa. IV rozbiór Polski*, A.L. Szcześniak (wstęp i oprac.), Warszawa 1990, s. 135.

oraz przez dziecięcą łatwowierność byłych kawalerzystów, których centrala wysyłała do ZSRR niemal bez przeszkolenia w celu błyskawicznej penetracji tamtejszych najwyższych urzędów państwowych i Armii Czerwonej. Żeby tym naprędce wysłanym w paszczę niedźwiedzia dwudziestoparoletnim szpiegom nie przewróciło się w głowach, armijni decydenci ograniczali budżet i doprowadzali do tego, że polskiemu wywiadowi brakowało pieniędzy, a oficerowie musieli płacić z własnej kieszeni nawet za korzystanie z samochodu polskiego Poselstwa.

Gdy Sowietom w końcu zdruziała się ta maskarada i ujawnili za pośrednictwem kolejnego prowokatora, że sieci agenturalne polskiego wywiadu na Wschodzie są de facto na żołdzie sowieckiego OGPU, kierownictwo Oddziału II, po okresie udawania, że nic się nie stało, nagle zareagowało z historyczną przesadą..., trwale rezygnując z werbunku informatorów w ZSRR. Tym sposobem, jak argumentowały najwyższe szarże polskiej szpiegokracji, miano uniknąć kolejnych pułapek sowieckich Azefów i skupić się jedynie na tym, co namacalne i realnie istniejące, w miejsce możliwych do sfalszowania dokumentów i raportów od agentów. Tyle, że Rosjanie sprawnie ograniczyli polskim oficerom możliwość poruszania się po ZSRR i w ten sposób skutecznie sparaliżowali polski wywiad. W wyniku tego Rzeczpospolita została oślepią.

Pomimo ogromnego wysiłku całego państwa polskiego, które przeznaczało (w zależności od metodologii wyliczeń) od ok. 23,5 proc. do 42 proc. budżetu na utrzymanie ogromnej armii złożonej z 30 dywizji piechoty i 10 brygad kawalerii, Polska na Wschodzie była bezbronna i niezdolna do przewidzenia, kiedy i w jaki sposób zostanie przeprowadzony atak. Mimo że już od 1925 r. Biuro Ścisłej Rady Wojennej słusznie zakładało, że polska obrona musi się opierać na sprawnym wywiadzie, to Rzeczpospolita – przynajmniej na Wschodzie – w praktyce nie miała go w ogóle.

Tylko brakiem elementarnych zdolności do rozpoznania intencji przeciwników (i sojuszników) można wytłumaczyć uwikłanie się przez RP w wojnę z Niemcami w sytuacji, gdy był podpisany traktat Ribbentrop–Mołotow. Polski wywiad nie potrafił wychwycić nawet absolutnie jednoznacznych symptomów katastrofy zbliżającej się ze wschodu.

Już w 1938 r. ambasador Francji w Moskwie Robert Coulondre uzyskał informacje, z których wynikało, że wiceminister spraw zagranicznych ZSRR Władimir Potiomkin lansuje tezę o nieuchronności IV rozbioru RP. Polski wywiad nie podniósł tej kwestii, podobnie jak i uzgodnień między sztabami głównymi Francji i Anglii z kwietnia 1939 r., z których wynikało, że sojusznicy będą czekali na ostateczne rozstrzygnięcie wojny polsko-niemieckiej, rezygnując z udzielenia pomocy w trakcie bitwy granicznej. A potem, gdy niemiecka machina wojenna zaczęła już Polskę miażdżyć, polski wywiad nie był w stanie dostrzec podniesienia stanu gotowości bojowej przez Armię Czerwoną i koncentracji sowieckich jednostek na całej granicy z RP. Nawet usunięcie zasieków granicznych przez Sowietów nie wzbudziło niepokoju ani w Oddziale II SG WP, ani w KOP. To sprawiło, że Wojsko Polskie na Kresach dało się Sowietom zaskoczyć i trafiło – niemal bez oporu – do obozów jenieckich, a ostatecznie do egzekucyjnych dołów Katynia.

Praca doktorska Konrada Paduszka opublikowana pod rynkowym tytułem *Zajrzeć do mózgu Lenina* pomaga w zrozumieniu, jak do opisanych powyżej wydarzeń doszło. Jej autor dokonuje tu drobiazgowego podsumowania dotyczącego działalności polskiego wywiadu na Wschód w najważniejszym z punktu widzenia późniejszych wydarzeń okresie: 1921–1927. Choć tym tematem od lat zajmują się uznani polscy historycy, to jednak brakowało dotąd tak szczegółowej monografii opartej na dokumentach źródłowych, która dawałaby precyzyjny obraz działania Oddziału II na Wschodzie i ułatwiała zrozumienie przyczyn, które doprowadziły do tej sytuacji.

Autor omawia po kolei działanie sieci wywiadowczych w ZSRR (zarówno w kraju, jak i za granicą), odnosi się do kadry oficerskiej aktywnej na kierunku sowieckim, omawia źródła informacji wykorzystywane przez polski wywiad na Wschodzie, współpracę Oddziału II z innymi służbami wywiadowczymi działającymi przeciwko ZSRR i wreszcie rezultaty działalności rozpoznawczej w ZSRR. Każdy z rozdziałów jest sumą aktualnej wiedzy na omawiany temat i repetycją dotychczasowych badań, uzupełnioną o rezultat dodatkowej starannej kwerendy archiwalnej.

K. Paduszek niezwykle obficie cytuje archiwalia i rysuje panoramę polskiego wywiadu na Wschodzie, pomimo rozległości zagadnienia. Utrzymuje przy tym drobiazgową narrację, opartą na zweryfikowanych faktach. Opis jest uzupełniony o zestawienia tabelaryczne, w których autor umieścił wyniki wieloletnich, szczegółowych kwerend. Bogactwo zaprezentowanej wiedzy świadczy o pracowitości autora, który przeanalizował tysiące dokumentów i stworzył rozległe kompendium faktograficzne oparte na klarownych założeniach porządkujących. Publikacja K. Paduszka pozwala na dalsze analizy i stawianie nowych hipotez. Dzięki temu stanowi nie tyle syntezę, ile prolegomenę do dalszych badań. Dodajmy, że z uwagi na swoją drobiazgowość i kompletność jest to publikacja, która powinna się znaleźć w podręcznej bibliotece każdego badacza wywiadu okresu dwudziestolecia międzywojennego. Przy czym, mimo objętości równej objętości książki telefonicznej, można ją z zaciekawieniem czytać w sposób tradycyjny, ale można też sięgać jedynie do wybranych rozdziałów i posiłkować się nimi w pracy badawczej.

Choć autor, tworząc swoje kompendium, nie przejawiał pasji demaskatorskiej i nie stawiał sobie za cel odbrażowienia pamięci o oficerach Oddziału II, to jednak zgromadzone przez niego i uporządkowane informacje są jednoznaczne w swojej wymowie. Wynika z nich, że Druga Rzeczpospolita nie rozumiała, z czym tak naprawdę ma na Wschodzie do czynienia. Mimo że w gazetach i za pomocą propagandy Rosję Sowiecką, zwaną Sowdepką, demonizowano, to jednocześnie kompletnie nie zdawano sobie sprawy z potęgi jej służb i nowatorstwa w zakresie prowadzenia przez nią tajnej wojny. Decydenci, którzy wysyłali polskich oficerów do Moskwy czy Mińska, żyli w świecie urojeń i nie przyjmowali do wiadomości, że nieliczny, źle opłacany i niedysponujący know how dostosowanym do absolutnie unikatowych rozwiązań stosowanych przez sowieckie służby Oddział II musiał tę walkę przegrać. Polscy oficerowie potrafili dawać swoim agentom instrukcje, w których radzili im, aby będąc w ZSRR, zupełnie otwarcie podchodzili do byłych towarzyszy pułkowych z carskiej armii, gdyż

ci z pewnością zachowali oficerską cześć i *esprit de corps*. Polscy wywiadowcy honorem ręczyli za swoich sowieckich agentów, którzy – ich zdaniem – byli tak honorowi i tak nienawidzili Sowietów, że przecież... nie mogli kłamać. Jeden z szefów Oddziału II pisemnie nakazał swoim oficerom, aby zweryfikowali, czy osoba podejrzewana o bycie konfidentem OGPU w Moskwie faktycznie nim jest, przez... zwrócenie się do niej z takim pytaniem. Pan pułkownik widocznie wyobrażał sobie, że człowiek spytany wprost nie będzie miał innego wyjścia, jak tylko powiedzieć prawdę, albo przynajmniej splełni się czy zacznie nerwowo przecierać okulary i w końcu drżącym głosem się pożegna, pozostawiając oficera winszującego sobie własnej przenikliwości. Polski korpus oficerski, mentalnie tkwiący w wyobrażeniach XIX-wiecznych, nie pojmował, że w „sowieckim raju”, pełnym masowych grobów, obozów koncentracyjnych i katowni tajnej policji, wszystkie ludzkie odruchy zamarły i że osoby, których rodziny mogły być w dowolnej chwili zgładzone, zrobią wszystko, czego zażąda operator z OGPU.

Dzięki publikacji Konrada Paduszka można zrozumieć, jak doszło do kłęski wrześniowej i późniejszego zniewolenia kraju przez sowieckich namiestników o polskobrzmiących nazwiskach. Jak napisał w krótkim omówieniu tej publikacji prof. Sławomir Cenckiewicz: *Józef Piłsudski miał kiedyś powiedzieć, że w prowadzonej przez Polskę grze z bolszewikami chodzi o to, by zajrzeć do mózgu Lenina. Niestety, plan Marszałka Polski (...) nie został zrealizowany.*

I właśnie w tym zawiera się wartość monografii Konrada Paduszka: zamiast mowy pochwalnej dostaliśmy staranny opis plusów i minusów przedwojennego polskiego wywiadu. A dzięki temu możemy wyciągać wnioski. Nie tylko w odniesieniu do przeszłości.

IV
ARTICLES
AND DISSERTATIONS

Andrzej Krzak

Wars of the future in Russian – hybrid, sociological and psychological war in view of the Ukrainian conflict

Introduction

After the end of the Cold War we have been observing rapid changes in tactics and the way conflicts and wars are waged. Increasing mutual interaction and combining of regular and irregular wars techniques have become noticeable. Current military conflicts, both regional and that on wider scale, are characterized by complexity of application and practical use of all available means of fight. Already preliminary analyses indicate mutual dependencies between individual phases of the plan realization and political and military goals of the enemy set on a tactical, operational and strategic level. Although, the complexity mentioned, should be understood in much wider sense. It would be better to use the term *hybridization* of the new battlefield. Nevertheless, the phenomenon is nothing new as the way of waging wars and it does not only come down to carrying operations in a military sense, but also to other numerous actions of information, political and economic nature. This does also not include only security forces of the attacked country but most of all it affects wide sections of society, national, ethnic and religious groups. The diversity of elements being a part of destruction activities has become a very popular topic of political and journalistic conversations and has nowadays become defined as *hybrid activities* or *hybrid war*.¹

There is no doubt that changes to international environment after the Cold War caused new challenges for the whole world when it comes to international security area in a very broad sense. There was no threat of a global conflict between the then two superpowers and blocks of states. The threat of nuclear destruction has also gone, which still, to a large extent, was present in security thinking in the early 1980s. New problems in the international security area have come to the fore.

Just after the communist bloc had collapsed it seemed that the main security threats in the coming years would be conflicts of ethnic, national and religious nature. Further crises turning into long-term wars in the former Soviet Union and Yugoslavia seemed to confirm that. „Thawing” of conflicts was also pointed out as they started to emerge because of geopolitical changes in different parts of the world. Some states happened to be in a new political reality faced also new problems (increasing contradictions) that they could not handle well. Previous system, which had concentrated around two superpowers maintaining the balance of forces, collapsed, and there was only one

¹ A. Dębczak, C. Pawlak, J. Keplin, *Analityczny model oceny hybrydowości współczesnych konfliktów*, „Zeszyty Naukowe AON” 2015, No 2, p. 45.

player left, who, as it seemed, facing no dangerous adversary, would impose its own democratic system successfully. Nevertheless, the situation after the Cold War has very quickly verified the hopes: it turned out that both international organizations as well as the biggest superpower cannot deal with numerous and rapid changes. Conflicts and wars from the beginning of 1990s caused necessity of thinking reevaluation and the way security in a broader sense had been perceived up to that moment. The situation got even more complicated after globalization processes had started.² It appeared that doctrines, strategies and old cold-war armies were things of the past. The way the role of a state and armed forces in the new reality was perceived, changed.

In these circumstances new theoretical trends of a new world vision based primarily on a unipolar domination of the USA. They focused on maintaining, supervision and widening areas of democracy, free market and western way of life. The pattern of an American way of living³ and, what comes next – also the way democracy was perceived, became a main determinant of the superpower politics in the end of the 20th century, and at the beginning of the next century. Successive administrations did not intend to change their politics nor the foreign policy which had been worked out after the Cold War ending. This politics was directed to enhance advantage gained after bipolar world had collapsed. This way it became unacceptable to let Russia rebuild its military and political position it had as the USSR, which could threaten the position of the USA. Normalization of internal situation after Yeltsin times and program of the first presidency of Putin raised concerns in the USA. Especially that the new Kremlin host specified his program very clearly: he acknowledged that burying the cold-war world and the USSR was the greatest catastrophe for Russians ever – to paraphrase it. American politicians, although looked at Putin's activities with fear, in reality did not believe that Russia could threaten the USA. Apart from that they started to be more and more preoccupied with growing terrorism phenomenon and fighting Islam. Also numerous dictators, particularly from Arab countries, started to pose a serious threat to American politics in the early 21st century, especially in view of the Al Qaeda offensive. Military operations by the USA to prevent global terror spreading, not only stopped the threat but, on the contrary, have speeded up consolidation of radical organizations and led to creation one terrorist centre. It occurred very soon that methods and ways of combating the new enemy through military and technology prevalence were not effective and completely useless.

In the described time there was a belief that military politics of the USA would still be defined through the lens of the Revolution in Military Affairs, RMA⁴ which was

² В.Н. Горбунов, С.А. Богданов, *О характере вооружённой борьбы в XXI веке*, „Военная мысль” 2009, No 3, pp. 2–3.

³ M.A. Piotrowski, *Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych*, „Sprawy Międzynarodowe” 2015, No 2, p. 8.

⁴ See: J. Blaker, *Understanding the RMA: A Guide to America's 21 Century Defense Military Affairs*, Washington 1997; E.C. Sloan, *The Revolution in Military Affairs: Implications for Canada and NATO*, Montreal 2002.

supposed to maintain technological, information and military prevalence. This idea, promoted from the late 1990s, referred to making use of new information technologies, leadership, intelligence⁵, munitions together with concepts of tactical operations, operational and strategic activities that make it possible to conduct immediate joint operations by all services, and ability to strike in each and every place of the battlefield any time of the day and night in any field and atmospheric conditions.⁶

If one conduct more complete and thorough examinations, it would turn out the RMA concept was not invented by Americans. Its roots should be looked for in the USSR between the 1970s and 1980s. Among some Soviet commanders and military theoreticians there was a very interesting and innovative of the time concept of military-technical revolution, worked out and the then Chief of the General Staff of the Soviet Union Armed Forces, marshal Nikolai Ogarkov claimed that effectiveness of conducting hostilities in the future would be determined by high-tech and non-nuclear technologies.⁷

Russian Chief of General Staff ideas had not influenced the then Russian warfare theory. Despite huge leap forward in civilization and scientific and technical progress fuelling creation of new weapon systems in the 20th century, military theoreticians were not able to establish the nature of future wars. Russian warfare theory and practice stopped on the previous generation wars as evidenced in Russian Warfare Doctrine of 1999.⁸

Due to an advanced technological development, technological and information revolution, it was a new technical and scientific base created to set new trends for the future wars and highly advanced technologies and information systems were to be its foundations. An extremely important role played: microelectronics, optoelectronics, sensor technology, new production technologies and technologies of high-grade materials application.⁹ Through these achievements there were created new advanced weapon and equipment systems which shall be capable of changing completely the nature of the fight and the war as such.¹⁰ But apart from the modern technologies, as it was to appear soon, also primitive models of struggle combining modern technologies with old weapon systems can be a killer app.

Whereas, totally different was the process of studying conflicts and war in the West. Reality and challenges enforced changes application in new tactics and doctrine of waging war in a new changed political and military environment. Some military professionals claimed that both RMA and other techniques of fighting in view of new challenges and treats do not meet the expectations and new solutions should be found.

⁵ M. Lekowski, *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*, „Bezpieczeństwo Narodowe” 2011, No 19, p. 267.

⁶ R.O. Hundley, *Past revolutions, future transformations. What can the history of revolution in military affairs tell us about transforming the US military?*, Washington 2009, pp. 9–10.

⁷ M. Wickers, R. Martinage, *The revolution in War*, Washington 2004, pp. 8–9.

⁸ И. Капитанец, *Битва за мировой океан*, Москва 2002, pp. 50–51.

⁹ В.Н. Горбунов, С.А. Богданов, *О характере вооружённой борьбы...*, p. 5.

¹⁰ И. Капитанец, *Битва за...*, pp. 50–51.

It was also agreed that political and military situation would generate new conflicts and could not be solved by the then methods and forms of combat action. Beliefs that diplomacy during crisis situations, were criticized. It was thought that peaceful conflict solving can be effective only in some strictly defined situations. Nevertheless, all previous events lead to a conclusion that the basic reason for future conflicts will be collapse of state structures, growing frustration and lack of prospects not only for a single country, but also for the whole regions as well as for the US domination. These beliefs seemed to be confirmed by conflicts in Afghanistan and Iraq, where American administration involvement was particularly strong.

What used to seem simple and resulted from a vast political, economy and military prevalence of the USA, occurred to be more complicated than politicians, planners, military men and intelligence experts thought. The USA was involved in a long-term conflict which seems to have no end. No changes in tactics and military philosophy in new weapon systems application have brought expected results, particularly to gain such prevalence which would allow turning the tide in favor of Americans.

In the light of experience in the late 20th, early 21st centuries there has been created a theory of asymmetric threats and wars, and the so called complex wars and 4 generation wars (4GW). To describe the last type shortly it should be pointed out that it refers to such actions that lead to weakening of the adversary by methods totally different to those applied by the opponent party.¹¹ Therefore, in strategic and operational spheres we will come across such phenomena as losing a state monopoly of waging wars, return to the world of cultures and states of war, domestic division of society (ethnic, religious, according to groups of interest), looking for the main goal of psychological strike (will of fight, public opinion) and disproportion between investments and results. In tactics area, it will result in moving strength from the adversary's line to his home front and using the adversary's potential against him.¹²

Professor Jacek Reginia-Zacharski stresses that in wars of that kind the role of a non-state factor grows having significant resources and using wars to make more money at the same time. Moreover, in such kind of wars terrorist organizations, organized crime groups and transnational corporations¹³ take part. So in a way, 4GW war can be defined as a hybrid war, if you take under consideration the assumptions of the theory. The world has changed so much that it made main international actors change their way of waging wars. One is for sure, strategies, tactics, combat actions with mass army's presence, known from the more or less distant past, are the past at the moment. It seems that new concepts and ways of waging wars seeking are justified by the growing discrepancies between RMA ideas and security policy practice in many countries, including foremost the USA. It had to lead in the end to a criticism

¹¹ H. Królikowski, *Siły operacji specjalnych (Wojska Specjalne) w konfliktach hybrydowych*, „Bezpieczeństwo. Teoria i Praktyka” 2016, No 3, p. 24.

¹² Ibidem.

¹³ See: J. Reginia-Zacharski, *Wojna w świecie współczesnym. Uczestnicy, cele, modele, teorie*, Łódź 2014, pp. 294–304.

of the security paradigm which was based on an elementary significance of using technologies in defense systems of individual countries and models of carrying modern combat actions. Basic charge being raised for a few years is that it is impossible to find such solution which would shift the deadlock on the current art of war. Deadlock, which is the effect of growing complexity of current (and most probably future) wars and conflicts and methods of their waging and resolving. It should be noticed that this deadlock current war actors face is the basic feature of the 21st century wars, in which no technological prevalence, nor psychological, nor command and organizational prevalence is (and most probably will be) decisive in gaining an ultimate success.¹⁴ It is not known, though, whether in few months' time or even years, there would be a necessity to base military potential on mass armies and whether manuals of huge operations with the use of groups of arms and fronts get back into favor. It should not be forgotten, therefore, that apart from irregular wars, guerilla wars, non-linear wars, complex wars and special operations practice there are still classical views on organization and the way wars should be waged.

Hybridity of current conflicts and wars in view of Russian and Western military thoughts

The concept of hybrid wars is nothing new in the history of wars and military thought and nowadays it should be understood in a much wider sense not only as the way of waging wars.¹⁵ It seems to be another America-centric depiction of current wars and an attempt to resolve „the American power dilemma” and to get the answer to a question why the USA were not able to use its position of a worldwide hegemony and resolve the confrontation with much weaker opponents in American favor.¹⁶ The American helplessness is a result of numerous complex phenomena happening in the current security area. *Imperial hubris* and *hegemonic presumption* are only some of the reasons of the American failure over the last twenty years. Moreover, there is

¹⁴ A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapala (ed.), Warszawa 2011, p. 9.

¹⁵ Numerous proposals of doctrine regarding the formation of hybridity theory in current wars seem to be another stage of seeking universal method of effective warfare on each and every level of army and institutions of military security in a broader sense. Western theoreticians, checking different variants of the struggle for Western (American) model of democracy do not take under consideration many vital practical and military factors. As if they forgot about such things like very fast changes in the battlefield, necessity of improvisation, leaving command initiative (especially on a tactical level) or regarded them as unnecessary. Creating strict doctrinal norms seems to be quite an interesting measure but it is risky as well, especially that in a couple of months somebody figures out or propose another “hybrid”. Combining different forms of fighting since the dawn the dawn of time has been a practiced way of waging wars. Politicians and military professionals, especially the second ones, have been delighted many times by a new concept of winning a war, being under pressure to finish a long-lasting conflict. Nevertheless, mostly the result came not because of new fighting techniques application but in skilful combination of numerous elements, both military and non-military.

¹⁶ N. Freier, *The defense identity crisis: It's a hybrid world*, „Parameters” 2009, No 3, p. 82.

a lack of one strategy and effective tactical techniques to achieve success. This is why there are so many concepts and war theories, which, instead of solving doubts, in fact create even bigger chaos, both in scientific as well as in practical sense. Undoubtedly, looking for a universal model of new forms of military actions in an environment, where there is no state-like opponent, made it necessary to find an effective antidote to helplessness of the biggest and the one superpower. Despite numerous studies and continuous search, unfortunately there has no solution been found, which would give military success and guarantee that the war ends. On the contrary, present wars or future conflicts will be long-term processes and technological, economic or military prevalence will not guarantee aims achievement of goals or that strategic or political interests¹⁷ will be achieved.

Etymology of the hybridity term leads to Latin *hybrida* which means something of mixed origin or composition, the offspring produced by breeding plants or animals of different varieties, species, or races.¹⁸ *Hybridity* can also be defined as

(...) quality resulting from the crossing or mixing features, elements of different, quite often structurally different and genetically distant, opposing subjects, organisms or states. So, hybridity means consolidation of opposing features into one separate being, while maintaining specific features of the species which decide about primacy of this new hybrid organism, as regards - for example - disease resistance, strength, or better adaptation abilities.¹⁹

Hybrid war term has been introduced into science by Frank G. Hoffman²⁰, a retired marine's lieutenant colonel. He claimed that this phenomenon is (...) „*a physical and psychological, kinetic and non-kinetic convergence of (...) militants and civilians (...) armed forces and societies, states and non-state actors as well as of their combat action*”.²¹ Nevertheless, hybrid wars term was used in scientific discussions in the 1990s *inter alia* thanks to Thomas R. Mockaitis²², historian of the DePaul

¹⁷ A. Gruszcak, *Hybrydowość współczesnych wojen...*, p. 10.

¹⁸ *Słownik wyrazów obcych PWN*, J. Tokarski (ed.), Warszawa 1980, p. 290.

¹⁹ A. Gruszcak, *Hybrydowość współczesnych wojen...*, p. 11.

²⁰ Hybrid activities and hybrid war are the terms used also in 2002 in the work of major William J. Nemeth *Future war and Chechnya. A case for hybrid warfare*. However, they were limited to the assessment of the Chechen society and some forms of operations carried out by Chechen rebels. This is a reason why it is difficult to acknowledge that vocabulary apparatus proposed by Nemeth gives a full complexity of hybridity phenomenon as a new form of military struggle, because it does not take account of the whole complexity of this phenomenon and is rather a clumsy attempt to analyze Chechen versus Russian conflict. Nevertheless, as very valuable should be acknowledged the assessment of possibilities of Russian army of that time and completely useless in new battlefield realities of that time. See: Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, No 14, p. 40, special edition.

²¹ F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, No 52, p. 34.

²² Mockaitis also stressed a hybrid nature of British expedition forces, which were supported by a diplomatic component and political actions. See T.R. Mockaitis, *British Counterinsurgency in*

University of Chicago and the American Strategic Studies Institute. This American historian, during his research into colonial wars by the UK, noticed that apart from classic conventional fighting there were anti-partisan, terrorist actions with the use of combined forms of combat operations carried out at that time as well.²³

In 1998 the term came up in some works on the history of Marine Corps. Commander Robert Walker described units of the Corps as hybrid²⁴ and operations carried out by them as hybrid actions. Also some other Western experts tried to formulate a new research paradigm towards changes in current military conflicts. Colonel Daniel T. Lasica, for example, considered „hybridity” as a combination of strategy and tactics, combining different forms of military activities.²⁵ Colonel John J. McCuen proposed to assume that hybrid war is nothing more than a connection between components of a symmetric and asymmetric war.²⁶ The proposed hybrid war term brings it to armed struggle within the ongoing conflict or the proxy war, i.e. formula of different ways of armed struggle depending on the place and adversaries.

It is worth noting that in literature of the subject in Russia the term hybrid war had not been used or at least very rarely until 2014. It showed up only in the context of deliberations on American and their allies’ military forces acting in Afghanistan and Iraq to give a picture of a new form of war waged by the West there. It is only the Ukrainian conflict that made this American version of hybrid war popular, which stayed in journalism as well as in political (scientific) discussions in Russian for good. It is something obvious, Russians willingly adapted notions and terms inseparable from new types of war, including hybridity of conflicts. It does not mean, however, that Russian theoreticians do not think of their own relevant vocabulary to describe hybridity of wars. As an example three definitions by Russian experts describing hybrid wars can be given. First, by C.F. Vikulov and J.J. Khrustal’jov, says that hybrid wars are complex and methodical impact of not only military (but also of political, economic, social) nature in international relations.²⁷ Another definition, close to that

the Post Imperial Era, London 1995, pp. 16–17, 30 and 38.

²³ M.A. Piotrowski, *Konflikt nigdy nie jest prosty...*, p. 10.

²⁴ See: R.G. Walker, *Spec Fi: The United States Marine Corps and Special Operations*, Monterey 1998; M.A. Piotrowski, *Konflikt nigdy nie jest prosty...*, p. 11.

²⁵ M. Wojnowski, *Mit „wojny hybrydowej”*. *Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, No 14, p. 9, special edition.

²⁶ According to the American theoretician, military decision-makers and experts faced the necessity to solve quite a big problem, how to carry out effectively military operations in new conditions, having as an adversary something that is not a state entity but different kinds of military (or paramilitary) organizations. So, how to win a war, if classical forms of fighting fail? Next problem in his considerations was to find such model of conduct, which would enable to keep order (stabilize situation) on territories under control of intervention power (as a basis for considerations conflicts in Vietnam, Somalia and Liban were taken). See: J.J. McCuen, *Hybrid Wars*, „Military Review” 2008, Vol. 2, pp. 107–108.

²⁷ In their opinion hybrid war is: „(...) комплексное применение различных методов (не только военного, но и экономического, социального, политического характера) воздействия

of Hoffman's, is presented by a well known political scientist, A.A. Bartosz. He gives the definition of a hybrid war as multiple actions of different kind carried out by an aggressor through irregular and conventional (classical) forms whilst being supported by a non-military component. Third definition is presented by Vladimir N. Akulinin and Natalia S. Epifanova, who, regarding political and military context, claim that hybrid war is a different military tactics, political actions and subversion actions as far as social and economic spheres are concerned on the territory of a potential adversary.²⁸

Classical definition of hybrid warfare seems to be still imperfect though, narrowing significance of the described phenomenon. It seems also quite often misinterpreted. Firstly, it regards mainly to activities carried out by organized military forces. Secondly, hybridity phenomenon defined nowadays is characterized by multiplatform activities and non-state actors taking part. One more element indicated by experts is the lack of declaration of war or introducing other states of emergency or a martial law. So, taking under consideration a broad spectrum, nature and scale of activities that follow the hybrid war and the fact that, usually, it is limited on purpose and kept under the level of regular war, instead of hybrid war there should rather be used terms like hybrid activities or operations of a hybrid nature.

Unfortunately, since 2014 on, i.e. since the conflict in Ukraine has started, hybrid war term has been abused because of its strong influence on public opinion, both domestically and internationally. Another abuse is creation of numerous references to the conflict in Ukraine, characterized as hybrid war, which is carried out by Russia against an independent and sovereign country. One basic question should, therefore, be asked here, whether the Ukrainian conflict is a classical example of hybrid war, like many Western theoreticians wish (journalists, politicians), or this hybridity phenomenon of military actions there is a new form of modern wars and was put into practice by Russian commanders and military decision-makers within the frames of politics to restore Russia's power position and making changes in the global balance of power? Many other questions can be asked to verify Western thesis that Russia had been preparing for the aggression for a long time, and the so called Gerasimov doctrine is one of the major pieces of evidence supporting it.

At present, Russia shall be assigned a particular role in creating and carrying out the new forms of activities, as hybrid wars. Many experts are obsessed with convincing the public that Russia, in particular its political and military decision-makers, had been preparing plans and strategies for many years to start hybrid activities. Such thesis seems false, though. To analyze thoroughly this problem, it should be assumed that

на противника в рамках межгосударственного противоборства (...)"'. See: С.Ф. Викулов, Е.Ю. Хрусталёв, *Методологические основы и специфика военно-экономического анализа*, „Экономический анализ: теория и практика” 2014, No 7, pp. 5–6.

²⁸ Гибридная война – это широкий диапазон действий, осуществляемых противником с использованием военных и иррегулярных формирований, с одновременным привлечением гражданских компонентов, В.Н. Акулинин, Н.С. Епифанова, *Концепция гибридной войны в практике межгосударственного противостояния*, „Национальные интересы: приоритеты и безопасность” 2015, No 36, p. 54.

each country (superpower or small or average), usually tends to create and introduce many normative acts, in which the strategic priorities in military and security areas are set up. These are doctrines, strategies, concepts of national security or military security. Generally, these are documents which are a basis of the state security system of the country. It is assumed that they have to be consistent not only with foreign policy (of security) but also and foremost with operational planning, training and armed forces development. That is why nobody should be surprised that Russia tends to modify and enhance its legal acts regarding national security in broader sense and its reason of state. Analyzing Russia's politics, one should take into consideration their professional attitude towards the topic of national security of the modern Russian country.

Russian theory of new wars. Gerasimov's concept

Several dozen of months back media were flooded by a wave of information indicating that Russians had been preparing the aggression on Ukraine for a very long time back (at least since 2008). Such news was adopted without a word of critics and stayed in media discussions for good, and, what is even worse, in scientific discussions as well. No one is arguing now that Russia for the last few years by changing its war doctrine and national security strategy clearly has shown that it does not intend to wait for further developments and do nothing. No one can also undermine the fact that political leaders of the Russian state have relatively clear policy, which aim is to change unipolar world and to get Russia back for a superpower position. It is worth remembering that in spite of numerous repeated trials Russia failed to get rid of fixed standards and beliefs coming back to the WWII that „human and equipment mass” would be able to counter effectively technological development. And patterns, which had been shaping it, for decades were recognized as indisputable canon. And it seemed that such idea was confirmed by the events of crushing the small Georgia. The assessment of the Georgia conflict done by the Russian General Staff showed that Russian army is not only unable to lead military operations in the long run but also it will not be able to fight effectively with a relatively strong adversary. Its training doctrine appeared to be out-of-date, moreover, Russian armed forces were not equipped with modern command and communication systems, combat equipment was archaic, and man power advantage and combat techniques advantage were only an illusion. Based on such assessment it has become necessary to implement system and modernization changes. Experiences from the war with Georgia, numerous corruption scandals and stagnation in armed forces reforms from the beginning of the 21st century made Putin realize that the necessity of changes both in doctrine and in organizational area regarding military security of the country in a broader sense, must become a priority of the state's political leadership. Apart from reforms of the armed forces a new training doctrine adjusted to an up-to-date battlefield has become a must. Based on security policy priorities and basic aims Russia dedicated itself in its foreign policy, some works were started on Russian vision for future wars and ways of conducting military activities in modern environment.

Nevertheless, it should be stated that concept of a new generation war was a topic discussed long back before the war in Georgia. At this moment, W. Kapitaniec views should be reminded which were published in *Битва за мировой океан* issued in 2002. He claimed that in spite of the huge leap forward in civilization and scientific-technological progress stimulating creation of new weapon systems in the 20th century, Russian art of war theoreticians were unable to establish the nature of future conflicts.²⁹ This is a reason why, in the beginning of the 21st century, there is a concept of the sixth-generation wars, in which precision-guided weapon and defense weapon play crucial role, not like in the past – mass land army. According to his assessments, whole aggressor's potential of a strike force shall be made to disrupt economy facilities by strong air strikes and mass precision-guided strikes from different positions, taking into account operations within global and regional information fight.³⁰ Furthermore, Kapitaniec claimed that new wars (6GW) would not be conducted on land, at sea or in the air only, but most of all in outer space. They would also not be of a chronic character³¹, with the use of mass troops and equipment. The whole process of armed struggle will be compact, quick and it will take the form of mass strikes of precision-guided weapon on economic and military facilities of the potential adversary³² with widespread use of radio electronic weapon (WRE). He noticed also that in this kind of fighting there may be a risk of the conflict transformation into a nuclear war.³³

However, the most interesting views of Kapitaniec refer to activities within information war since he claimed that with the growing saturation of the current battlefield with means of radio electronic struggle, there is an urgent need to take relevant remedial actions in order to paralyze adversary's electromagnetic emission means. The term WRE operations in a new war mean a complex of undertakings and activities to paralyze an aggressor by radio electronic means and protection of one's own troops and weapon systems from radio electronic impact of the potential adversary. The most likely components of such operations would be fire annihilation of the adversary's WRE systems and systems of every electromagnetic radiation, paralysis of the whole system of radio electronic means, protection of one's own sources of electromagnetic radiation, radio electronic cover against precision-guided

²⁹ И. Капитанец, *Битва за...*, pp. 50–51.

³⁰ *Ibidem*, pp. 51–52.

³¹ Russian theoretician, using the term chronic, made reference to experiences from the Great War time, when after a short phase of a maneuver warfare mass armies came to devastating positional activities.

³² A living force of an adversary may not be a target of strikes. Instead, economic facilities and state administration facilities on the whole of its territory will be attacked. No strategic reserves will be attacked formed on the basis of ground troops, because in new generation wars they are not going to pose a threat for a country that is the attacker, who wages a war using precision-guided weapon. This way, there is no need to occupy the territory of an adversary that is derived of economy, political system of which will the most probably collapse. These views clearly show that their author has based most of all on analysis of two conflicts, i.e. the second war in Persian Gulf and the so called NATO–Yugoslavia.

³³ И. Капитанец, *Битва за...*, pp. 53–54.

strikes. Activities carried out within WRA operation, together with fire and maneuvers, will be conducted simultaneously during strike operation in the air, in outer space, at sea and strategic operation to repel aggression. Information activities, on the other hand, were to be an active part of the striking component of the precision-guided means of destruction. Information resource of the countries was to be one of the most important elements of strategic striking forces systems and strategic defense forces of the country. It is going to embrace all areas of struggle (space, cyberspace, air, land, sea) and is going to concentrate on securing nets, telecommunication systems, radio navigational systems, power system, systems of command, transportation, finance, etc.

Also space recognition means will be added to information struggle measures and will become the main sources of information, both at planning stage, as well as at organizational stage, and conducting combat actions. There is going to be carried out a constant (uninterrupted) and to a large extent communication, radar, infrared, radiation, chemical, photographic and TV recognition from the space, which is to deliver information in real time.

Information counteracting³⁴ will be gained by the rule in information space and permanent information protection of strike and defense systems.³⁵

The main goal of information struggle, according to Kapitaniec, will be keeping necessary level of information security and decreasing such level of the adversary. The goal may be reached through the implementation of many interrelated tasks, from which the most important are: disrupting information resource and information field of the opponent and securing once own resource and fields.

Information countering, therefore, will be realized in the following directions and field of struggle:

- with command systems on different levels,
- fighting between strike and defense systems,
- creating information system in the whole outer space,
- Information securing/protection for its own offensive and defense systems.³⁶

Military and political goals in the sixth-generation war³⁷ will be possible to

³⁴ Information counteracting in wars of future should be understood as a new strategic form of warfare, in which special forms and methods influencing the opponent's information environment will be used and securing their own space in order to achieve strategic goals of the war.

³⁵ И. Капитанец, *Битва за...*, p. 69.

³⁶ Ibidem.

³⁷ The sixth generation war refers to the classification given primarily by Russian military theoreticians. They assume a division into 2 basic war categories: pre-nuclear era and nuclear one. There are four generations included in the first period of time (white weapon – war on a tactical scale; powder – war on a operational and tactical scale; rifled weapon – wars on operational and strategic scale; semi-automatic weapon, mass armies – wars on a strategic scale). The second period of time embraces two generations of weapon, i.e. nuclear weapon (threat to the world) – the Cold War time and non-contact war – operations in three basic dimentions: on land, in the air and space, development of precision-guided weapon. Its goal was to destroy basic functions of a state and economy as well as command systems and the most important military facilities. И.В. Бочарников, С.В. Лемешев,

achieve only by application on a large scale a precise offensive weapon, recognition and information systems and WRE. Therefore, it is necessary to integrate those components into one common weapons system combining information area in the outer space, in the air, at sea, on land and in cyberspace, which could change the nature of the future warfare.

Presented above views by Kapitaniec indicate that long before changes which brought armed forces reform in the Russian Federation, among Russian experts there had been noticed the necessity of changes in regard to transformation in the area of the future military conflict. Growing importance of information struggle deserves particular attention. After analysis of the mentioned Gerasimov's doctrine, it should be stated that much of Kapitaniec ideas have been adapted for the current theory of Russian military thought, especially, when it comes to forms and ways of conducting military actions during conflicts and wars in the beginning of the 21st century. Undoubtedly, some aspects of that vision have been also used during development and implementation of a new training doctrine in armed forces of the Russian Federation.

I. Kapitaniec was not the only Russian expert who had undertaken much earlier an analysis of changing war and military conflict realities and presentation of Russian point of view on this subject. Similar views presented also the late general major Vladimir Sliptchenko. He also believed that future wars would be based on a non-contact fighting with the use of precision-guided weapon (systems).³⁸ Different views on the future military conflicts presented another Russian military professional, general Makhmut Gareev, who – based on experiences for the war in Georgia in August 2008 – believed that only a mass attack of conventional forces, possibly with a support of modern measures, would characterize future battles.³⁹

After general Gerasimov's speech about his views on theory of future wars at the scientific conference in January 25, 2013 in the Military Sciences Academy in Moscow, large number of Russian scientists started to present many theories regarding different forms of waging wars in the future. The most interesting are those of J.J. Gorbachev concerning wars in cyberspace. In the article published in 2013 *Кибервойна уже идет*⁴⁰ he stated that we had been dealing with wars in the net for a long time because of computer technology developments. Moreover, computerization of weapon systems, communication and command and other fields of life would have a major impact on the way future wars would be waged. Gorbachev notes that every way of fighting could not be undertaken without operations in the net.⁴¹

Г.В. Люткене, *Современные концепции войн и практика военного строительства*, Москва 2013, р. 62; H. Sołkiewicz, *Wojna przyszłości – wojną niekontaktową (wg aktualnych poglądów rosyjskich)*, „Zeszyty Naukowe Akademii Marynarki Wojennej” 2009, No 1, pp. 72–73; В.И. Слипченко, *Войны нового поколения: дистанционные бесконтактные*, Москва 2004, pp. 44–58.

³⁸ И.В. Бочарников, С.В. Лемешев, Г.В. Люткене, *Современные концепции войн...*, pp. 61–62.

³⁹ М.А. Гареев, *Проблемы стратегического сдерживания в современных условиях*, „Военная мысль” 2009, No 4, pp. 3–6.

⁴⁰ See: Ю.Е. Горбачев, *Кибервойна уже идет*, „Независимое военное обозрение” 2013, No 13.

⁴¹ С.Г. Чекинов, С.А. Богданов, *О характере и содержании войны нового поколения*,

Furthermore, he points out that gaining dominance in a future war will depend on its gaining in the net. In his views he was supported by Dmitry Rogozin, who said that (...) *without robotics, effective reconnaissance (intelligence), weapon systems, command and communication automation, there is no way now or in the future to conduct armed struggle.*⁴²

Another idea, although controversial one, is the so called *консциентальных войн*, i.e. social wars or ones impacting on subconscious by W. Potehin and J. Gromyko. According to those two Russian scientists, it is a combination of undertakings which include the following elements of war: psychological (in terms of forms), civilization (essence), and information (the use of means and tools).⁴³ The basic goal of such war is to incapacitate the elites and whole nations by using different techniques of psychological and information influence so that they surrender. Russian scientists claim that current Russia has been a subject to such mechanisms for a dozen years which are typical for such kind of actions.⁴⁴

In the context of such considerations by Russian scientists and experts gen. Valeriy Gerasimov public announcement together with his article from the beginning of 2013 means, at the same time, an outline and systematization of views of Russian political and military decision makers, both on changes going on in international relationships and on future conflicts and wars. It was undoubtedly a presentation of Russian perspective and, in a way, political and doctrine assumptions, including foreign policy directions as well as using military and non-military potential of the Russian Federation.

V. Gerasimov thinks that, after the so called colorful revolutions, the world has changed so dramatically that the line between war and stable peace had been blurred.⁴⁵ Also the basic war paradigm involving defeating armed forces and the will of the adversary, taking over his territory, forcing him to take the conditions of peace, must give way to new solutions, at least as tools, methods and ways of getting the goal are concerned.⁴⁶ So, wars of the future will not certainly be waged with the use of military potential, but also with other tools and ways leading to a destruction of the potential adversary. Methods of conventional conduct have not been abandoned, nevertheless, they must be supported by operations of intelligence, political, psychological, economic, information, humanitarian and social nature, which are led together with the use of „protesting potential”.⁴⁷ Particular place in these activities should have all

„Военная мысль” 2013, No 10, p. 14.

⁴² Д.О. Рогозин, *Перейти от заклинаний и воззваний к практической деятельности*, „Военно-промышленный курьер” 2013, No 14.

⁴³ И.В. Бочарников, С.В. Лемешев, Г.В. Люткене, *Современные концепции войн...*, pp. 64–65.

⁴⁴ *Ibidem*, pp. 65–67.

⁴⁵ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, No 8, p. 2.

⁴⁶ M. Wojnowski, *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, No 13, p. 14.

⁴⁷ Gerasimov stressed that in Wars of future there is further automation of a battlefield, that is

kinds of special forces operations, and intelligence and counterintelligence services operations. On each stage of waging war, actions by specialized groups and sub-units of special forces are to play the most important role. Special forces and intelligence take an active part in non-military undertakings as far as information and psychological war is concerned. Basically, the future war will consist of three or four stages. First stage shall consist in intelligence preparation, recognition, infiltration, and active psychological and information activities (disinformation, subversion, sabotage, terrorism, infiltration, anarchizing the area of potential aggression); second – active and permanent internal destabilization and isolation of the target internationally; third – military action with the use of special forces, mercenary units, paramilitary and rebels to invade a part of the aggression target territory (activities without declaring war); fourth – operations with the use of all kinds of troops to destroy military and economic potential of the attacked country using precision-guided strikes systems as well as methods and forms of actions typical for a psychological and information war.⁴⁸

V. Gerasimov stressed a particular role of asymmetric and irregular actions on each and every stage of the conflict. Apart from partisan activities, sabotage or similar to terrorist activities he added also, for example, use of the so called protests potential, i.e. domestic opposition forces, national a religious minorities in the particular country.⁴⁹ Using those forces against the potential adversary will allow destabilizing the target of aggression, weakening of his potential, not only military but also political and economic. To realize that, according to Gerasimov, tools from the psychological and information war should be used. Such solutions are not, that should be stressed, anything new in Russian war tactics. Irregular activities or subversive acts, sabotage and terrorist have been practiced for over 70 years of the Soviet Union. Disinformation, inspiration, manipulating societies (active measures)⁵⁰, subversion, acts of terror (assassination), irregular activities (the so called active intelligence) have entered the arsenal used by Russians for good not only against political opponents, but also against neighbor countries and all those who were classified as hostile.⁵¹ Of particular concern should be the fact that exceptionally great emphasis was placed on information war tools on each step of future wars. According to Gerasimov, information struggle in broad sense is a separate kind of confrontation done by information, technical and psychological

why he considered necessary to carry out studies on possible application of artificial intelligence in lighting systems. See: *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces*, „Military Review” 2016, January–February, p. 26.

⁴⁸ В. Герасимов, *Ценность науки...*, p. 3.

⁴⁹ M. Wojnowski, *Koncepcja „wojny nowej generacji”...*, p. 15.

⁵⁰ See: J. Darczewska, P. Żochowski, *Środki aktywne. Rosyjski towar eksportowy*, Warszawa 2017.

⁵¹ M. Snegovaya, *Putin's information warfare in Ukraine. Soviet origins of Russia's Hybrid Warfare*, Washington 2015, pp. 11–12; M. Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*, without the place of edition 2016, pp. 44–47.

measures practically in all spheres of the state's activity (political, economic, diplomatic, humanitarian, military) as well as during a war.⁵²

Concept of a new generation war has become also a subject of considerations by two prominent military experts, colonel Sergey Tchekinov and general lieutenant retired Sergey Bogdanov. They both managed to assess tendencies which are to dominate in armed struggle in the 21st century. According to those two experts in current century there has been a significant growth in the importance of weapons designed on the basis of artificial intelligence, nanotechnology and robotic complexes of weapon of prospective generation.⁵³ It is particularly a geophysical weapon (which enables to influence lithosphere, atmosphere, ionosphere, influence climate changes and volcanoes eruptions, earthquakes initiation and other weather rapid changes⁵⁴), as well as laser weapon, plasma and psychotropic weapon.

Furthermore, according to Russian experts, revolution in technology caused a significantly growing role of measures and forces acting in the air and space area (what I. Kapitaniec had predicted) and information significance at all military struggle stages. The time taken to prepare operations or conduct combat action fell significantly. It was possible thanks to modern command systems that allow insight into a sphere of activities of an individual soldier on the battlefield.

S. Tchekinov and S. Bogdanov presented in October 2013 extended and original concept of a new generation war taking into account Gerasimov's theses. The proposed model was based on the eight consecutive stages.

1. Asymmetric activities.
2. Political leadership disinformation and general command disinformation by the so called active influence with the use of combined – overt and covert – special operations via media in a very broad sense, as well as via specialized entities, including special services.
3. Political and military systems disintegration (by intimidating, deceiving and corrupting political and military elites).
4. Using tools of information and psychological war on operational and strategic scale together with subversive and sabotage influence (terrorist).
5. Establishment of a no-fly zone over territory of the attacked country, roadblocks, bridges blockages, nodes blockages simultaneously with the use of mercenaries organizations and social regime and political system opponents of the country being an aggression target.
6. Conventional combat activities preceded by special forces operations and radio electronic (WRE), psychological and intelligence influence.
7. Intensification of military activities with support of information war tools.

⁵² В. Герасимов, *Ценность науки...*, p. 2–3; M. Snegovaya, *Putin's information warfare in Ukraine...*, pp. 15–17; P. Eronen, *Russian Hybrid Warfare: How to Confront a New Challenge to the West*, Washington 2016, p. 7.

⁵³ M. Wojnowski, *Mit „wojny hybrydowej”...*, p. 16.

⁵⁴ Ibidem.

8. Taking control over sensitive facilities and points of opposition. Elimination of the opponent troops, seizure, cleaning and maintenance of the area taken (final operations of land forces and airborne).⁵⁵

As we can see, both proposals by Gerasimov and Tchekinov and Bogdanov, complement each other and are a systematized Russian view on a future battlefield at the same time, both tactically and strategically. What is important here, it is an attempt to respond to Western proposals, especially of American theorists. While trying to analyze in details theoretical bases of definition by Hoffman and Gerasimov's concept as well as of S. Tchekinov and S. Bogdanov, one could acknowledge that substantial differences do not come from different views on the way military activities should be conducted, but they come from the authors' mentality and the way they perceive reality, which is closely linked to history and culture of nations they represent.

Hybrid war and Ukrainian conflict

Undoubtedly, the Ukrainian conflict has got many characteristics in line with classical definition of the described phenomenon. Whether this convergence should decide if we are to call the war in Ukraine, nowadays or in the future, a classical example of hybrid war and identify Russia as the country which had used its elements for the first time in practice? Even if we agree with the opinion that Russia's involvement in the conflict took a form of hybrid actions, doubts, however, about the nature of the conflict will stay. It is indisputable that Russia has taken Crimea and has used in the course of its actions new forms and ways of operations typical for hybrid conflicts. Also its involvement in the rebellion in the eastern provinces of Ukraine is unquestionable. Nevertheless, many aspects of terminology by Hoffman do not coincide with events in the course of the Ukrainian conflict. So, further definitions of those events seem to be a pure simplification and are more like an element of information war waged both by Russians as well as the West and Ukraine itself. Therefore, it should be stressed that Ukrainian conflict should be defined rather as a civil war or a rebellious war, in which new, combined forms and ways of military actions were used, both conventional (although without direct presence of entities of the international law) and other non-military methods. Especially the term *c i v i l w a r* is justified in its classical meaning because it is a political and ethnic conflict conducted by armed struggle within one country. At the same time, outer player (subject) does not affect the relevance of the term usage to the description of events connected to Ukrainian conflict. In the past there were at least few examples of civil wars with even bunch of outer players and the course of events was characterized by some basic for hybrid wars features. A very good example can be the Spanish Civil War 1936–1939. In this case one may speak about a classic example of armed clashes between two political options using different forms of combat actions and different methods, including

⁵⁵ С.Г. Чекинов, С.А. Богданов, *О характере и содержании войны...*, pp. 16–23.

non-military ones, in their fight. Apart from classical operations there were elements of guerilla war, irregular activities (subversion, sabotage), psychological and information war. Both sides were supported by outer actors which had also been carrying out not only armed struggle but also psychological and information struggle although range and intensity of it were limited by technological capabilities. So, it is possible in theory to find a lot of similarities between Ukrainian and Spanish conflicts:

- war in Ukraine and in Spain served as testing grounds for both Russia and the West,
- in the two conflicts there are paramilitary troops, irregular troops and volunteers, including outer actors,
- the parties to the conflict are waging fierce war for hearts and minds and at the same time they influence intensively the general public,
- in case of both wars there were both conventional and irregular (guerilla) operations carried out.

It is worth noting that the nature of conflict sides is a differentiation element as far as the two wars are concerned. In Spain we are dealing with political adversaries, there is no interference of a neighboring country and the reason of the war is, first of all, ideological conflict and to some extent religious and social conflict. While in Ukraine, there was a political conflict in the first phase with a significant interference of the neighboring country which changed in a due course (or rather developed) into an ethnic conflict of a rebellion nature (form of rebellion war typical for civil wars). Certainly, there are also numerous differences of historical nature. That is the reason, what should be stressed, the Spanish civil war example is in this case only a hypothesis indicating some similarities as far as civil war phenomenon is concerned.

Coming back to consideration of hybridity of Ukrainian conflict, there should undoubtedly be noticed that it is an example of new forms of combined activities typical for new wars of the 21st century. This Ukrainian example clearly proves that application of different forms of military and non-military (hybrid) impact in scope of conducted operations proved to be very effective only because the target of aggression was weak⁵⁶, with no solid democratic institutions and, what is more important, torn apart by domestic conflicts, which had deepened in the course of its short history. A major issue for the conflict development was a lack of a state-building experience and patterns that could support political elites in the course of a system transformation. From its very beginning, Ukrainian state by building its statehood, had been taking eastern patterns.

⁵⁶ Krzysztof Wąsowski claims (after: Military Balance 2015) that during Russia's operations in Ukraine there were 3 characteristics of a hybrid war occurred. These were: conventional activities, psychological and information activities, special forces operations as well as influencing cyberspace and political and economic spheres. At the same time he distinguished as many as nine groups (attributes) typical for hybrid methods. These were: asymmetric nature, ambiguity and war via intermediaries (irregular character). Such division, although interesting and definitely authorian is a mixture of different forms and methods of military and non-military action, Rather freely assigned. It also causes chaos in terms of vocabulary and problems. See: K. Wąsowski, *Istota i uniwersalność rosyjskiego modelu wojny hybrydowej wykorzystanego na Ukrainie*, „Sprawy Międzynarodowe” 2015, No 2, pp. 45–47.

That is the reason why it appeared to be only a matter of time that the internal conflict would occur, which almost led to a disintegration of the country.

Undoubtedly, Russia had been very well prepared for the events of 2014. It used weaknesses of its neighbor. Earlier on, it had very well recognized the political scene and even had stimulated some events. Acting on the basis of already checked patterns it took over the control over Crimea territory in a bloodless way. It was a practical implementation of some elements of the Gerasimov's doctrine. According to unconfirmed information, both before annexation of Crimea and during the Crimea operation, most of the territory of Ukraine had been covered by radio electronic shielding and got under organized cyber strike⁵⁷, which enabled, to a large extent, the management of governmental administration and of military and internal security sector on the peninsula. Furthermore, there had been tactical recognition done before and all levels of state management from the central level to the local one⁵⁸ had been worked out by intelligence. Russian-speaking population unwillingness to Ukrainian authorities was perfectly used and opposition forces were logistically prepared. It all happened under the watchful eye of the governmental administration and security forces of Ukraine.⁵⁹ However, it should not be a surprise for the majority of analysts who had been observing the situation in the country and changes in the defense system of the Russian Federation very carefully. Rapidly escalating internal chaos in Ukraine, numerous unresolved social problems, common corruption, unemployment, constant conflicts with Russia and lack of any perspectives to improve citizens' life together with laxity of oligarchs to ruin the country, like Cossack warlords prowling in the former borderland of the Second Republic of Poland, had been sui generis trademark of Ukraine from its very beginning.⁶⁰

⁵⁷ According to some Western experts Russia was to use operations in cyberspace during the political dispute in 2007 with Estonia for the first time with regard to liquidation of Soviet occupation symbols in public space as well as during the war with Georgia in 2008. It was pointed out, though, that hacking activities against Estonia were not coordinated and most probably were not supervised by Russian special services, so – if experts can be believed – the initiative came from the grassroots from Russian patriots (hackers). Totally different was supposed to be the situation of attacks on Georgia's informative systems before the country was attacked. It is not only that part of the nets used by governmental institutions that was blocked but also some data on possible preparations of military forces to an offensive against Georgia were installed. Behind that, according to Pasi Eronen inter alia, were Russian hackers and members of nationalist youth groups. Such scenario reminds modus operandi characteristic to active operations inspired by Soviet (Russian) special forces. See. *Georgia on Their Minds*, „The Wall Street Journal” 2009, October 1, http://www.wsj.com/articles/SB1000142405274870447150457444658_2129281924 [access: 12 I 2018]; A. Hagen, *The Russo-Georgian War 2008*, in: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, by J. Healey, K. Grindal, Arlington 2013, p. 196–200; P. Eronen, *Russian Hybrid Warfare...*, p. 8.

⁵⁸ Mark Galeotti assessed that in the eastern Ukraine FSB had perfectly penetrated Ukrainian security apparatus and at the same time it had been taking activities stimulating to a desertion, monitoring planning and activities by Kiev. See: M. Snegovaya, *Putin's information warfare in Ukraine...*, p. 12.

⁵⁹ This way, as Polish and Western experts claim, definition basis for hybrid war was fulfilled with regard to Ukrainian conflict.

⁶⁰ In terms of GDP, Ukraine was and still is one of the poorest European countries. According to the IMF data from 2013, GDP per capita in Ukraine was 3900 USD. For comparison: in Estonia –

Furthermore, police forces, special services and army suffered from underinvestment and there was no way to counteract the adversary. On the one hand administrative apparatus had been corrupted by oligarchs and, on the other hand, it had been infiltrated by Russian special services.⁶¹ Not to simply pay lip-service, words of general lieutenant A. Skipalsky, founder of the Ukrainian military counterintelligence and former deputy chief of the SBU should be cited. He said: *In the days of Janukovich almost all heads of Ukrainian military forces and Spetsnaz used to belong to the Russian Association of Airborne landing Soldiers led by one of deputies of the Defense Minister of the Russian Federation. Most of them have hold their high positions until now.*⁶²

And this is the following assessment of the SBU by gen. Skipalsky: *We have a structure born with qualities of being unprofessional and corrupt, saturated with anti-Ukrainian, pro-Russian, thieving and immoral elements (...). Former KGB officers who had stayed to work in our country, did not counteract but favored anti-Ukrainian sentiments in the course of Russian special services activities.*⁶³

It should be noted that while Skipalsky was assessing the condition of Ukrainian special services, in reality he was assessing condition of the whole country. What can you say about the country whose head of special services deserts and takes refuge at the hostile neighbor. It was A.G. Yakimenko, a graduate of Yuriy Gagarin Air Force Academy, until 1998 officer of Russian Army. Until the time of Maidan, he had been at the head of the most powerful and influential special service of Ukraine and had knowledge about the whole security system in Ukraine. How it happened then that political decision-makers had put him in charge of such a sensitive institution a Russian guy? Partial response can be found in Yakimenko's internet entry: *after graduating from the academy I understood that my skills are of no use to anybody. So, I quit. And those jerks noticed it and recalled me again. So I'm still acting.*⁶⁴

„The jerks” had accepted a former Russian officer to serve in the SBU Regional Department in Donetsk, then appointed him the Chief of SBU in Sevastopol and then sent this exquisite expert back to Donbas for the post of the Chief of the SBU Regional Department in Donbas. On January 9, 2013 Yakimenko became the SBU Chief and this position gave him the right to be a member of the National Security and Defense

18 000 USD, in Russia – 15 000 USD, in Poland – 13 000 USD, in Belarus – 7400 USD. In 2016 GDP in Ukraine was 2185 USD per capita and GDB in Belarus was almost 5 000 USD per capita. In the same year Russian GDP was assessed to be ca. 8700 USD and Polish GDP more than 12 300 USD. Making Ukraine with its chernozemes, natural resources, rivers and seas two times poorer than barren Belarus is a unique result, which had not been achieved so far by any king, hetman or any secretary general.

⁶¹ In 2010, after Yanukovych took the power in Ukraine, the Chief of the SBU became Valeriy Khoroshkovsky, who was stressing many times in press interviews, that what stood behind a good cooperation with the FSB was a common chekist past. It resulted in signing in 2010 an agreement on cooperation with FSB and breaking contacts with the CIA at the same time, and easing any operations against Russian special services in Ukraine.

⁶² М. Солонин, *Проект «Новороссия» – итоги*, „Военно-промышленный курьер” 2014, No 38, p. 11.

⁶³ Ibidem.

⁶⁴ Ibidem.

Council. This way he got the access to all intelligence and military secrets of Ukraine. On February 24, 2014, after the overthrow of Yanukovich, he fled to Russia where he has been hiding up to now.⁶⁵ Any comments are unnecessary here.

It is not only special services that were a problem in Ukraine. Ukrainian army was not in a better shape. Military forces stance in the country during the conflict is best reflected in one of the Chinese philosophers thoughts: *the army of morons under the lion's command matters more than the army of lions under the moron's command*. At first, it should be underlined that military forces of Ukraine had been penetrated by the Russian intelligence as much as other elements of law enforcement structures of the Ukrainian country. One should agree with a conclusion by Andrzej Wilk, an excellent expert on eastern Europe political and military issues that it was a quarter of a century for Ukraine to build efficient military forces from the very beginning. Conflict in Donbas and seizure of Crimea revealed, however, that the country did not have sufficient military potential in the spring of 2014 to prevent annexation of the peninsula and rebellion in the eastern provinces of the country.⁶⁶ Informal ties and connections between Ukrainian and Russian army personnel had never been broken, which caused, in consequence, that Ukrainian personnel switched sides after Crimea annexation. Changes observed by Ukrainian soldiers in the military forces of their eastern neighbor, especially as far as economic aspect was concerned, were also crucial. The Ukrainian army, as from 2010, found itself in permanent collapse. Corruption, underfunding (budget of 1%⁶⁷), abandonment of integration into NATO, were those indicators that made the process even deeper. Reforms, which had been initiated back in the 1990s, were limited because of lack of money. Also personnel decisions did not make restructurization processes easier. A. Gricenko, former Chairman of the Supreme Committee of the Council of Ukraine on National Security and Defense, gave the picture of the Ukrainian military forces from 2011: *at present Ukrainian military forces do not have even one battalion with combat capacity, no one squadron in shape to fight, there are twenty two thousands of vacant posts in the army at the moment with no candidates for them. There is a lack of lower-level and mid-level officers in the army. Commanding officers are paid slightly less than cashiers at cashiers' desks in supermarkets*.⁶⁸ However, there was plenty of generals – 450, including 14 army generals⁶⁹ (the highest rank in the Ukrainian army). The quality of management and command personnel did not meet requirements of the 21st century as well. There are two examples that give

⁶⁵ Ibidem.

⁶⁶ A. Wilk, *Najlepsza armia, jaką miała Ukraina. Zmiany w Siłach Zbrojnych Ukrainy po agresji rosyjskiej*, Warszawa 2017, p. 8.

⁶⁷ Still in 2006 the budget was about 1,36–1,74% of the GDP, to gain 0,79% three years later and ca. 1% in the next few years – with progressing degradation of equipment and decreasing number of recruits and after the professional army was established – with practically no interest from Ukrainian nationals in entering the service in the army. See: D. Sanders, 'The War We Want. The War That We Get': *Ukraine's Military Reform and the Conflict in the East*, „Journal of Slavic Military Studies” 2017, Vol. 30, No 1, pp. 33–34.

⁶⁸ М. Солонин, *Проект «Новороссия»...*, p. 11.

⁶⁹ Ibidem.

a good picture of the situation: first – designation of a businessman Pavel Lebedev as the Minister of Defense and second – giving admiral Denis Berezhovskiy command over Ukrainian Navy who, just after his appointment, went over to the Russian side.⁷⁰ Anyway, he was not the only soldier who abandoned service in the Ukrainian military forces towards military forces of the Russian Federation.

So, how was it possible that this internally broken, infiltrated and full of domestic conflicts Ukraine could resist a mighty neighbor? The answer seems to be simple: the country could not be able to do that. What is more, practically no other country, maybe with the exception of the USA, could manage to deal with aggression based on hybrid tools and methods on a strategic scale. It is possible that some part of countries of the so called old democracies circle would eventually fend off the possible attack, but its results would be very hard to assess. However, the case of Ukraine shows that weak democratic institutions together with a lack of state-building experiences are basic factors contributing to the state disintegration. This is the reason why there should not any special plan (strategy) be found with regard to Moscow activities toward Ukrainian state. One should also agree (at least partially) with some assessments of Russian politicians and experts, who claimed that, both in Crimea and in the eastern regions of Ukraine, Russia has not used any new forms and methods of combat, nor tactic solutions defined by the West as hybrid war. This is also the opinion of the Head of the Center for Strategy and Technology Assessment in Moscow, Ruslan Puhov.⁷¹ His assessments are only partially true. Russians, indeed, did not use any new methods of combat which can be described as destabilizing or disintegrating the country. They just used experiences from the past, both from the history of their own military forces and special services, as well as from the experiences of the West (particularly the USA). In this way they worked out their own model of fighting in a globalization era.

To summarize, it has to be concluded that Puhov's ideas and assessments fit into a new Russian doctrine of future wars. At the same time we should also agree with the opinion of a Russian scientist, who had assessed Ukrainian military troops correctly by saying that Russians did not have to lead more or less advanced information operations because of low grade computerization of the Ukrainian army and archaic equipment it had, especially its units based on Crimea. However, other assessments and analyses by Puhov should undoubtedly be regarded as deliberate disinformation of social public, fitting perfectly into a Russian model of information fight.

By analyzing the Ukrainian conflict, one more – interesting as it seems – aspect should be pointed out. While assessing the course of events, starting from the protests in Maidan, via Crimea annexation, to struggles in eastern provinces of Ukraine, one may have the distinct impression that our eastern neighbor has become a one huge training ground used by current actors of international relations as area for testing new military doctrines (tactics and strategy of fighting on current battlefield), techniques,

⁷⁰ A. Wilk, *Najlepsza armia, jaką miała Ukraina...*, p. 10.

⁷¹ Р. Пухов, *Миф о «гибридной войне». Никаких принципиально новых действий наша армия в Крыму и на Украине не вела*, „Независимое военное обозрение” 2015, No 19, p. 1.

equipment (gear and weapon systems) and diplomatic plays. Both Russians and the West (and obviously Ukraine) carry out massive and universal information and psychological war, test new weapon systems, systems of command and support, new training doctrine and future wars concept (in this area Russians are the leaders). Damage, destabilization of Ukraine and its disorganization do not mean anything for Russia and countries of the so called old democracies. Only one accounts: checking whether Russia can be finally eliminated from the global market and make it to submit to a general worldwide trend and post Cold-War order. No one from among political leaders does not probably realize what the reality after the Ukrainian crisis will look like and to what extent experiences gained during the war in Ukraine in military and political spheres will be used. Undoubtedly, apart from damage and human and material losses Ukrainian state lost most in mental and state-building spheres, which anyway, has its reference to non-military hybrid activities. Despite the change of those in power and, as it seems, the opening for the West, internal situation in Ukraine is still very complicated. It is still a corrupt country, ruled *de facto* by *familijas*, building up its credibility among its citizens and military potential very slowly. In spite of the fact that intensity of fighting has dropped visibly it does not mean that the process of dealing with the crisis and conflict gives hope for the peaceful war ending. Quite opposite, it seems that sides of the conflict are at the serious impasse and hybrid war has turned into a trench warfare.

Recommendations

It should be clear that the West in broader sense has entered probably the most stormy era of an aggressive confrontation to overthrow fundamental basis of democratic models and institutions. Asymmetric and hybrid warfare makes it possible that even less mighty players are able to carry out many effective strikes despite of a lack of enough military potential, and, in some favorable circumstances, to take initiative both on tactical as well as on strategic level. It should be remembered that it is a state that will be even more threatening adversary, by using developed hybrid techniques and tools because it has a worked out doctrine of action and measures, and it is determined to gain political aims by using them especially against potentially weaker opponent.

Undoubtedly, it is the USA, the European Union and NATO that have such proper measures at their disposal to prevent Russia from leading hybrid operations, but it would be a waste if each and every Russia's move was counteracted. It is Russia strategy to inspire actions by the West and to force presence in expensive operations. Instead of that the West should clearly identify the most important strategic and economic infrastructure and take effective steps to eliminate and weaken Russian possibilities of waging hybrid wars. In view of this there should be intelligence activities on a broad scale carried out, including those which allow to permanently eliminate Kremlin's abilities and limit its possibilities of information and psychological actions. By using

asymmetric and hybrid tools the potential and influences from the Gerasimov's doctrine should be effectively limited. Moreover, the following should be done:

- building (creating) national and international coordination centers against hybrid war,
- doing scientific research into structures and procedures able to oppose hybrid and asymmetric threats on each level and to use them,
- studies on Russian strategic investments area, recognizing them and diminishing their influences,
- introducing new strict procedures and legal solutions regarding cyber security and security of information in a broad sense,
- leading diversified and effective propaganda campaign with regard to social opinion of the West and Russia,
- developing defensive capabilities and alliances in frame of economic war,
- developing abilities and anti-corruption tools.

Abstract

After the collapse of the Cold War we have been observing sudden changes in tactics and ways the wars and conflicts are waged. Increasing mutual penetration and combining of regular and irregular war techniques has been noticeable. Current military conflicts, both regional and with broader range, are characterized by complexity of all possible warfare means and their practical usage. This diversity of elements included in destructive actions has become extremely popular subject of political and media discussions and has currently been defined as hybrid activities or hybrid war.

It has to be clear that the West in broader sense has entered the most stormy era of the aggressive confrontation to overthrow fundamental basis of democratic models and institutions. Asymmetric and hybrid warfare makes it possible that even less mighty players are able to carry out many effective strikes despite of a lack of enough military potential, and in some favorable circumstances to take initiative both on tactical as well as on strategic level.

Keywords: hybrid wars, future wars, war in Ukraine, Gerasimov's concept, military conflict, asymmetric war, rebellious wars, sixth generation wars (6G wars), irregular war.

Jolanta Darczewska

Active measures as the Russian hybrid aggression in a retrospect. Chosen aspects

Outline of the subject

Political and military pressure by Russia on its closer or further international neighborhood, and its readiness to escalate tensions have become one of the subjects in security discussions for the last years. High level of Russian hybrid threats¹ has been a subject of numerous analyses and articles. But still the reflection on the subject is fragmentary, because it does not embrace all its aspects and symptoms. Most authors tend to concentrate on disinformation and propaganda, i.e. activities in an informative sphere (media and cyberspace). Meanwhile, information pressure is admittedly a dominant but only one instrument of crisis-prone impact of Russia. Very often deliberately provoked intelligence incidents as well as border incidents, migration, events both abroad and domestically (for example conferences, festivals, peaceful camps), parliamentary and presidential elections interference, financial and political support for radical elements and centrifugal trends within the European Union, decision making interference, discrediting politicians unfriendly to Kremlin are pretexts for overt and covert media operations. Such activities during the Cold War were called *a c t i v e m e a s u r e s*.² If we put them into a hybrid threats paradigm, it makes it possible to look at them from a broader perspective, to diagnose them and counteract them.

Counteracting hybrid threats makes it a challenge for counterintelligence services. It is determined by the complex of resources used by Russia. The threat is both external and internal, domestic and transnational, military and intelligence, which you cannot respond symmetrically. Hybrid operations are carried out by state and non-state actors secretly and semi-overtly with the use of legal and illegal methods. They are carried out both in physical and information and psychological spheres. Military vocabulary (“information war”, “psychological war”, “propaganda war”, “civilization war”, “political war”) used by Russian experts and journalists makes it difficult to fight with them. It suggests that it is a war between parties using adequate measures. Meanwhile, the situations is asymmetric from nature: hybrid operations on a large scale are used by an aggressor, while the attacked – if only because of respect for basic rights and freedoms and state of law values – have to

¹ More on <http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html> [access: 5 I 2018].

² See J. Darczewska, P. Żochowski, *Środki aktywne. Rosyjski towar eksportowy*, <https://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2017-05-30/srodki-aktywne-rosyjski-towar-eksportowy> [access: 5 I 2018].

find other effective countermeasures and counter methods to contrast the aggressor's narrative their own positive narrative. In NATO terminology it is called a strategic communication. The term "strategic communication"³ has apparently widened its former meaning (informative security of the battlefield) and has become *sui generis* methodological foundation of hybrid threats counteracting treated according to one universal standard. In order to have a consistent approach, the European Union took over the NATO terminology.⁴

A genuine renaissance of the topic of active measures⁵ observed in the West is caused by the controversial and imprecise terms containing qualifier "hybrid" and also by the attempts of more complex approach to hybrid forms of aggression. Military origin of the terms, as it seems, overrides sometimes the fact that the army is not the only one (and even not the main) participant of a hybrid war: it is used in a limited scope – as an ultimate argument. In this context, a historical term *a c t i v e m e a s u r e s* accurately reflects a complex nature of this phenomenon and synthesizes different techniques: political, military, intelligence, economic, diplomatic, financial, media and cyber. It also stresses important (if not crucial) role of intelligence services in preparing and creating executing background for Russian influence operations and close links between these activities and acts of defiance, diversion, terrorism, international organized crime and other symptoms of disruptive activities. Regarded as hybrid threats in retrospect it indicates that they are of intelligence nature. Moreover, the term gives a broader political, social and historical perspective to a picture of threats from Russia.

³ The cited term of *s t r a t e g i c c o m m u n i c a t i o n s* as well as the others in the text have been defined in: *the National Security Bureau (BBN) mini(dictionary). Proposals of the new terms from security area*, <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035...html> [access: 5 I 2018]. More on strategic communication Tomasz Kacala, *Komunikacja strategiczna*, <http://sdis.wp.mil.pl/plik/file/Publikacje/kacala.pdf> [access: 5 I 2018].

⁴ See for example: Joint Communication to the European Parliament and to the Council of 6 April 2016, Joint framework on countering hybrid threats. The document set out strategic lines of NATO and the EU cooperation: **enhancing public awareness** by forming special mechanisms of exchanging information between Member States and coordination of the EU activities to gain consistent strategic communication; **enhancing resistance** of the main strategic sectors, like cyber security, critical infrastructure (transmission of electricity, transportation, cosmic space) as well as enhanced security of financial system, public health protection and support for efforts to counteract any extremism and radicalization; **crisis prevention, response and overcoming** (definition of efficient procedures, including solidarity clause – Article 222 TFEU and mutual defense clause – Article 42.7 TEU in case of a huge hybrid attack); **tightening of cooperation between NATO and the EU, as well as other partner organizations** in a common effort to counteract hybrid threats, with respect to openness rule and independence of decision making process of each of those organizations.

⁵ See for example: С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnye-sovetskie-meropriyatiya-v-putinskoy-rossii> [access: 4 I 2018]; <https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war> [access: 4 I 2018]; <http://www.cyberdefence24.pl/704854.prof-andrew-wilson-rosja-jest-pewnego-rodzaju-patologicznym-panstwem-pirackim-wywiad> [access: 4 I 2018].

Two models of Russian discussions on hybrid strategies

1. Military model. In Russian military thought the terms hybrid strategies, hybrid war, hybrid technologies have appeared relatively not long ago. The start of their implementation has captured Michał Wojnowski⁶ and put it in the context of Russian military thought and strategic culture. He brought forward basic assumptions and terms and put them in a geopolitical paradigm. In general, in Russia they are implemented in the military model of reflection on the nature of present war as development of the so called Gerasimov doctrine, following up amorphous concepts of “small wars”, “rebellious wars” and “asymmetric answers”. The author rightly judged the address of the Chief of the General Staff of the Russian Federation during general assembly of the Academy of Military Sciences⁷ in 2013, disseminated in the Russian and international media as information and psychological operation. As he pointed out:

The general words about alleged changes in the ways the wars were to be waged, what reportedly “colorful revolutions” in North Africa and in the Middle East showed, are treated too literally in the West. It is not about innovative way of revolutions incitements (practiced since centuries) but about modern measures used for that purpose. In case of the so called “Arab spring” it was, for example, the use of media on a broader scale, including social networks (Facebook, Twitter), which is a modern solution. The idea of the artificial revolution initiation is not new as such but the tools used for this purpose are indeed.⁸

⁶ M. Wojnowski, *Mit „wojny hybrydowej”*, <https://www.abw.gov.pl/.../1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE...> [access: 5 I 2018].

⁷ Contrary to the name Academy of Military Sciences (AMS) is not a scientific institution, although it claims so. It is financed by private sponsors, who get titles of the honored members of AMS. It focuses ca. 15000 experts in the field of security and defense, who – in public – presents themselves as “the real members” and “the members correspondents” of AMS. It was founded by the president Yeltsin’s decree of 1995 as a centre for independent defense studies. Its constant president is army general Mahmut Gareev. Among founder members were Russian Institute of Strategic Studies (being back then within the Foreign Intelligence Service structures), Scientists Committee “For a global security”, Defense Businesses Supporting League, Russian and American University, Russian Association of Industry and Businessmen, International Studies Centre and others. The Academy employed personnel of liquidated science institutions and political and military personnel assigned to the army reserve. Officially under this prestigious name there is an association of analytical and research centers of the military forces, Ministry of Internal Affairs, Border Guards of FSB, Ministry of Emergency Situations and independent experts and journalists specialized in security and defense area. The Academy combines research and study with social and educational activity: since 2008 it has been publishing a quarterly “Information wars”; its members supply media with information and take part in different system projects by law enforcement institutions, the National Council, the State Duma and the Federation Council. Annual conferences are an important platform of vocabulary and narration standardization used next in media campaigns and of contacts between retired officers of the army and active personnel of military information system.

⁸ M. Wojnowski, *Mit wojny hybrydowej...*, p. 30.

By the way, back then, Valeriy Gerasimov did not speak about hybrid war but about new generation wars, which he described using Western terms like non military measures and indirect activities with the use of potential of protest from among the local people. Asymmetric indirect activities are due to rely on the country political isolation, economic sanctions, communication routs blockade, intimidating by the use of force and bringing in international troops on the pretext of human rights protection and humanitarian operations. General stressed foremost a particular meaning of information actions and special operations which were a core feature of the colorful revolutions inspired from outside. By the way, the concept of colorful revolutions, leaded reportedly according to the principles of the warfare, appeared also in Gerasimov's speeches in the Academy of Military Sciences in 2014 and 2015. In 2016 the General used "soft power" to describe Russian hybrid activities and in 2017 he spoke about the so called hybrid method of waging a war as one should regard as equivalent of a non-contact war⁹, which was confirmed in remarks of the authors of Internal Security Review special edition 2015.

Military researchers of a hybrid war notion stress its small usefulness for Russian wars theory on the one hand, and Western geology of hybrid war on the second, which combines elements of conventional war with guerilla war, terrorism and diversion, propaganda and information war. Their analyses on NATO and USA hybrid operations have socio-technical potential: giving a picture of "the gravity of situation" they justify a mobilization model of a country (embracing not only a military and information sphere but also an extensive state management sphere together with legal, cultural, education spheres, in which there is a clear image of an enemy). It was confirmed by the Academy of Military Sciences conference of March 2017. The panelists agreed that the hybrid specific nature of current conflicts is determined by the superiority of non-military measures over armed struggle. They refer to the General Staff of the Russian Federation assessments of its proportion as 1:4 in favor of non-military factors.¹⁰ And it was concluded that (...) *conventional wars are waged by losers nowadays*.

2. Civilian model. Civilian analysts linked to Russian special services have attempted more dynamically to adapt NATO concepts of a hybrid war. (At this point it should be reserved though, that the proposed division is simplified. In Russia as

⁹ See for example В. Герасимов, *Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны*, <http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/862-vestnik-avn-2-2016> [access: 10 XII 2017]; В. Герасимов, *Мир на гранях войны*, <https://www.vpk-news.ru/articles/35591> [access: 10 XII 2017].

¹⁰ А. Бартош, *Разведка России в противостоянии гибридным угрозам*, http://nvo.ng.ru/sp-forces/2017-10-06/1_968_scouting.html [access: 5 I 2018]. See the same author: *Гибридная война становится новой формой межгосударственного противоборства*, http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html [access: 5 I 2018]; <https://topwar.ru/112955-gibridnaya-voyna-stanovitsya-novoy-formoy-mezhgosudarstvennogo-protivoborstva.html> [access: 5 I 2018]. See also: А. Бартош, *Конфликты XXI века. Гибридная война и цветная революция*, Москва 2017.

„military” all possible kinds of military services are described: army, border guards, National Guards, special services and so on. In political language to distinguish them it is used a term from the 1990s: *siloviks*. Analysts linked to special services noticed an important practical value of this concept. Transforming it into their own narrative and strategic culture they acknowledged information war as the essence of hybrid war and its core. Most theorists of this consideration movement tend to limit a definition scope of the notion taking out elements of armed struggle, i.e. limiting to actions in NATO terminology described as *non-military* (or *non-kinetic*). Generally, in this „non-military” model the three approaches are possible (although they cross with each other mostly, they are complementary):

- 1) phenomenological,
- 2) technological,
- 3) functional.

The most important indicators of the first approach are attempts to define hybrid war, its origin and symptoms on multidisciplinary ground (sociology, political sciences, military sciences, security science, psychology, ethnology and others). As a sociologist, Farhad Iliasov¹¹ put among its referents the following:

- propaganda influence on different suitable audiences in the aggressor’s country and in the attacked countries;
- creating and inspiring of separatists and collaborationists groups in attacked countries;
- initiation of unrests and mass protests;
- diversion and terrorist actions carried out by an aggressor together with insurgents;
- secret support for separatists with arms, intelligence, finance and irregular formations activities;
- activities to destabilize and weaken the economy of the attacked country;
- diplomatic support and information backup for special projects.

According to the author the goals of such actions would be occupation, annexation of the territory, change of political regime or the present government. Alexander Bartosz¹², while concentrating on the reasons of the current hybrid conflicts, presents a concept of instability catalists worldwide. They are:

- USA and NATO activities (presence on Russia’s doorstep)
- unilateral use of force in international relations
- unlawful usage of economic sanctions against Russia
- provoking financial and economic crises
- lack of consensus as far as fight with international terrorism is concerned
- global information confrontation and constant improvements of fighting methods in cyberspace
- tensions and chaos in international relations by support for nationalists sentiments, xenophobia, separatism, extremism, religious fundamentalism

¹¹ Ф.Н. Ильясов, *Словарь социальных исследований*, 2016, <http://www.jsr.su/dic/dictionary.html> [access: 5 I 2018].

¹² А. Бартош, *Разведка России...*, *ibidem*.

- migration crises, problems with drugs and human trafficking
- reinforcement of fight for raw materials and mineral resources (Middle East, Arctic, Central Asia and the Caspian Sea).

In this context Bartosz puts the notion catalysts of decomposition/disintegration processes (diplomatic notes, paramilitary organizations activity). Also, according to him the most powerful catalyst are the so called colorful revolutions, organized in the watershed stage of hybrid war to get a rapid effect of destabilization in the attacked country.

Technological approach is based on the isolation of hybrid war basic dimensions and its mechanisms. Cited above Bartosz features political, diplomatic, information, paramilitary and historical fronts. Igor Panarin adds ethnic front and develops historical front which, in this case, is grotesque. The origins of hybrid operations against Russia, according to Panarin, are in a secret alliance between France, Austria and the United Kingdom (1815) and in founding Russian Masonic lodge in order to carry out a coup d'état in Russia. Its indication was the Decembrists revolt in 1825 against Nicholas I. Intensified hybrid operation of the Masonic lodge and the British MI6 in the beginning of 1900s resulted in the February Revolution of 1917 and the biggest geopolitical catastrophe in the world, the collapse of the Imperial Russia (second such catastrophe was the USSR collapse). According to Bartosz such beginning dates back to the Times of Troubles (Great Smuta 1598–1613) resulting in (...) *hybrid aggression of Poland and Sweden, supported by the Vatican which had realized a plan of creation Polish-Lithuanian-Swedish superpower, partition of Russia and its subordination to the capital of papacy*.¹³

Former GRU analyst, Sergey Devatov¹⁴ perceives hybrid war foremost as a war between civilizations of the East and the West. Apart from the warfare he adds finance front (according to Devatov the worldwide finances are a main front of a hybrid war), semantic (war of narration), economic (fight for resources and technologies) and social front (education, culture and sports).

Finance, economic and trade wars were also of interest of Yuriy Bobylov¹⁵ what is reflected in his numerous blog posts and in traditional media. Intellectual efforts of this longtime employee of the Soviet secret Military and Industry Commission and, at present, a deputy rector of the Russian State Geological University and a member of the Russian International Relationships Council, is focused on bringing the hybrid information war experiences to other spheres of life (financial, economic, trade, innovations and technologies). According to him, it is the organizational capabilities

¹³ И. Панарин, *Гибридная война против России (1816–2016 гг)*, Москва 2016; А. Бартош, *Россия в эпоху гибридных войн*, http://nvo.ng.ru/gpolit/2017-10-20/1_970_hybrid.html [access: 10 XII 2017]. The same author: *Разведка России в противостоянии гибридным угрозам*, http://nvo.ng.ru/spforces/2017-10-06/1_968_scouting.html [access: 10 XII 2017].

¹⁴ <https://devyatov.su/articles/251-nebopolitika/29572-gibridnaja-vo-na-na-finansowom-fronte> [access: 5 I 2018].

¹⁵ <http://www.park.futurrussia.ru/extranet/blogs/Bobylov> [access: 5 I 2018].

of Russian intelligence services, i.e. executive potential working on the basis of the state and private partnership that have contributed to the effectiveness of information war.

Functional approach linking all the above ideas, is characterized by the form not the merit. It is characterized by the propaganda language, constant using key words like influence agent, the fifth column, colorful revolution. One can come across such approach in official statements of the Russian Federation officials which give the theory its practical sense. During the session of the Council of the Heads of Security Organizations of the Commonwealth of Independent States, CIS, of 19 December 2017 director of the Foreign Intelligence Service, Sergey Naryshkin, accusing the West of (...) *undeclared hybrid war against the CIS countries*, stated that (...) *the UK, Poland, Sweden and Baltic countries are in the vanguard of efforts to transform Russian emigration communities in the so called revolutionary ячейка*.¹⁶ This is also a current Kremlin political technologists and the so called opinion leaders approach to interpret the events according to a “Kremlin line”. Aleksei Pushkov, Head of the Federation Council committee on information policy and cooperation with the media, commenting in the pro government newspaper amendments to a bill on *Information, information technologies and security of information*, meaning that foreign media can be regarded as foreign agents (a symmetric Russian answer for making Russian media Russia Today and Sputnik to register in USA as foreign agents) had commented American move as (...) *information component of American hybrid war against Russia to restrict Russian influence on the course of events worldwide, undermining status and image of the Russian Federation*.¹⁷

Functional dimension of Russian considerations are shown in the last release of mentioned Igor Panarin¹⁸, professor of Diplomatic Academy by the Ministry of Foreign Affairs of the Russian Federation, a former KGB and Federal Agency of Government Communication and Information (FAPSI) analyst. This well known theorist of information wars (proponent and the main representative of information geopolitics) transformed terms and research assumptions used in the past in scope of the information war into a language of theory of hybrid war waged by the West against Russia. In fact, they have the same wide range of referents. A model

¹⁶ <http://www.interfax.ru/world/592442> [access: 20 XII 2017]; <http://www.mk.ru/politics/2017/12/19/naryshkin-na-zapade-iz-rossiyskikh-emigrantov-gotovyat-revolucionerov.html> [access: 20 XII 2017].

¹⁷ <http://rg.ru/interviews/3070.html> [access: 5 I 2018].

¹⁸ И. Панарин, *Гибридная война против России...*; the same author, *Гибридная война. Теория и практика*, Москва 2017. See also the same author: *Гладиаторы гибридной войны*, <http://ruspravda.info/Gladiator-i-gibridnoy-voyni-23791.html> [access: 5 I 2018]; *Гибридная война: прошлое, настоящее и будущее*, <http://новости.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B3%D0%B8%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0%D1%8F-%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0-%D0%B-F%D1%80%D0%BE%D1%88%D0%BB%D0%BE%D0%B5-%D0%BD%D0%B0%D1%81%D1%82%D0%BE%D1%8F%D1%89%D0%B5%D0%B5-%D0%B8-%D0%B1%D1%83%D0%B4%D1%83%D1%89%D0%B5%D0%B5-%D0%B8%D0%B3%D0%BE%D1%80%D1%8C-%D0%BF%D0%B0%D0%BD%D0%B0%D1%80%D0%B8%D0%BD/> [access: 5 I 2018].

of a country sovereignty defense by him (requiring enhancement of Russian information presence in all strategically important regions in the world) appeared useful in his considerations on counteracting Western technologies of hybrid war. In his own hybrid war definition, Panarin took under consideration current trends in discussions on the subject:

Hybrid war – is a set of military and force pressure, as well as political, diplomatic, information, psychological, and technical pressure together with technologies of colorful revolutions, terrorism, extremisms, special services activities and public diplomacy structures realized according to a plan by the state organs, military and political block or transnational corporations.¹⁹

According to the author the instruments of hybrid war are as follow: information operations, psychological operations, cyber attacks, economic sanctions, ethnic weapons, organization weapons, financial and information support of opposition and destructive activities of agents of influence located within public authorities. Panarin stresses also that the most important soldiers (gladiators) of this war are special services thanks to the tools they have.

Scientific and publishing activities of authors close to intelligence services confirm they active participation in a political war of Russia with the West.²⁰ It is a constant war. Hybrid non-military tools are the same that the one used in the Cold War and being described as active measures. The same tools are recalled in the context of information, psychological and economic wars. At present, as shows the above discussion, to describe them Russian theoreticians publicize the term hybrid technologies instead of the former information and psychological technologies or non-violent conflict solving technologies.²¹ Such change of terms does not change their substance: like former ones they give Russians the possibility of double use: as a constructive mobilization and optimization tool, and as a destructive “weapon” (conceptual, information). These, the so called wars, planned for a long time, require constant renewing of concepts and adjusting to up-to-date reality, mobilization of “soldiers” and training new generations of them. “Hybrid” approach has aroused

¹⁹ И. Панарин, *Гладиаторы гибридной войны...* [access: 5 I 2018].

²⁰ M. Galeotti, *Śłużby wywiadowcze Rosji są w stanie politycznej wojny*, <https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/PL/index.htm> [access: 5 I 2018].

²¹ See for example: А.В., Манойло, *Технологии несилового разрешения конфликтов*, Москва 2014. Currently there are many synonym words are used like *support measures* or *special influence measures*. They have appeared already in the War Doctrine and in the Doctrine of Information Security of 2000; in further texts they have been replaced with the following terms: non-military measures, indirect activities, i.e. subversion, sabotage, organization of irregular military formations, information influence, information and psychological impact, information and technical impact. In the last version of the War Doctrine of December 2014 there was additional term introduced information technologies. It was introduced also into a new edition of the Doctrine of Information Security of December 2016.

a new wave of interest in cold war, there are more and more voices that it had never stopped. It leads to a new ideologization of Russian aggression against Ukraine or in Syria – as a Russian “just” war against the US and NATO. Because of that, stressing the role of law enforcement and intelligence as having mandate and means to fight colorful revolutions – the most important technology of confrontation between the West and Russia, is an important element of current Russian narrative. Such “hybrid” narrative has not become a symbol of a contemporary thinking and acting, on the contrary, it leads to tested methods from the past.

History: active measures as a hybrid strategy

Active measures is a term as much multidimensional as hybrid technologies. This historical term is a kind of facade that covers different forms of influence always dominated by disinformation and special propaganda. They were carried out by different actors, mostly under the supervision of special services. The term appeared in 1960s when ideological struggle of the Soviet Union against the West was high as a complex term embracing such terms as disinformation, subversion, diversion, etc. to hide offensive activities presented as defensive. Active measures belonged both to intelligence and counterintelligence services. Their most comprehensive definition comes from *The counterintelligence vocabulary* (Moscow 1972)²², issued by the KGB Felix Dherzhinsky High School (Edited by W.F. Nikitchenko). Active measures term (*активные средства*) has been defined as:

(...) counterintelligence activities to realize what the opponent is up to, in order to be ahead of his unwelcome steps, to mislead them, to take the initiative, to foil their subversive actions. Active measures, unlike security measures regarding for example protecting confidentiality and state or military secrets, are of an offensive nature, allow for detection and breaking insurgent activities at an early stage, push the enemy to expose, allow to impose ones’ will on them, push to act in a hostile environment and in directions desired for counterintelligence. In practice of counterintelligence activities active measures are those activities which lead to creation of agent situations/positions within the opponent’s place or their close circle, operational games with the opponent, disinformation, disgrace and depravation, transfer to the USSR of people of particular operational value, gaining intelligence and so on.

Intelligence definition of active measures gave a former senior archivist for the Soviet Union’s Foreign Intelligence Service, the First Chief Directorate of the KGB, Vasili Mitrokhin, paying attention to their political, economic, military and ideological dimension. He claimed that in the foreign intelligence of the KGB they were defined as:

²² *Контрразведывательный словарь*, Москва 1972, pp. 161–162, <http://www.kgbdocuments.eu/index.php?1442843474>; <https://docviewer.yandex.com/?url=ya-disk-public%3A%2F%2FfAl-GUq9IcULWRmqEoOAPcEXoJ1HxKPkixIzbR4mngdg%3D&arc> [access: 15 VI 2017].

(...) operational activities with the use of agents to influence internal and external policy of third countries in the interest of the Soviet Union, other socialist countries, worldwide communism and national and liberation movements; to weaken political, military, economic and ideological position of capitalism; to sabotage its aggressive plans in order to create favorable conditions for a successful Soviet Union's foreign policy and to secure peace and social development.²³

Both definitions have the same perception of active measures aims, i.e. influencing the opponent, disinformation, compromising and corrupting with intent to create favorable conditions for a successful Soviet Union's foreign policy. Disinformation is meant, in a very extensive way, as an influence with words but also as actions.

Special services played the most important role in performing these techniques, mainly because they had tools to formulate strategic goals and tasks of Kremlin, to indicate their outer operators and to finance them secretly. First Soviet disinformation office was created in 1923 within OGPU/NKVD (Joint State Political Directorate/The People's Commissariat for Internal Affairs). A separate cell for such activities was the "D" Unit ('disinformation') established in 1959 within the First Chief Directorate (Foreign Operations), transformed in time into the "A" Service ('active operations'). Similar structures were organized by the Main Intelligence Directorate (GRU), in which up to 1991 there had been operated the Seventh Directorate (special propaganda); the Chief Political Directorate of Army and Navy, as Oleg Demidov²⁴ writes, had also other branched structures for information war. This presented institutionalization of active measures indicated that different forms of influence were to be linked into a coordinated and planned process. Practice shows significant evolution of Kremlin's attitude to disinformation strategy as well: from words to actions and from soft methods to hard ones (from information and ideological subversion to hard subversion).

Active measures were a subject of detailed studies by western analysts, experts on psychological war performed by the USSR during the Cold War.²⁵ Limiting the subject, it was described at times as disinformation.²⁶ It was Vladimir Volkoff himself, a French writer, who elaborated an anthology of such kind of texts. In the introduction of the anthology he described disinformation as a "doctrine" (a system of thinking and acting), regarding deceiving as one of the techniques.²⁷ His comments to the texts show precisely goals, methods and measures used in Soviet operations of influence both the public as well as other countries politics. A source of knowledge on the topic is a rich literature translated into Polish by known KGB

²³ W. Mitrochin, *KGB Lexicon: The Soviet Intelligence Officer's Handbook*, London 2002, p. 13.

²⁴ О. Демидов, *Инфовойска России: к структуре нового типа?*, <http://vpoanalytics.com/2017/03/08/infovojska-rossii-k-strukture-novogo-tipa/> [access: 5 I 2018].

²⁵ С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnye-sovetskie-meropriyatiya-v-putinskoy-rossii> [access: 10 XI 2017].

²⁶ *Psychosocjotechnika. Dezinformacja – oręż wojny*, V. Volkoff (ed.), Komorów 1999.

²⁷ *Ibidem*, p. 11.

defectors (Yuri Bezmenov, Oleg Kalugin, Oleg Gordevsky, Anatoliy Golitsyn and others). Rare Russian works are, by its very nature, in more or less disguised way a mythopoeia. They serve as motivation for Russian services as the topic of Soviet active measures is secret in Russia nowadays.

History may occur helpful in identification and diagnosing secret mechanisms of current Russian operations. As Marek Świerczek²⁸ states:

While analyzing activities of contemporary Russian special services one should be aware of the fact that their *modus operandi* has been developed in the beginning of 1920s. It is back then revolutionary ideas and disinformation operations of offensive counterintelligence creators encountered the Okhrana achievements, which officers joined not only emerging intelligence within the Red Army, but also VCheKa and later GPU and OGPU. This is the reason why trying to understand contemporary Russian intelligence both on operational arena and as a foreign policy element requires a historical perspective. Only such perspective allows to understand operational instruments used in the past and to draw conclusions from the goals achieved by them.

The above cited text is an example of an excellent historical analysis of diversified tools used by Soviet services against the Second Polish Republic. To destabilize Polish country Soviet services used all accessible tools: from subversive, terrorist and quasi-military measures, a mass anti-Polish propaganda, both in Poland and in the western Europe, to backstage political actions. Destabilization techniques described by M. Świerczek lead to a conclusion that Russians do not use only one *modus operandi* but they adjust methods to goals. In view of this it is possible to identify some universal rules for Russian intelligence services. Such unchanging rule is for example looking for the adversary's weak points or sensitive subjects and using them afterwards to deepen divisions in society and to escalate the situation. Long-term influence is a universal rule (process of the Second Polish Republic decomposition had been going on for the whole period of its existence). Changing vectors in propaganda actions accompanying active activities stays unchangeable, although it was Russia that was an aggressor but Poland, according to the then propaganda and agitation, was presented as (...) *predator; grotesque bastard with an imperial syndrome, watchdog, Trojan horse of the West* and so on. *The above analysis, apart from already mentioned, allows to distinguish other organizational principles presented as follow.*

²⁸ M. Świerczek, *Wojna hybrydowa jako strategia polityczna. Próba analizy historycznej na przykładzie działań ZSRS wobec II RP*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-8/1323,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-16-9-2017.html> [access: 5 I 2018]. The same author: *Działania wobec Attachatu Wojskowego przy Poselstwie RP w Moskwie w początkach jego funkcjonowania jako egzemplifikacja kontrwywiadowczego modus operandi stosowanego przez służby rosyjskie*, <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-9/1384,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-17-9-2017.html> [access: 5 I 2018]; <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-1/1008,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-10-6-2014.html> [access: 5 I 2018]; <https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-3/1180,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-12-7-2015.html> [access: 5 I 2018].

Tab. 1. Rules used during covert operations (intelligence and organizational).

| Operational undertakings | Organizational principles |
|--|--|
| Mass propaganda action to Poles and minorities living in the then Kresy Wschodnie or Kresy (Polish Eastern Borderlands or Borderlands) and territories to the west | Transborder nature (exterritoriality) of information and propaganda activities |
| Transfer of provocateurs, saboteurs, agitators, spies | Secrecy and inspiration of an opponent |
| Inspiration to riots in the Polish Borderlands | Taking an opponent by surprise and their confusion |
| A series of bomb attacks in central Poland, for example on powder magazine in Warsaw Citadel | Emotional influence on an opponent's society |
| Influence on Polish political scene by the Communist party of Poland (KPRP), Belarusian Hramada, parties and parliamentary fractions in the Second Polish Republic | Using one's own resources as well as opponent's |
| Incitement of turmoil because of economic reasons | Complexity of methods of influence (political, economic, social, etc.) |
| Campaign of intimidation of Polish law enforcement (attempts on Police provocateurs) | Weakening of an opponent's morale |
| Treacherous assassinations, plan to murder Marshall Józef Piłsudski | The end justifies the means, rule |

Source: private study on the basis of: M. Świerczek, *Hybrid war as political strategy. Historical analysis attempt on the basis of USSR activities against the Second Polish Republic*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, No 16, pp. 81–97.

From the perspective of history, it may appear that Russian services have not abandoned methods used in the past. First task of the mentioned KGB Unit “D” was to compromise the Federal Republic of Germany as the land of neo-Nazism. There were agents from the East Germany transferred to the West Germany to profane Jewish tombs, paint anti-Semitic slogans on the walls of synagogues, shops and Jewish organizations head offices and to provoke indigenous people to similar acts. In 1959, as John Barron wrote²⁹, the authorities of the Federal Republic of Germany noted 833 anti-Semitic acts, which was condemned worldwide and undermined the image of the country. It is hard not to see similar situation as far as “monuments wars” are concerned. They turn instantly in anti-Polish, anti-Ukrainian, anti-Lithuanian, anti-Latvian, anti-Estonian demonstrations.

²⁹ Cited from: V. Volkoff, *Psychosocjotechnika. Dezinformacja...*, p. 130.

There are many more examples. Nevertheless, it is worth noting that tested mechanisms from the past are bested, diversified, adjusted to current realities and needs. An example of this is the evolution of simulated groups (groups of undercover agents and officers). The first time when such a group was used, as professor Igor Halagid³⁰ writes, in 1918 in an operation known as the so called Lockhart plot (alleged conspirators were CheKa agents who came forward to a British diplomat). That provocation was used by Felix Dzerzhinsky as an argument against western diplomacy which tried to carry out a coup d'état in the USSR. The attempts were widely publicized domestically and abroad. Simulated groups organization (as fabricated independence movement structures and anti-regime) were brought to perfect during the World War II, using them for liquidation anti-Communist communities on the occupied territories (Ukraine, Belarus, Lithuania, Latvia, Estonia and others) and just after the end of WWII – for liquidation anti-Communist underground in countries of the Eastern Block. At present simulated groups appear in places of conflicts (for example in eastern Ukraine or during unsuccessful coup in Montenegro in 2016) in various forms: private military companies, Cossacks organizations, self-defense troops, youth combats or extremist groups, volunteers, special forces without any ranks, etc.

Secret hybrid technologies as intelligence threat

Intelligence operations called hybrid technologies or active measures are not typical intelligence activities because they have nothing to do with information gathering and analysis – they serve Russian foreign, economic and defense policy. Generally, they stand out from the “classic” intelligence activities by their creative nature.³¹ While the first ones apply to decision making after something happens, the second are something is to happen. It is – as A. Bartosz³² explains – to project and create the enemy's future.

New reality and, first of all, abandoning rigid communist ideology after the collapse of the USSR, as well as impetuous social and economic changes widened possibilities of Russian services domestically and abroad. Intelligence service, subordinated directly to the president, performed from the very beginning in the sense of purposefulness. It was guaranteed by the *Law on Foreign Intelligence Organs* adopted in August 1992 and written by the Foreign Intelligence Service. It stipulated that “*career personnel may occupy positions in ministries, departments, establishments, enterprises and organizations in accordance with the requirements of this law without*

³⁰ <http://polska1918-89.pl/pdf/miedzy-dezinformacja-a-rzeczywistoscia.-prowokacyjne-dzialania-sluzb-k,5366.pdf> [access: 5 I 2018].

³¹ In Anglo-Saxon vocabulary such undertakings are defined as *covert actions*. See: M. Herman, *Potega wywiadu*, Warszawa 2002, pp. 61–62. Mirosław Minkina calls them non-inforamtion operations of intelligence forces, See: M. Minkina, *Sztuka wywiadu we współczesnym świecie*, Warszawa 2014, pp. 209–245.

³² А. Бартош, *Гибридная война...*, ibidem.

compromising their association with foreign intelligence agencies. If, during the KGB times, the intelligence had been based in foreign posts under diplomatic cover and in recognized western posts (representative offices of Aeroflot Airlines, dealerships, foreign correspondents' offices), from the time of the Act they could act under cover any political, economic or social organization. The possibilities have been widened by the Russian-speaking diaspora scattered in all post-USSR countries.

New technology development, i.e. new information and communication techniques, common use of computers, growing dependence on IT infrastructure also favored Russian services. It makes information gathering easier but also facilitates manipulations.

Traditionally in their struggle for information (knowledge) Russian strategic intelligence shows a tendency to broaden activities in different areas: political, economic, social, science and technology, sociological, cultural and military. This struggle for information in Russian intelligence doctrine and strategic assumptions has been quickly transformed into information struggle (or more precisely – disinformation) in the areas relevant to intelligence activities. It suffices to recall that the term *information struggle* appeared in the West only in the middle of 1990s and almost immediately it has been implemented in Russian official documents (it already occurred in *Security Information Doctrine* and *Military Doctrine of 2000*). Long tradition of information and psychological measures and current experiences of the two Chechen wars as well as NATO and the European Union enlargement being a challenge, have also favored. They were accompanied by very dynamic information campaigns. It does not come as a surprise that most Russian theorists stress this particular role of information tools on all stages of hybrid operations (as a passive measure – from monitoring course of events to look for inconsistencies and splits in the attacked countries, by planning and choosing executors to its accomplishment and the so called media coverage).

In this context, as J. Bobylov states, creation of mobilization nets of information cannot be overstated (and the underlying intelligence mechanism, public – private partnership and competence building like analytical and executive personnel able to act autonomously), which should be a model pattern for “hybrid activities” in other areas: economic, financial, business and industrial innovations.³³ Stressing a particular role

³³ Ю. Бобылов, *Экспортно-ориентированные инновационные промышленные прорывы России по стратегиям гибридных войн*, «Информационные войны» 2015, No 1, pp. 55–61. Of particular interest are the articles of the same author, *Спецслужбы и стратегия гибридных войн*, www.rusnor.org/pubs/articles/12200.htm [access: 5 I 2018]; *Проблема внешней ведомственной конкурентной разведки России. Информационные, правовые и организационные аспекты*, «Информационные войны» 2016, No 4, pp. 67–79; *Новые наукоемкие гибридные войны*, <http://www.proatom.ru/modules.php?name=News&file=print&sid=7397> [access: 5 I 2018]. According to the author current economic reality worldwide are kind of a new mobilization challenge for Russia: to build adequate structures of governing the country and mobilization economic net using covert technologies of secret services and with an active participation of secret services and different private entities, including criminal world. In this context it is

of intelligence³⁴ Bobylov distinguishes special operations (performed by intelligence services) and special projects (in which intelligence services are involved). Following special operations he gives the following characteristics:

- destructive nature (liquidation or weakening of the opponent is a goal),
- secrecy and inspiration (secret activities can be either lawful or unlawful),
- lack of dimensional restraints/limits,
- using indigenous people and foreign nationals,
- comprehensiveness („the end justifies the means” rule),
- wide range of methods on different levels of problem solution,
- special executive structure (using both permanent resources as well as one-time organizations, created only for a single action),
- special material security (including financial),
- special procedure of operation management: their independence and anonymity require responsibility delegation from the decision – making center to executive structures,
- variety of methods depending on the goal,
- concentrating on the opponent’s weak points (vulnerabilities),
- surprise and confusion of the opponent,
- planning,
- unlimited use of resources by priority tasks solution,
- information and psychological struggle along with special operations.

It is very difficult to find in Russian literature information on executive measures necessary to perform special operations and special projects. Which is not surprising, no intelligence service nor Kremlin disclose their active role in such kind of operations and projects. Historical research into active measures as well as studies of contemporary mechanisms of disinformation spreading show that they are used by many different entities. They can be divided into two categories: state entities and non-state entities – intermediary (at present called “proxy”). They have been shown in tab. 2.

proposed that separate structures in public institutions, businesses, strategic companies and private concerns, the so called three (dealing with economic security) equivalent to the one (a cell for state secrecy protection and information security in a broad sense) and the two (for mobilization and crisis management). This is an indication of the attachment of Russian theoreticians to old Soviet bureaucratic solutions.

³⁴ Its subsidiary role stresses also the Russian intelligence. According to a one defector from the Foreign Intelligence Service of the Russian Federation Sergey Tretjakov after KGB transformation Service „A” was transformed into Service „MS” (*Russ. mieroprijatija sodiejstwija – ‘means of support’, read: support of Kremlin*). See: P. Earley, *Towarzysz J. Tajemnice szefa rosyjskiej siatki szpiegowskiej w Stanach Zjednoczonych po zimnej wojnie*, Poznań 2008, pp. 184–185.

Tab. 2. Subjects to operations and special projects.

| State entities | Instrumentalized entities (proxy) |
|---|--|
| Intelligence services of the Russian Federation | Associations created by former military officers and functionaries |
| Functionaries of other law enforcement agencies and Ministry of Foreign Affairs | Quasi-military groups (Cossacks, combat sports clubs, Night Wolves) |
| State administration workers of different levels | Orthodox church |
| Diplomatic personnel on Russian diplomatic posts | Russian third sector organizations (like CIS EMO – public diplomacy) |
| Personnel of the Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation (Rossotrudnichestvo) | Russian-speaking diaspora |
| State foundations like Russkiy Mir Foundation | International foundations (sponsored by oligarchs, for example Vladimir Yakunin, Konstantin Malofeev) |
| Security services of state concerns (Gazprom, Rosneft, Rosatom) | Security services of private concerns |
| State analytical centres | „Independent” analytical centers gathering theorists and practitioners |
| Associations sponsored by the state (Russian Geographical Society, Military Historical Society) | Criminal groups members), corrupt businessmen |
| Cultural associations, friendship and cooperation societies | Subversion troops acting commercially (for example Wagner’s private military company or in social networks (trolling and factories of trolls) |
| System political parties (for example Liberal Democratic Party of Russia led by Vladimir Zhirinovsky) | Nationalist and extremist organizations as well as youth affiliations to such organizations |
| State media (including Rossiya Segodnya) | Oligarchs’ media (for example Katehon by Malofeev or British “The Independent” and “The Evening Standard”, controlled by Alexandr and Yevgeni Lebedev) |

Source: private study.

Subjects mentioned in the table are treated by Russian theorists as the so called “own resources”. Non-state entities are to join organizational “mobilization networks” as their autonomous elements managed in a particular way. Separate group of entities is made up of those which belong to intelligence assets of Russia abroad. These are

illegals, agents in countries of operational interest, unaware agents called also “useful idiots”, the so called friends of Russia in the West (corrupt politicians and businessmen, networks of people understanding Russia (political parties, ecologists, anti-globalists, pacifists) and others requiring more detailed research. Naturally, stressing by Russians themselves operational capabilities and the role of non-state domestic and international actors as “Russian soft power” makes it to raise a question whether it is not a part of any disinformation operations. In this context, more important appears to be precise indication of different influence centers of Russia, which also play a role of recruitment centers³⁵. It makes it also easier to precise goals and to identify more precisely the areas threatened by Russian activities³⁶.

Current hybrid technologies: conceptual and organizational basis/grounds

Active measures, which have been changed hybrid technologies, were a subject of a thorough research in the West during the Cold War. Much successful in this field was interdepartmental commission for tackling them by the US State Department acting between 1981 and 1992 under the leadership of vice secretary of the state Dennis Kux. Experts of the commission as well as its members were preparing cyclical reports on Soviet activities. It was Kux himself who tried to classify those diverse instruments by dividing them according to intelligence sources typology into white, grey and black. Perpetration and responsibility for activities in a white area (overt activities, lawful) and in a grey area (with the use of semi-lawful methods, under different kinds of cover) he assigned to Kremlin, and activities in a black area with the use of intelligence technical and personal methods were assigned to the KGB.

This division, as one may think, is very up-to-date despite the fact that Russia has abandoned the idea of changing the world according to ideological preferences, which was initial reason for active measures in the Cold War times. The doctrine model, which is to justify present actions, is as much inflexible; it is based on the setting the Russian world against the West because of the civilization disparity of „Russian world” sometimes widened to „Eurasian world”. Narration based on the so called geopolitical scientific outlook is at the same time very simplified which was shown by the pseudo-intellectual base of the projects and hybrid operations at the beginning of this paper. The narration is also free from the system of values which had not been described by Russia until now. The narration comes down therefore to undermine others’ values. The narrative is determined also by geopolitics: USA and NATO have become „absolute enemies” that tend to challenge Russia’s position as significant point of strength in the world, taking advantage of Russia’s trust and constant humiliating

³⁵ Such recruitment under foreign flag carry out also citizens of other countries, what was confirmed by the example of a citizen of Belarus, Alexandr Usovsky. See for example: P. Reszka, M. Tomaszewicz, *Jak Kreml finansował skrajną prawicę w Polsce?*, <http://www.newsweek.pl/polska/polityka/jak-kreml-finansowal-skraina-prawice-w-polsce-artykuly,408023,1.html> [access: 8 I 2018].

³⁶ See: J. Darczewska, P. Żochowski, *Środki aktywne...*, ibidem, pp. 63–68.

the country by shaping the world by colorful revolutions. Competition between Russia and the USA and NATO has become a universal argument for domestic politics (creating the illusion of constant threat and omnipresent anti-Russian hysteria and Russophobia) as well as foreign politics. Undermining others' values (like for example Georgia and Ukraine sovereign right to determine their own ways of development and establishing alliances) as well as fight for widening their influence zone, Russia presents it as an act of defending its sovereignty and a mirror answer to a cynical game of the West. Such way of thinking has become a basis for thinking and acting of the Russian Federation and its law enforcement institutions. It is treated as an effective „conceptual weapon”.

As far as organizational basis and organizational weapon are concerned, their substance is a social systems management, including mechanisms of their self-organization, and organization of special projects with the use of different entities described above. In theory, it is described as a paradigm of „reflective management”.³⁷ It is clear that modelling the adversary's social behaviors requires a very meticulous research and knowledge provided by intelligence. According to Igor Eydman³⁸, sociologist, intelligence services are admittedly the most important but only one of many executive entities and recruitment centers. Highly developed organizational system resembles a pyramid with President Putin on top of it making all strategic decisions. His instructions are realized by the President's Administration (for example its vice chief Aleksey Gromov supervising media concern, including Russia Today broadcast and Sputnik agency, i.e. all the propaganda issues directed to organizing „Russia's friends” abroad). Individual advisers to president supervise the Ministry of Foreign Affairs and law enforcement institutions. These *sui generis* „command posts” within the president's administration are then active through huge concerns, social associations, international foundations, individual oligarchs, and so on. Thus the conclusion is that, in the end, it is Kremlin that mobilizes and gives the signal to start or end hybrid wars.

What is new about the topic is that new technologies and new channels of communication are used which have significantly widened possibilities of Russia in this respect. Internet lifted former communication barriers, allowed access to information online and thus enabled services to gain information on the subject. Development of the so called new media (traditional media online and social media) has created possibilities of immediate spreading of false information (issuing the information all over the world, replicate them, getting rid of unnecessary information, imposing one's own interpretations), giving, at the same time, anonymity to senders and access to recipients without intermediaries. It also got the possibilities to „whiten”

³⁷ More on the topic see: M. Wojnowski, „Zarządzanie refleksyjne” jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w., „Przegląd Bezpieczeństwa Wewnętrznego” 2015, No 12, pp. 11–36; the same author: *Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, No 17, pp. 11–55.

³⁸ И. Эйдман, *Первая мировая гибридная война*, <http://www.kasparov.ru/material.php?id=59D27ACA13CFD>; <http://www.aravot-ru.am/2017/10/05/252828> [access: 5 I 2018].

disinformation: while looking for confirmation of a given information recipient gets it from a few others sources being disinformation as well. Nowadays, it is possible do deliver disinformation not only to humans but also to machines, i.e. bad (harmful) bots managing the traffic on the network and direct it to an aggressor's information website by changing their positions they rank among search engines (so called good bots). In the result, global network has delivered inboxes with new tools what makes current problems with Russia's aggressive foreign policy only an enhanced version of the old problems.

Looking at studies carried out during the Cold War and bearing in mind new elements, reinvented arsenal of active measures, i.e. hybrid technologies – according to current terminology – can be presented as follow (tab. 3).

Tab. 3. Current arsenal of hybrid technologies.

| Type | Organizational undertakings |
|---|---|
| BLACK (coordinated by special services) | <ul style="list-style-type: none"> – getting agents of influence and preparing unaware people for gaining aims of Russia – assassination and terrorism – fabrication of documents (false documents, fakes) – diversionary groups to perform acts of provocation (devastating monuments, memorial sites) – quasi-military actions: subversion, secret limited violence) – inspirations for demonstrations and riots – bribing, corruption and blackmailing politicians – creating false inboxes and botnets to carry out cyber attacks, propaganda 2.0. and cyber propaganda |
| GREY (coordinated by Kremlin) | <ul style="list-style-type: none"> – instrumentalization and inspiring of different social groups, including political parties and extreme organizations – activities via Russian non-governmental sector and international organizations under control, – instrumentalization of Russian foundations and associations, e.g. Russkiy Mir Foundation, Russian Historic Association – opening pro-Russia portals and financing them – troll factories and pro-Kremlin networks creation – trolling and activities in social networks |

| | |
|--------------------------------|---|
| WHITE (coordinated by Kremlin) | <ul style="list-style-type: none"> – propaganda actions led via state information multimedia agencies (Russia Today, Sputnik Radio, RIA Novosti) – undertakings performed via branches of Rossodruzhestvo, Russian culture and science centers by Russian embassies, other executive and legislative organs (Commission for Russian Sovereignty Defense by the Federation Council) – organization of cultural and scientific events (conferences, exhibitions, memory rallies, scholarships, language courses) |
|--------------------------------|---|

Source: private study on the basis of D. Kux *Soviet Active Measures and Disinformation: Overview and Assessment*, “Parameters, Journal of the US Army War College” (Winter 1985). After: С. Абрамс, *Больше, чем пропаганда: активные советские мероприятия в путинской России*, <http://connections-qj.org/ru/article/bolshe-chem-propaganda-aktivnyye-sovetskie-meropriyatiya-v-putinskoy-rossii> [access: 29 XII 2017].

Finally, it is worth to stress once again, that hybrid technologies, known previously as active measures, rooted in tradition and in political as well as in strategic culture of Russia, were of different nature: from ordinary propaganda and disinformation based on frauds to political assassinations and political terrorism. Between them there is a wide grey zone. That zone is a major theatre of Russia’s confrontation with the West aimed at destruction of foundations of the attacked country (administrative, political, social, economic, cultural, etc.). The zone itself is a rather poorly studied area going beyond analyses because of secret and semi-lawful nature of activities (therefore lack of hard facts), lack of proper tools to measure their scale and devastation also because of numerous and diverse intermediaries.

Summary. Complex nature of Russian threat

Russia’s activities fit into current security situation, which is characterized by growing significance of non-military threats (just under conventional wars threshold), variability and unpredictability. In NATO strategies they are named *hybrid threats* based within defense area, which does not make it easier to understand their complexity and to counteract them. Described above activities by Russian special services and other „civil” entities are very far from straightforward military dimension so counteracting by military methods is not sufficient. Because of their backstage nature they should be treated as intelligence threats from security area.

Historical term active measures reflects in a very good manner cross-sectoral nature of Russian threat. Most techniques of Russian confrontation with external environment are of indirect character and as such are very hard to reach. Their goal is to reach strategic interests and to strengthen international position of Russia and „to disarm” opponents, i.e. to create such situation that domestic actors will be capable of realizing aims of Russia foreign policy. Making use of weak

resistance and hurdles in threats identification, Russia tends to destabilize situation in attacked countries, influences in a destructive way their administrative and decision-making structures, undermines their social and economic foundations as well as cultural background (ideology, system of values, political culture, rule of law). The threat is both internal as well as external, domestic and transnational, to which it cannot be responded symmetrically. Disruptive activities are performed by state and non-state entities, both covertly and openly, lawfully and unlawfully. This is a constant process based on integrated state activity on multiple fronts with the use of different channels (diplomatic, political, economic, military, social, media) subordinated to the long-term strategy of support for Kremlin's politics.

Strategic narration imposed by Russia blurs boundaries between war and peace, between offensive and defensive activities. Its major goal is to shape the picture of Russia as a victim of cynical play by the West and imposing opinions that it is a war between two parties using the same and adequate measures. Meanwhile, the situation is of asymmetrical nature: the attacked party will be able to assess destruction scale until after its effects. Because long-term goals of Russian foreign policy take into account revision of the present international security system, in the mid-term perspective it should be expected that intensity and scope of activities against NATO and EU member countries will not diminish. Systematic widening of conceptual and executive background as well as including forces and military measures in the so called influence arsenal prove it. It means that crisis-building role of Russian threat will be increasing and its effective repulse will require increased attention of security and defense entities involved and more intensive studies concerning Russian organizational projects, their conceptual assumptions, new techniques of influence, corrupt methods of financing and inventing procedures to quickly and effectively neutralize them. It will allow to avoid thinking that aggressor is schematic: it is a must to be prepared for new, yet unknown, methods of political confrontation.

Abstract

The subject of active measures as elements of hybrid activities strategy has been raised in the article. According to the author historical perspective is useful in recognizing and detecting current operations of Russian special services. Such analytical frameworks of terms make it easier to show some generalizations, they also lead to the conclusion that the activities being a clue of described terms are of constant and complex nature.

Active measures and hybrid technology appearing in the title of the article have the same scope of designates and are collective terms embracing different instruments for political, military, intelligence, business, diplomatic, me-

dia, economic, social and cyber influence to realize long-term goals of the Kremlin policy. Naturally, counteracting Russian threats requires just as complex approach.

Keywords: active measures, hybrid war, threats, intelligence, disinformation-subversive operations, covert action.

Danuta Gibas-Krzak

Russian concept of the Eurasian Aerospace Defense System. Analysis of the problem

The goal of this article is to present possibilities of creation of the Eurasian System of Aerospace Defense as a main direction in development of Eurasian integration under Russian Federation leadership and presenting the most important geopolitical role of Eurasia in contemporary international relations. Conclusions and interpretations coming from the works of professor Aleksey Podberezkin, a scientist from the National Institute of International Relationships by the Ministry of Foreign Affairs in Moscow are a starting point for the analysis. He is an esteemed scientist, adviser to the President of Russian Federation and author of some works on security and international relations (inter alia: Алексей Иванович Подберезкин, Евразийская воздушно-космическая оборона, Москва 2013). In 2017 he issued a two-volume piece on current military politics of the Russian Federation Современная военная политика России: учебно-методический комплекс (Москва 2017).

Geopolitical importance of Eurasia

Zbigniew Brzeziński pointed out in his paper of 1990, *Great Chessboard*, the importance of Eurasia. He was stressing military and political phenomenon of that region showed there as a giant chessboard, on which there was a struggle for worldwide hegemony going on. Nevertheless, it was only in 1904 that the great importance of the region was noticed by a British geographer, Halgord John Mackinder. He claimed that the one who rules the so called „World Island”¹, rules the world because this was a region where the most important events for the human mankind take place. In other words – this is where the history was going on. Central point of *the world island* is Eurasia and Heartland as a part of it (in its northern and central part). According to this theory, the supervision over Heartland guarantees power over the world. H.J.Mackinder agreed that its borders cannot be clearly established. He himself changed its range many times, once limiting it to the territory of Russia, next time stretching it to Mongolia.²

The assumptions mentioned earlier had a serious impact on Russian political environment which resulted in one of the most important Russian geopolitical concepts during the times of the USSR – Eurasia concept. It refers not only to ideology

¹ „World Island” embraces continental mass which is comprised of Europe, Asia and Africa. The other areas, South and North America, Australia and Malayan Archipelago are satellites of the “World Island” and play a minor role. See: A. Cianciara, *Klasyczne koncepcje geopolityczne*, in: *Geopolityka*, A. Dybczyński (scientific editor), Warszawa 2013, pp. 59–61.

² Ibidem.

but it is also meant as an original mental movement that was stressing uniqueness of Russian history and culture treated as a separate civilization. It has become a basis for the statement that Eurasia concept is the key to a secret of Russian soul.³ According to the Eurasia concept Russia's supporters are not Asia nor Europe, and it should be treated as a separate geographical unit, since it is a region development of which was influenced by ethnic specific of Great Russ' people. It was assumed that the area of Eurasia is the same as the area of Russia. Eurasians were reluctant to the West, and their task was to prove that Russia has the right to civilization and cultural distinctness. Piotr Sawicki kept stressing that Russian civilization was called to play unique role within the Old World (Asia and Europe), in the sense of keeping its unity.⁴ In this sense Russia should continue geopolitical traditions of the Mongol Empire what was explained by the fact that Russia's pressure on Scandinavia, Poland, Persia and Turkey replaced raids of nomads on the continental and oceanic zone.⁵

Many scientists recall that after the USSR had collapsed Eurasia concept became the most influential orientation in Russian geopolitics. It was reborn in a doctrinal form of Neoeurasia idea with Aleksandr Dugin as its main representative. In this concept the West (primarily the US) is regarded as enemy, as well as the Atlanticism concept.⁶ A. Dugin recognized cultural and geographical individuality of Eurasia, nevertheless, in his theories Eurasian empire stretches to Central Africa. According to this ideology Russia was to create alliance with China, India and Iran (even Iraq and Tibet are also mentioned) against Anglo-Saxon world. Together they would take actions against mortal enemy, as the West with the USA, because of the belief that American version of liberalism poses a threat to Russia and the whole planet. Europe and pro-Western countries of the Eastern Asia with Japan to lead the way, were to be included finally in the Eurasia alliance.⁷

It is also worth mentioning that in 1997 Vladimir Hatchaturov presented a very interesting geopolitical concept which was paying attention to the following four determinants of the world order:

- 1) geographical area occupied by China and India is the geopolitical center of the world,
- 2) global geopolitical processes are initiated by the geopolitical center of the world,
- 3) in the course of global geopolitical processes there are two poles emerging: stable, embracing geopolitical center of the world, and unstable,
- 4) together with any change in the area of even one of the poles the world enters the period of geopolitical instability (global wars and revolutions).

³ R. Paradowski, *Eurazjatyckie imperium Rosji. Studium idei*, Toruń 2001, pp. 38–39.

⁴ J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, p. 113 et seq.

⁵ Ibidem.

⁶ I. Massaka, *Eurazjatyzm. Z dziejów rosyjskiego misjonizmu*, Wrocław 2001, pp. 175–194. Atlanticism is one of the streams in current Russian geopolitics referring to traditions of Russian Westernizer movement, main Assumption of which was to link Russian prosperity with its cooperation with the West. See: J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej...*, p. 38.

⁷ T. Klin, *Geopolityka pozimnowojenna*, in: *Geopolityka...*, p. 253.

As one can see, according to these assumptions, Russia is perceived as a part of both stable and unstable pole, and because of that it plays a role of geopolitical axis of the world. According to V. Hatchaturov the aim of the Russian politics should be to enhance the significance of the axis by reintegration of the country and building strong ties and relations with China and India.⁸

Renaissance of geopolitical programs caused the significant influence on the whole international community in the second half of the 20th century what is associated with reorientation of forces in the present system as a follow up to changes in American foreign politics. It regards foremost political situation in Central and South-Eastern Asia. We cannot deny that there is much increase in instabilities in some countries and regions of the world, particularly in the area of Eurasia, where ca. 90% of military conflicts during the last few decades took place. This is a reason why it is so important to take complex actions towards a complex defense in this region, along with the Heartland paradigm which seems exceptionally influential in current strategic relations, especially with regard to current politics of the Russian Federation. According to Russian analysts:

Post Soviet Central Asia in Washington's foreign policy has gone from a third-rate attention in Russia to one of the most important points of American interests worldwide. Predicted complication of Afghan problems will entail an increase of the US, Russia and China interest in this region. In this respect, conflict of interest in the region is possible.⁹

In this area, it is worth noting that military and political attributes of Eurasia have become an underlying cause for the aggravation of confrontation in the region in the second half of the 21st century. These attributes are reflected primarily in the following:

- special geopolitical, economic and historic role of Eurasia worldwide, which is to grow rapidly in the coming decade. And not only because of a rapid pace of China's, India's or other countries development but also because of numerous civilization and geopolitical contradictions cumulated for the past decades;
- growing role of Russia in Eurasia, which can be the main player on the continent and influences of which are totally inadequate to the role it wished to play, especially in the regions east of the Ural mountains with a huge potential and transportation routes of global importance;
- concentration of reserves, (...) *not only energy but also agriculture, water, forest. A tremendous human potential in Eurasia, which quality indicator has been*

⁸ Z. Lach, J. Skrzypl, *Geopolityka i geostrategia*, Warszawa 2007, pp. 56–57.

⁹ А.А. Казанцев, *Политика США в постсоветской Центральной Азии: характер и перспективы*, <http://ehd.mgimo.ru/IORManagerMgimo/file?id=E3DAB956-8956-310D-0D4C-2235B2392202> [access: 3 I 2018].

*growing very fast, will start unavoidably play a key role in a global development. It is only in China during reforms time that over 300 million of people got higher education*¹⁰;

- some independence from „maritime countries”- former world leaders – which can be taken away only with strategic offence and defense potentials development.¹¹

Programmed grounds for the Eurasian System of Aerospace Defense

Research done by A. Podberezkin, when there still remains an up-to-date conflict between Moscow and Washington, Moscow and the European Union, allow to see another perspective in activities within international security area and to define the role of Russia on this „Asian chessboard”. Indeed, the process of NATO enlargement to the east after the Cold War ended, transformed the alliance from the regional organization into a global organization, including whole Eurasia region in its scope of responsibility area. The course of events in Iraq, Afghanistan, its approach to Syria and Iran proved that NATO as military and political coalition is the one and only real international power to ensure security to Eurasia. Nevertheless, the alternative for its potential can be the Shanghai Cooperation Organization¹² and the Collective Security Treaty Organization within the Commonwealth of Independent States (CIS), which is a tool of post Soviet area integration in a military and defense sense.

In the Shanghai Cooperation Organization it is China and Russia that play predominant role, although China is the leader in economy and Russia offers foremost political and military cooperation to other members of the organization.¹³ What is more, Russians and Chinese are ready to support financially independence of other members of the organization from the West. Russia is very interested in enhancing this organization as a tool in its global competition with the US so that the Shanghai Cooperation Organization was a political counterbalance to Western countries.¹⁴

These activities are supported by research done by scientists from the National Institute of International Relations in Moscow (Московский государственный институт международных отношений, MGIMO), including A. Podberezkin, who

¹⁰ А.И. Подберезкин, *Евразийская воздушно-космическая оборона*, Москва 2013, p. 25.

¹¹ Ibidem. This problem refers to a geopolitical theory, according to which the most important significance to the World history does not have Heartland but a broad strip of peninsulas (Rimland) surrounding Heartland. It has an important role in geopolitical theories by Nicholas John Spykman, according to him Rimland is the centre of the world’s power. Within the boundaries of Rimland there are continental Europe, the Middle East, India, China and Indo-Chinese Peninsula, Malay Peninsula and Korean peninsula. See: N.J. Spykman, *The geography of the peace*, New York 1944, pp. 36–40.

¹² Ł. Firmanty, *Szanghajaska Organizacja Współpracy jako element polityki bezpieczeństwa Chińskiej Republiki Ludowej*, in: *Badania wschodnie. Polityka wewnętrzna i międzynarodowa*, W. Baluk, Z.J. Winnicki (ed.), Wrocław 2008, pp. 236–237.

¹³ M. de Haas, *Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization*, „The Journal of Slavic Military Studies” 2017, No 1, pp. 1–2.

¹⁴ Ł. Firmanty, *Szanghajaska Organizacja Współpracy...*, pp. 236–237.

is one of numerous supporters of more active politics based on Eurasian ideas with Russia playing the main role. The actions taken are strategic and were expressed by establishing in December 2011 Russian Aerospace Defense Forces as a new armed force to defense aerial and space security of Russia¹⁵. During the summit of the Commonwealth of Independent States in December 2012 in Ashgabat not only economic projects were discussed but establishing the joint air defense system. For this purpose a special coordination committee was established. Russian proposal to integrate Russian units with sub-units of Russian Aerospace Defense Forces Branch (from 2015 Russian Aerospace Forces) in the frame of the above initiative was supported. It can be called the first step to create Eurasian Aerospace Defense Forces.

Establishing a few military forces centers in Eurasia is to gain potentials of strategic offensive weapon, and foremost aerial and space precision-guided component of different purpose.¹⁶ Works on Eurasian Aerospace Defense Forces are Russia's assertive step to assume responsibility for Eurasia security in a concern of NATO and the USA domination in this region. Main thoughts of A. Podberezkin's paper establish a paradigm of common security, what is particularly interesting in view of the growing threats in modern world, to be – at the same time – an answer for anti-Russian (according to Russian analysts) plans and aims of NATO.

At present, the problem of North Korea seems to be particularly dangerous, because of nuclear tests done by the country, what raises the risk of pushing the Peninsula into a war. And this would definitively cause American intervention in the area. Possible results of any conflict with the superpower are even hard to predict. According to some research by Russian analysts one can be concluded: Russia is afraid of American domination in Eurasia. According to A. Podberezkin it is obvious that the US continues to seek obstruction to renewal of Russia's strategic presence in the region and political alliance between Moscow, Beijing and Tehran. It is also not insignificant that Central Asia is for the US geopolitically important bridgehead in the region in case of an eventual confrontation with China and Russia. These ideas go along with a maritime doctrine of the Russian Federation of 2015. Basic thought of the new doctrine was given in point 52 of the document: *the main unacceptable for the Russian Federation element in relations with NATO are its plans to move military infrastructure and facilities towards its borders and attempts to grant the alliance global functions*.¹⁷ The doctrine has got two dimensions, global – addressed mainly to the US and European – addressed to NATO. This thought can be perceived as a message for military decision-makers in the US and NATO that Russian Federation will not allow American dominance on a global scale.¹⁸ It is worth noting that other

¹⁵ On February 5, 2006 the idea of formation until 2016 was authorized. See: M. Depczyński, *Rosyjskie Siły Zbrojne. Od Milutina do Putina*, Warszawa 2015, p. 240.

¹⁶ А.И. Подберезкин, *Евразийская воздушно-космическая...*, pp. 50–51 et seq.

¹⁷ J. Symonides, *Nowa doktryna morska Federacji Rosyjskiej*, „Kwartalnik Bellona” 2016, No 1, p. 13.

¹⁸ *Ibidem*.

strategic documents of the Russian Federation are of the same meaning, for example updated Strategy of Security or Defense Doctrine of 2010. Basic priorities concerning security, i.e. political and economic internal threats were substituted by external threats, i.e. interference by other entity into a zone of influence.

Also large scale military conflicts were listed as a vital threat. At the same time the role of the Russian Federation was highlighted as a power which was to guarantee its own influences in regional and global dimension. It was also stressed that NATO and the US were trying to interfere unlawfully into Russian interest zone and keeping unipolar order with American hegemony leads to disturbances and conflicts on a global scale.¹⁹

In this context demonstrations by A. Podberezkin raise no astonishment and demonstrate that Russia pretends to be the main actor of Eurasian integration and promotes its own system of values not only in culture and economy but also in the international security area. To achieve this Russia will have to promote and emphasize to an even greater extent its foreign and military politics as far as the south and the east are concerned. Areas east of the Ural mountains have become of its most political interest. At the same time Russian state is afraid of western aspirations, what A. Podberezkin expressed in the following words:

Hoping that territorial unity, sovereignty and security of Eurasia will be kept only by international law and international institutions – it is naivety. Similarly naive was to count by M. Gorbachev on general values. There are quite many comments that Russia cannot govern itself by wealth hidden in the middle of deep Siberia or constantly make use of vast areas with huge supplies of natural resources (M. Albright, M. Thatcher, Z. Brzeziński), which openly interfere with international norms. Also open attempts to use force pressure and soft power against Russia. This injustice can be fixed, according to many politicians, only by revision of the Russian Federation state borders what seems not so impossible in the eyes of Western politicians. To gain such aims there can be a whole range of scenarios realized, among which the most secure and proper from the political point of view, would be making Russia to refrain from the control over transportation corridors, resources and then over territorial unity. At present, such calculations really exist. What is more, history proves that similar course of events is more often a norm than exception. And it is not only in the past but also in the newest history, with the USSR and Yugoslavia as examples²⁰ (interpretation by the author).

These thoughts show that Russia should take some counteractions against any possible revisionist actions against this country.

¹⁹ М. Децзыński, *Rosyjskie Siły Zbrojne...*, pp. 29–30.

²⁰ А.И. Подберезкин, *Евразийская воздушно-космическая...*, pp. 49–50.

Vladimir Putin doctrine follow-up

According to A. Podberezkin's idea, that there is no grounds to think that the reduction of tension in Eurasia will take place or that the US will resign from counteracting integration processes in the continent. Strategic interests of the US in Central Asia were clearly defined for the first time in April 1997 in a special report of the State Department to Congress. In the report it was pointed out that the USA, as the biggest energy consumers in the world, is interested in "widening and diversification" of the world's energy resources. What is more, because of their nature, American interests in that region are not only economic but also strategic, because (...) *the problem applies directly to ensuring security of the West*. On the other hand, in a doctrinal approach of Russians there are ideas that Russian policy's aim in Eurasia region is to create common peaceful security and stabilization area based on the rule of integrity of common security, cooperation and mutual trust.²¹

It is no wonder that these points of strategic priorities to existence in international environment are immutable exponent of foreign policy led by president Vladimir Putin since 2000. It is worth mentioning that they were firmly emphasized during his speech at the security conference in Munich on February 10, 2007, during which he gave the so called Munich speech, further known as *Putin's Doctrine*. It is the interpretation of principles of modern Russia's foreign policy based on the total criticism of the unipolar idea, i.e. such world order where the power belongs to only one hegemonic entity (the US). According to Putin, the unipolar idea is the cause of new wars and tensions in international relations, leads to unstoppable hyper use of military power in international relations. And that, in turn, makes the world facing permanent conflict, further arms race and lack of security in view of new threats, like terrorism.²² What is more, Putin presented Russian counter proposal to American strategy, which is creation of a new architecture of global security²³ to make the world multipolar with influences of one country balanced by interaction of regional centers of power: the EU, Japan, Russia, China, India and Brazil.²⁴

Putin's doctrine was assessed as the critique of the Western approach to Russia. The West, trying to ensure geopolitical prevalence in Europe and Central Asia, had underestimated Russian Federation's aspirations after the Cold War time. Meantime, Russia felt threatened by American unilateral approach which was reflected in ringing the country by NATO forces starting with former Baltic republics to American bases in Central Asia. In view of numerous commentators, Russia presented itself as "a beleaguered

²¹ А.И. Подберезкин, *Современная военная политика России: учебно-методический комплекс*, Vol. 2, Москва 2017, p. 910.

²² D. Gibas-Krzak, *Świat w polityce zagranicznej Federacji Rosyjskiej*, „Kwartalnik Bellona” 2010, No 4, pp. 32–42.

²³ V. Putin, *Speech and the Following Discussion at the Munich Conference on Security Policy*, <http://en.kremlin.ru/events/president/transcripts/24034> [access: 3 I 2018].

²⁴ *Ibidem*.

castle”, accused the US of a new arms race, failing to uphold the international law and interference in politics of the CIS²⁵. And, what is most important – it did not accept the unipolar order and wanted its political situation to be improved internationally.²⁶

Present politics of the Russian Federation after the end of the Cold War proposes a new collective security pact which was presented by Dmitry Medvedev in 2008. The first stage of this new plan was to convene the summit of the Organization for Security and Co-operation in Europe (OSCE) and all security structures, including NATO, EU, CIS and the Collective Security Treaty Organization (CSTO).²⁷ The proposal was a follow up to ideas and programs in Russian foreign policy after the Cold War, because it was already in 1994 when Russia proposed transformation of the Conference for Security and Co-operation in Europe (CSCE) into a kind of regional United Nations Organization with Security Council (Executive Committee). CSCE-OSCE was supposed to be a political superstructure for the European security system and provide Russia with equal influence on Euro-Atlantic zone management (it was mostly about the possibility of co-decision as far as NATO enlargement was concerned).²⁸ On October 8, 2008 during a conference in Evian, France, president Medvedev posited the UN enhancement and presented some rules, called later *Medvedev's Plan*, on which the new architecture of European security was to be based. The rules were as follow:

- respect of territorial integrity, of sovereignty and political independence,
- avoiding to use force or the threat to use force,
- opposition to attempts to ensure one's own security at the expense of the security of others,
- disagreement on activities weakening unity of the common security area,
- disagreement on development of other military alliances to the disadvantage of security of other treaty participants.

The most important for the increase of Russia's position as a power was the idea of indivisibility of security for all, thanks to which Russia would be given influence on NATO enlargement processes and decisions on the placement of anti-missile shield elements in Central Europe.²⁹ It is worth stressing that these ideas became basic to political elites of the Russian Federation and strategic programs in the field of defense have been based on the same assumptions which had been formulated after the end of inter-block confrontation. Nevertheless, in the assessment of many analysts, Russia's goal is not creation of a multipolar order but taking over the role of a hegemonic entity, what is, in reality, a step back to the Cold War competition between the USSR and the US.

²⁵ S. Blank, *Threats to and from Russia: an assessment*, „Journal of Slavic Military Studies” 2008, No 3, p. 515.

²⁶ M. Stuermer: *Putin i odrodzenie Rosji*, Wrocław 2008, p. 15.

²⁷ A. Krzymowski: *Plan Miedwiediewa – nowa architektura bezpieczeństwa?*, „Sprawy Międzynarodowe” 2009, No 2, pp. 23–24.

²⁸ A. Брыс, *Rosja w XXI wieku. Gracz światowy czy koniec gry?*, Warszawa 2008, p. 120.

²⁹ Д. Медведев, *Выступление на Конференции по вопросам мировой политики*, Evian, <http://kremlin.ru/events/president/transcripts/1659> [access: 3 I 2018].

The future of A. Podberezkin's concept

It should be assumed that the idea of the Eurasian Aerospace Defense Forces is the extension of previous ideological and program concepts of Russia connected to international order transformation. This time, though, it is based on the military component and refers to Eurasia region. Under the name of the Eurasian System of Aerospace Defense there are means and measures developed to defend the Russian Federation and its allies on land and at sea, in the air and space, linked by functional contacts from aerial and space assault. Its tasks include:

- warning before rocket and space assault and recognizing space and informing military forces about it;
- destroying battle blocks of intercontinental ballistic missiles and ballistic missiles of submarines; destroying space equipment of the adversary;
- warning before aerial assault, recognizing air situation and control over airspace; defense of the most important state management and military facilities from airspace measures, defense of the economy and infrastructure, massive troops and military facilities;
- establishment of radio electronic situation, securing radio electronic defense of Aerospace Defense targets.³⁰

Further development and integration of military systems is required so that the system worked properly. It is to equip military forces of the Russian Federation in modern means and systems of Aerospace Defense and to compete with the main producers of Aerospace Defense systems on an equal footing. At present, the most powerful political and military potential have NATO members, that are main suppliers of both aero-cosmic strikes means and aero-cosmic defense measures worldwide. What is more, military and industry complex and arms market of the People's Republic of China tends to intensify. NATO members and its allies as well as China are interested in development of their own aero and cosmic defense measures.³¹

The importance of Aerospace Defense program is that currently there is no common Eurasian security system and it is only NATO at the moment that continues to pretend to this role and tends to widen its influences across the whole continent.

According to A. Podberezkin there are a few scenarios of shaping a new system possible, which come down to:

- 1) creation of an Eurasian security system (modeled on OSCE), in which there would all countries from Ireland to the Philippines be included. It would have political obligations together with implementation mechanisms;
- 2) creation of coalition systems of international security which would include the most important countries and alliances on the continent:

³⁰ S. Kleszcz, M. Kloske, *Rosyjska strategia*, „Kwartalnik Bellona” 2010, No 4, p. 47; А.И. Подберезкин, *Евразийская воздушно-космическая...*, pp. 448–449.

³¹ Ibidem.

- USA,
 - EU,
 - China,
 - India,
 - Russia;
- 3) developments of already existing military and political alliances (coalitions) and creation new ones.³²

Russian analysts, afraid of NATO prevalence, claim that integration initiatives in Eurasia under Russian leadership will be regarded by the US as unnecessary because they pose a threat to American hegemony.³³ That is the reason why NATO will, by all means, counteract any attempts of launching any coalition. Because the alliance has got many instruments to prevent such situation that bilateral or multilateral cooperation in specific areas could transform into a military and political coalition in Eurasia, also with participation of members of the European Union. In the West, in turn, analysts criticize Putin's politics and point out that because of current Russian actions on the international stage it is possible only to take "the strategy of force", what should be done together by the US and the EU.³⁴

China and India towards the Eurasian Aerospace Defense

It is a Russian idea that common Eurasian Aerospace Defense should become a part of a broader political agreement, similar to the OSCE Helsinki Final Act from 1975, in which a sovereign right to ensure military security of national territories would be guaranteed. Particularly that many Eurasian countries, primarily China and India, very quickly move in that direction in their independent way and their strategic documents and activities on the international stage clearly indicate that they want to be important, if not key, players on the "Eurasian chessboard"³⁵. Increasing potentials of China or India are unquestionable and it is definite that it is going to influence heavily the balance of power in the region.

According to Indian foreign policy concepts in the post Cold War era the aim of the country has become a strive for power status in the 21st century³⁶. It is mainly

³² Ibidem, pp. 32–33.

³³ Ibidem, p. 33.

³⁴ An example of such rhetoric are statements of Theresa May, the UK Prime Minister, who pointed out that Putin had to choose another strategy than annexation of Crimea, conflict in Ukraine and cyber attacks on European governments and parliaments. At the same time, the British Prime Minister did not refer in a negative way to the partnership with Russia but under condition that the country would obey the rule of a democratic country. See: *May do Rosjan: Wiemy co robicie. Nie odniesiecie sukcesu*, TVN24 of 14 XI 2017, <https://www.tvn24.pl/wiadomosci-ze-swiate,2/theresa-may-krytykuje-rosje-putina,789946.html> [access: 3 I 2018]; *Die Welt: Reset z Rosją niemożliwy. Jedyną opcją strategia siły*, Defence24 of 27 XII 201., <http://www.defence24.pl/719274,die-welt-reset-z-rosja-niemozliwy-jedyna-opcja-strategia-sily> [access: 3 I 2018].

³⁵ А.И. Подберезкин, *Евразийская воздушно-космическая...*, pp. 459–460.

³⁶ J. Zajączkowski, *Polityka zagraniczna Indii po zakończeniu zimnej wojny*, in: *Polityka*

about recognition by other powers of India's global aspirations. According to Indian analysts, in the world based on hierarchy India should stand in the same line with such powers as the EU, the US, China, Japan and Russia and also belong together with them to the club of world powers. It is true that in the beginning of the 21st century India has chosen a bandwagoning strategy, i.e. alliance with a stronger power (in this particular case – the US). Nevertheless, it does not mean that the country intends to submit to the hegemonic entity. India inspire more to the role of an equal partner in international relations, especially that the symbol of the country strength are still nuclear weapon and army. It is mainly a significant military potential, including nuclear power, that decides about the country's power status. In this context, it is worth noting that Shakti – Indian goddess of strength – more and more often reflects Indian perception of international order.³⁷ Furthermore, it should be mentioned that Indian nuclear doctrine is based on the *minimal reliable deterrence* notion and on the *no first use* rule, also to countries which also possess nuclear weapon. It means, inter alia, that the basic thing is the ability to survive enemy strike (it regards both to means of transfer as well as command structures) and to launch an effective counter-strike. The strength of such strike should be so much significant to discourage a potential aggressor from application of its own nuclear forces. In this context, it is understandable that all used and developed ballistic systems are mobile systems (wheeled or rail).³⁸ It is also worth pointing out that the outline of Indian nuclear doctrine disclosed in 1999 included the term *nuclear triad* (missiles with nuclear warheads placed on land, on submarines and on bombers).

Following strategic assumptions made India has noted progress in developing the national two-tier air defense system, which components are AAD anti-ballistic missiles which are designed to take out targets transferring nuclear warheads. Indian rocket forces are equipped currently with three types of ballistic missiles and two more are to be developed. At present, as it is assessed, their air defense system is capable to intercept missiles launched at the range of 2000 km. In 2016 the new Indian missile was capable of destroying ballistic missiles at the range of 5000 km. Ten years earlier a construction of the first Indian strategic nuclear submarine (called boomer) had been started. Available information speak about three to five boomers, but it seems hardly likely that the target system for them is a short range missile, which would highly limit their strategic role³⁹. It is no doubt that there are new modifications of Indian anti-missiles on the table and the end of works on the plan of the air defense system placement. The open question is still whether any cooperation with Americans is planned. All the more so, since Indians, as a rule, do not reject any foreign cooperation in the field of air defense construction – Israel takes part in their program and provides assistance by early warning radar networks.

zagraniczna. Aktorzy. Potencjały. Strategie, T. Łoś-Nowak (ed.), Warszawa 2011, p. 178.

³⁷ Ibidem, pp. 178–179.

³⁸ R. Ciastoń, *Indie vs. Pakistan – nuklearna rywalizacja*, geopolityka.org of 13 September 2011, <http://www.psz.pl/116-bezpieczenstwo/indie-vs-pakistan-nuklearna-rywalizacja> [access: 5 I 2018].

³⁹ *Indie testują nową antyrakietę*, Defence24 of 11 February 2017, <http://www.defence24.pl/545788,indie-testuja-nowa-antyrakiete> [access: 3 I 2018].

China, concentrated on political stability, pay the most attention to economic expansion. One should be remembered, though, without the so-called Central State modern world could not exist – this is a result of a significant development of Chinese economy. Solving important global problems is obtained by pragmatic politics and it makes China not to miss any possibility to widen its presence on foreign markets also via Chinese minority settled in many countries. So, one can speak not only about expansionism but also about sinocentrism. China, by its centripetal force, becomes an attractive centre and creates a separate civilization, which desirability decides about the scale of influence. A very important aspect of national strategy⁴⁰ is the fact that in China information and communication prevalence is regarded as the biggest threat to national security. In fact, it is not possible that social nets are used for coordination of anti-governmental groups activities or demonstrations of subversive nature, which is a result of Facebook and Twitter prohibition. And Chinese social websites are under control of Chinese government. These kind of activities are to oppose American domination, especially when it comes to influencing Chinese information policy and the way Chinese Internet resources are used in stimulating different kinds of dissenting activities.⁴¹ Although, a new geopolitical reality becomes formation of two military and political centers of military power – China and the US – which can compete against each other in the next decade but cooperation cannot be excluded as well. Analysts very often indicate that establishing the Chinese superpower could mean return to a bipolar order, in which two power centers, one in Washington, and the second in Beijing, could represent different patterns of globalization and political systems, what would resemble the Cold War order.⁴² The scale of cooperation and competition is hard to predict but there is a threat that such processes can be at the expense of other countries.

What role could Russia play in the new power structure? In Russian commentators' assessment hampering Russia's aerial and cosmic defense development would cause inevitably that in the medium term the US gains the potential capable of not only overpowering strikes but also potential able to neutralize extant forces planned to be used in a counter-strike. Such action can lead to a destabilization of global situation and make military potential again a global instrument of the US and NATO foreign policy.⁴³ This is the reason why A. Podberezkin postulates Russia and Europe to unite in order to control Eurasian space.⁴⁴ It is worth noting that for the last few years Russia has been perceived in China as a main stabilization actor in Eurasia able to weaken American politics. In view of this China seeks to loser cooperation with Russians on the military stage, starting from common tactical training flights to cooperation in scope of anti-aircraft and logistic tasks.

⁴⁰ C. Jean, *Geopolityka*, Wrocław–Warszawa–Kraków 2007, pp. 320–321.

⁴¹ А.И. Подберезкин, *Евразийская воздушно-космическая...*, p. 373.

⁴² J. Marszałek-Kawa, *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, in: *Polityka zagraniczna. Aktorzy. Potencjały. Strategie...*, p. 123.

⁴³ А.И. Подберезкин, *Евразийская воздушно-космическая...*, p. 452.

⁴⁴ Ibidem.

The headline in the area is military potential building which can play an important role on a global scale. Undoubtedly, Pentagon observes such activities with great concern. There are numerous articles in the American press on the subject, particularly on anti-missiles defense component and air defense cooperation between the two countries which leads to common air defense in Eurasian space. Development of this potential may diminish existing unique capabilities of the US of leading air operations in Asia and Pacific area and on the European action theatre, what slows down the American expansion and shows changing international order.⁴⁵

Conclusions

In the second decade of the 21st century there has been going on a pursuit of air space and information space transformation into one battlefield, on which there will be no strict boundaries as far as altitude, space, or even information influence is concerned. It is a new global theatre of fighting which becomes decisive and tends to relegate traditional areas of military potential application, i.e. land and marine space. Russians expect that in the medium term perspective – 2018-2020, preliminary stage will be finished. During that time basically new weapon systems will be created and new concepts of their application will be elaborated and tested. Together with the devaluation of nuclear deterrence idea and increase of contradictions between new power centers it means that countries with significant military potential can move an active phase of its application. As a consequence, means of engagement in a such aero and information space become decisive for the victory. Such kind of integration will inevitably cause harmonizing state management and military command of strategic offensive weapon (nuclear and conventional) and defensive weapon (strategic offensive weapon and aerospace defense) as well as means of information influence. It seems appropriate to hypothesize that it is going to be *sui generis* „the battle for Eurasia” and solution to this task will be a challenge for international cooperation supported by political efforts. Final outcome will depend on military and technical potential, strategic offensive and defensive armament and development of industry in terms of their components production⁴⁶.

It should also be stressed that according to Russians the battle for Eurasia is a run-in with American hegemony which calls into question Russian strengthening on the outskirts of the former USSR and building counterbalance to the US⁴⁷. It is worth

⁴⁵ *Sky's the limit for joint Russian-Chinese Eurasian Air Defense Zone*, 1 VIII 2017, <https://sputniknews.com/military/201708011056086886-russian-chinese-common-airspace-defense/> [access: 18 I 2018].

⁴⁶ *Ibidem*.

⁴⁷ The American document list also Iran and North Korea and accuses those countries of destabilizing their neighborhood. At the same time it stresses that North Korea has become a global threat because of advanced nuclear program. See: M.A. Piotrowski, B. Wiśniewski, *Strategia bezpieczeństwa narodowego USA: podejście administracji Trumpa*, „Biuletyn PISM” of 21 XII 2017, <http://www.pism.pl/publikacje/biuletyn/nr-128-1570> [access: 3 I 2018].

noting that in the latest National Security Strategy of December 19, 2017 China and Russia are those countries that actively affect security weakening and diminishing role of the US. What is more, those countries have propaganda, asymmetric, conventional and nuclear potentials which can be used to revise the existing international order. It is sort of admitting by Americans that Russia and China are their rivals on a global scale. In this context the battle for Eurasia can be regarded as a clash to control Heartland, that is struggle for supremacy of the world which brings back two-block competition from the Cold War times. There is the US (NATO) and Russia on opposite sides and the unknown shall remain what strategy will India and China adopt. One can predict with high probability that international order will definitely be revisioned. It is not known, at the same time, whether tendencies of expansionist nature from the world's major actors would strengthen.

Abstract

The author of the article describes the most important theses of A. Podberezkin plan against the geopolitical Russia background which form a paradigm of a common security in Russian terms on a strategic area of Eurasia. It is of a particular significance in view of the growing threats to modern world. Especially of hazardous nature is current problem of North Korea in connection with nuclear testing carried out by unpredictable regime of Kim Jong-un which creates the risk that sudden conflict can drag the whole Peninsula into a war. This, in turn, would lead to the US intervention there. Effects of the possible conflict involving superpower are hard to predict. Another current problem is Moscow-Washington conflict and Moscow-European Union conflict. Indeed, NATO enlargement to the east transformed the block from regional to global and included the whole Eurasia into their scope of responsibility. Meanwhile, Russia being in opposition to such strategy, has been trying to build counterbalance to American politics. Research done by scientists, including A. Podberezkin, serve this purpose. He is one of the numerous supporters of more active politics based on Eurasiatic ideas with the supreme role of Russia. During the Collective Security Treaty Organization summit in Ashgabad Russia's proposal concerning *przepisać ze strony wcześniej* was accepted. This way the Eurasian Aerospace Defense was initiated. Few military centers in Eurasia together with growing importance of India and China and their economic and military capabilities is to obtain potentials of strategic offensive weapons, and most of all, aerial and cosmic precision-guided component of various purpose. Russians predict finishing preliminary stage in the years 2018-2020, during which new weapon systems are to be created and new concepts of their applications are to be developed and tested. It was stressed in the article that it would be a *sui generis* the battle for Eurasia and solution to this task was going to be a challenge to the international cooperation

supported by political efforts. The final result will depend on technical and military potential, strategic offensive and defensive weapon and development of industry in scope of its components production.

Keywords: Eurasia, Russia, China, India, the US, Aerospace Defense, Putin's doctrine, post Cold War competition, change of international order, geopolitics.

V
STUDIES
AND ANALYSES

Anna Łasińska

Selected imaging techniques applied in forensic science

Forensic science is a broad, multidisciplinary science using various techniques and research methods, which have been recognized and developed for a long time in the natural sciences. For thousands of years, a human amassed the knowledge about animated objects based on what he could see with the naked eye. In the 16th and early 17th centuries the first microscopes became available. The Dutch, Hans and Zacharias Janssen are considered to be the invention of the microscope. They made the first designs around 1590. At that time microscopes didn't get recognizing as a research tool, due to the weak magnification (approximately 10x). The power of microscopy was realized by Antonie van Leeuwenhoek already in the 17th century. He has refined the design of the microscope, and then developed the production of these devices. A. Leeuwenhoek first watched live cells – sperm cells, protozoa, erythrocytes, etc. The development of imaging methods contributed to the discovery of X rays by Wilhelm Röntgen. These methods allow for non-destructive examination of the interior of living organisms.

The technological progress that we see in the modern world entails changes in all areas of life, improving them, accelerating their development and opening to new possibilities. In order to optimize results and deliver their justice in the fullest and safest form, the modern forensic science has adapted new research methods, technologies and equipment. The task of the experts working in the forensic labs is to provide the fullest information on the secured material. The examination of trace amounts of a wide variety of chemical substances that make up the trace on the site of the crime and which constitute evidence is especially relevant. Thanks to the use of both destructive and non-destructive methods of research. Microtrace as evidence of the material in the case, should not be destroyed or used up during the test. It places great demands on the experts and the techniques which they use. In the structural studies of microtraces and their physical and chemical properties a variety methods and imaging techniques are used. The main objective of these methods – whatever technical solutions and tools (from the simplest magnifying glass to advanced electron microscopes) is to obtain a magnified view of small objects.

Currently, in the world many types of microscopes and joined with them other multi-functional devices are used. In order to obtain information about the shape of the analysed samples and objects, their size, chemical composition, crystal structure, mechanical, electrical, or magnetic properties. The most commonly used techniques are optical microscopy and electron microscopy, spectrometric techniques, such as infrared and Raman, and x-rays analysis.

In this article some imaging techniques such as confocal microscopy¹, electron microscopy and atomic force microscopy and micro-Raman spectrometry will be presented, which are applied in many fields of forensic science. In table 1 a comparison of basic properties of the microscopes is presented: optical microscope, scanning electron microscope, (SEM) and atomic force microscope (AFM).

Tab. 1. Basic properties of the microscopes: optical microscope, scanning electron microscope, (SEM) and atomic force microscope (AFM).²

| Feature of the microscope | Optical microscope | SEM | AFM |
|---------------------------|--|--------------------------|---------------------|
| Resolution x, y axis | 1000 nm | 5 nm | 0,1 nm |
| Resolution z axis | – | – | 0,01 nm |
| Magnification | do 2000 | do 10 ⁶ | do 10 ⁸ |
| Depth of field | the average | large | small |
| Environment research | air, liquid, vacuum | vacuum | air, liquid, vacuum |
| Type restrictions | diffraction of light (CLSM – confocal microscope – diffraction of laser) | diffraction of electrons | needle size |

Regardless of the type of devices used to image, one of the important parameters is called a resolving power – the shortest distance between two points, which are considered as separate on the obtained image. Diffraction of light is the cause of limited resolving power of the **optical microscope**. This makes the images adjacent on the sample details become indistinguishable, when the distance between them was close to the wavelength of light. The idea of the construction of optical microscope became the basis for electron microscopy. The beam has been replaced by electron beam for getting the image parameters (magnification, resolution) that are not available for the classical light microscopy. The technique of electron microscopy, provides images with a resolution of the order of 0.1–0.05 nm, more than 4000 times better than a typical optical microscope. It is a resolving power of about 4 000 000x better than the ability of the human eye. Optical microscopy has many advantages, features and functionality that are not available for other types of microscopy. Recent conceptual and technical solutions used in confocal scanning microscopy increase the scope this method.

¹ Specific form of the light microscopy characterized by increasing contrast and optical resolution. Capturing multiple two-dimensional images at different depths in a sample enables the reconstruction of three-dimensional structures within an object, https://pl.wikipedia.org/wiki/Mikroskopia_konfokalna [access: 29 XII 2017] (note ed.).

² All the tables and artwork have been developed by the author of the text (note ed.).

Optical microscope is an essential device presented in biological, medical and forensic laboratories. Due to the simple construction and low price it is still the most commonly used microscope. For more than a century, the construction of a standard optical microscope has remained unchanged. Classic light microscope consist of two lenses: lens and eyepiece, whose combined magnification is the final magnification of the image.

In studies of quality materials stereoscopic microscopes are indispensable (fig. 1). These are optical microscopes which enable spatial vision of the observed object.



Fig. 1. The stereomicroscope integrated with microscopic digital camera and LCD screen.

Light running by the optical stereomicroscope, separately for each eye, produces the image perceived by the human mind as three-dimensional. This kind of microscopes are characterized by low magnification, a little more than 300 x. The observation is done by transmitted or reflected light. Stereomicroscopes are recommended for work related to the study of handwriting, archaeology, gemmology, botany, research quality electronic circuit boards, research quality samples for analysis of SEM/EDX, for observation of crystalline structures at the level of micrometer, for the preliminary examination of evidence (fig. 2) and any precision work.

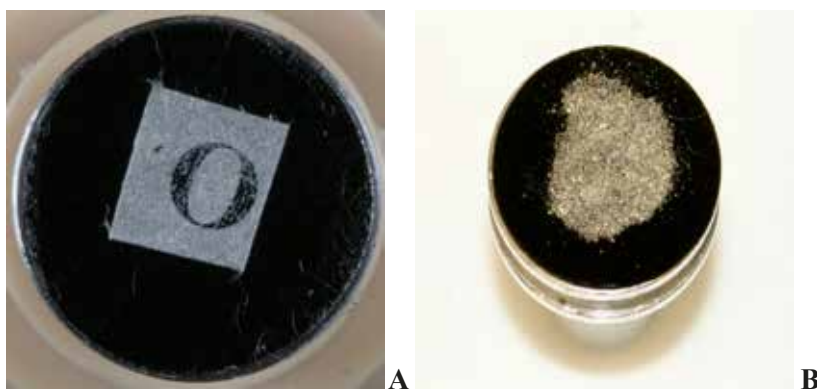


Fig. 2. SEM stubs with samples of printout on paper (A) and pyrotechnic mixture (B) seen in stereomicroscope.³

The light originated from the outside of the focal plane is one of the important limitations of classic optical microscopy. The lens of the microscope collects images not only from the focal plane, but also from the entire cross section of the sample. The image of the focal plane is sharp and clear. Images of objects lying in front of and behind the focal plane are not sharp (blurry) and much more, the further they lie from this plane. As a result, image of the visible object in the classic microscope is characterized by high background reducing the sharpness of outlines.

The most perfect type of light microscope in terms of optical is **confocal microscope**. Marvin Minsky said, that the perfect light microscope should cut the light not originated from the focus plane of the lens and scan point by point the tested material. Nowadays, the parameters of the Laser Scanning Confocal Microscope, LSCM, moved closer to the theoretical limits of magnification and image resolution. These parameters are valid for light microscopy from the 19th century (their author is a German physicist, Ernst Abbe). The construction of laser confocal microscopy (fig. 3) was based on fluorescent microscope⁴, and a laser or a few lasers are a light source. Lasers generate beam with very high intensity.

³ A. Łasińska, K. Barszcz, *Ilościowa i jakościowa analiza mieszanin pirotechnicznych SEM/EDS*, „Przegląd Bezpieczeństwa Wewnętrznego” 2014, No 11, p. 181.

⁴ Fluorescence microscopy – the type of light microscopy, which is used to test of fluorescent sample (absorbing single wavelength of light and emitting different). Light of a single wavelength is used to excitation fluorescent molecules and the light at a different wavelength, which is emitted by the particles is gathered and used to produce the image. In most cases, for example, parts of the cells or tissues that may be observed, do not exhibit fluorescence. Therefore, it must be marked before the observation of the fluorescent dye or marker.



Fig. 3. Inverted confocal microscope Nikon TiE Eclipse A1 with microselection and laser microdissection (A) optical microscope with the C1 confocal equipment Nikon Eclipse 80i (B).

The light beam is focused on the examined object. The confocal microscopy assumes eliminating images, which are originated from outside of the focal plane. The light is focused on one point of preparation and at a predetermined depth. The fluorescence is excited at the point of focus, but also above and below the plane point. With the help a pinhole conjugated with the orificial aperture of the path of the illumination in detector, only by size and position image of the focal plane point of sample is recorded. The depth of laser excitation of the fluorescence and the getting of the transmitted lighting is about 50 micrometers. In two-Fign confocal microscopes the range of excitation is extended to 400–500 micrometers. Automatic repeating scanning and other reallocations along the z axis enable the collection of a stack of images (called optical slices) of next layers of specimen. The resulting image layer is characterized by a weak background and sharper contours. This method allows to obtain a higher magnification tested materials and facilitates their interpretation. It creates a three-dimensional image of the object and its internal structure through a set of images. In confocal microscopes the most frequently used lasers are: argon, argon-krypton, helium-neon, semiconductor – diode, on the solid – state (femto-, nano-, pico- second - titanium-sapphire). Depending on the type of the laser the spectral lines⁵ of the emitted light are different. For example, laser Ar, which is a type of ion gas laser emits light in the visible light and UV wavelengths (351, 454, 528 nm).

⁵ Spectral line – dark or bright line in an otherwise uniform and continuous spectrum, resulting from emission or absorption of light in a narrow frequency range, compared with the nearby frequencies.

In modern confocal microscopes two different design solutions are applied. In both cases the cross section image object is obtained at a certain depth. However, these images are obtained in a different way. In laser scanning confocal microscope the laser beam goes into the object and excites emission of fluorochrome particles. Pinhole is placed in the optical path in order to obtain strong focus of the light beam in the focal plane. The light beam goes to the dichromatic mirror, after passing through the pinhole. Dichromatic mirror reflects the light of the excitation beam and transmits the light emitted by the fluorochrome (with longer wavelength). The excitation beam then passes through the lens, which ultimately focuses it in the form of a microscopic spot on the focal plane. The light emitted by the fluorochrome particles passes through the lens and dichromatic mirror (without reflection), and goes to the second aperture. The light from the focal plane passes through the aperture to the detector. The others are stopped at the aperture. Any change to the position of the dichromatic mirror allows to change the position of the focus beam on the focal plane. The position of the mirror is controlled by the computer system. The system records the position of the light spot and the intensity of the light, which are recorded by the detector. Information about the analyzed object is obtained by systematic scanning of the focal plane.

In **two-Fign confocal microscope** (TPCM) for the excitation of fluorochrome, near-infrared radiation with a quantum energy equal to half of the excitation energy is used. Under such conditions, excitation of the fluorochrome molecule occurs only when the molecule absorbs two quanta of radiation simultaneously. In practice, only in the place of a strong focus of the beam this phenomenon occurs. Therefore, in TPCM do not need pinhole before the detector, as emitted light comes only from the focal plain. The laser generates short pulses of radiation with high Fign density (tens of kilowatts at maximum impulse), but with low-energy pulse (nanodżul per pulse). In this case the principle of scanning object is analogous to the operation of the microscope with scanning laser. Two-Fign microscopes or multiFign microscopes have many advantages that derive from the application of the excitation beam of near-infrared range. These are:

- low energy carried by a beam that causes much less thermal and Fignchemical damage to the object,
- better penetration of biological specimen than using shortwave visible light or UV radiation. This enables to work with the objects of greater thickness,
- greater sensitivity than LSCM, which allows to work with lower concentrations of fluorochromes.

The analysed data are collected in the form of luminous intensity of the point and by their nature are monochrome. After collecting the data set, the image is processed on a typical format for digital Figs. In this form it can be easily coloured. If it is stained with more than one fluorochrome, they must differ in the wavelength of the excitation light. Independent data about the object are collected for each wavelength. Typically emissions of each fluorochrome assigned a contrasting color. At the stage

of creating digital pictures data are compiled in one image. Currently, there are available confocal microscopes, which allow the excitation of light with three or more wave ranges. Confocal microscopy is becoming an increasingly available research technique that provides large amounts of detailed information. This is done with the development of the deals available fluorochrome and increase in their specificity. It is possible to obtain a single scan at the time of less than 0.05 s. This allows for recording rapidly changing processes in the living cell or tissue and observation in the form of a video.

The advantage of confocal microscopy, not present in other technologies, is a possibility to obtain a series of cross-sections of the tested specimen from different depths. The series of cross-sections can be used to reproduce the spatial structure of the object.

The technique of confocal microscopy is widely applied in the biological sciences, medicine, genetic engineering⁶, as well as in forensic science. In forensic medicine this technique allow to detect and visualize pathological changes in the case of sudden death, to distinguish between input and output of the wound after the bullet, specify the distance of the shot, as well as skin lesions and injuries incurred after the explosion. Confocal microscopy gives the possibility to direct three-dimensional microscopic imaging of individual cells or pieces of tissue (fig. 4).

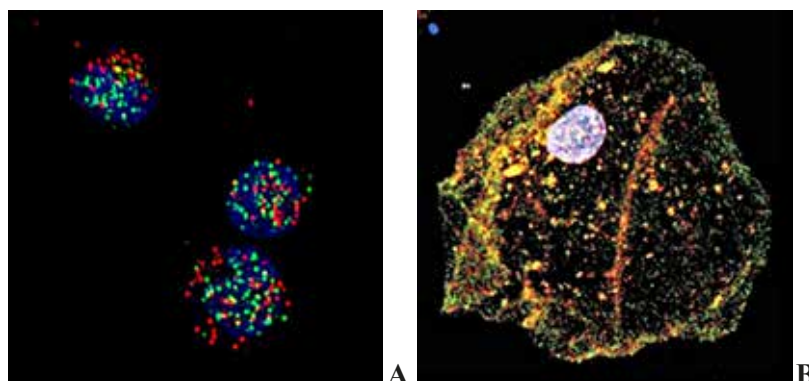


Fig. 4. 3D image of human lymphocyte cells (A) and (B) HeLa made using inverted laser confocal microscope Nikon Eclipse TiE A1.

Already in the 19th century it was noted that some of the fluorochrome have the ability to impact on some components of the cells: proteins, lipids, nucleic acids, etc. Over time, standard staining procedures were developed to allow visualization of significant elements for the cell. Fig. 4 shows the microFiggraphy of human cells stained with a mixture of three dyes. Due to the combination of dyes, both cell membranes and cell nuclei can be seen

⁶ A. Raczkowska and others, *Pleiotropic effects of a Yersinia enterocolitica ompR mutation on adherent-invasive abilities and biofilm formation*, „FEMS Microbiology Letters” 2011, No 321, pp. 43–49.

simultaneously. Also some fluorescent dyes have the ability to selectively bind to the cell components. The use of fluorescent dyes has a lot of advantages and allows:

- to observe light emission on the dark background, which increases the sensitivity of the method and enhances the contrast observed details. This increase in sensitivity is so important, that in all the techniques of selective staining of specific macro-molecules fluorescent dyes are used in principle, and not the classic absorption dyes,
- to differentiate between the cells or their fragments due to the existing conditions in them. For this purpose the strength and colour of fluorescence are used. The latter depends on conditions in the environment, ie: pH, redox potential, lipophilicity, membrane potential. Fig. 4 shows the cell nuclei stained the dye DAPI. This compound fluoresces blue after intercalation⁷ to DNA,
- to detect differences in the concentration of some ions, e.g.. Ca^{2+} , what determines the strength and colour fluorescence.

Currently, advanced laser microdissection systems are equipped with laser modules emitting UV or IR, integrated with high-quality fluorescence or confocal microscopes and a motorised table. The unit completed a computer system to control the process of cutting the cells by using software, camera and monitor. Developed originally for use in the field of oncology, microdissection systems are also applied in areas of the biological and forensic sciences. Confocal microscopy conjugated with laser microdissection have created new opportunities for genetic profiling of biological traces, traditionally secured to swab and forensic tape.⁸ As a result of the phenomenon of cold ablation, by the action of the laser the individual cells or fragments of tissues are separated from the rest of the mixture along with the part of the membrane. Laser mikrodisekcja module contains the picosecond pulse laser, on 4 mW solid state, emitting radiation in the UV spectrum (at the wavelength of 355 nm). Imaging and qualification of fragments of undergoing microdissection is done by transmitted light, using high-speed films internal digital camera. The microdissection is carried out with variable parameters and a focal length of the laser beam.

Now another method of analysis and isolation of cells is microselection. The system is controlled by computer using dedicated software. Previously the isolation process requires the adequate calibration of the system, which allows to obtain high-precision acquisition and deposition of selected cells. Isolating single cells takes place in three stages: identification, acquisition and embedding. Imaging and qualification of fragments of the specimen is done by transmitted light, using high-speed films internal digital camera, as in laser microdissection. The technique of laser confocal

⁷ In chemistry, intercalation is the reversible inclusion or insertion of a molecule (or ion) into materials with layered structures. Examples are found in graphite and transition metal dichalcogenides, [https://en.wikipedia.org/wiki/Intercalation_\(chemistry\)](https://en.wikipedia.org/wiki/Intercalation_(chemistry)) [access: 29 XII 2017] (note ed.).

⁸ A. Łasińska and others, *Ocena przydatności folii adhezyjnych do zabezpieczania śladów biologicznych oraz izolacji komórek ludzkich metodą mikrodyssekcji laserowej*, „Problemy Kryminalistyki” 2014, No 283, pp. 18–28.

microscopy is also used to identify documents printed on paper⁹, and to determine the uniformity of the implementation of the document by the disclosure, whether the text was added to an already existing (fig. 5).

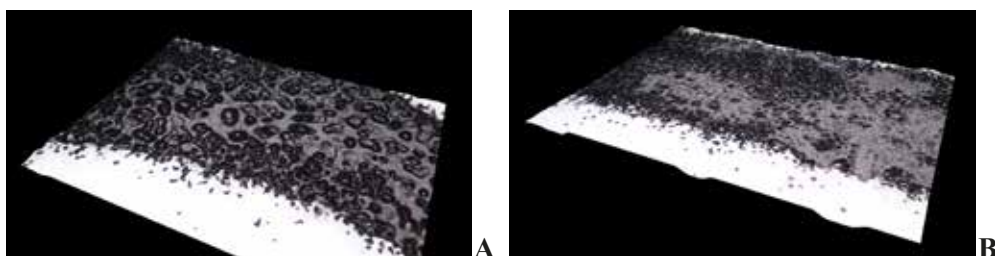


Fig. 5. 3D image of the surface of toner visible on the printout obtained from the laser printer: the document twice passed by the device (A), the document once passed through the device (B). Figgraphs in 200x of magnification, using a Nikon 80i microscope.

In order to determine the characteristics of the toner on printouts optical microscope Nikon Eclipse 80i with confocal equipment C1 was used (fig. 5B). Fragments of printouts were observed in transmitted light using a Nikon DS5NC color CCD camera with cooling, with 2560 x 1980 resolution and LU Plan Fluor 200x N.A. 0.90, WD 1.0. lens. The construction of the microscope allows to perform examination of documents of A4 format, in a non-destructive method. Microscopic observation shows that the surface of toner on the paper is strongly enhanced (fig. 6). For each printout creates a distinctive individual layout structures. Visible are two types of specific areas: more flat solid surface and granular surface, creating smaller or larger aggregations of varying density.

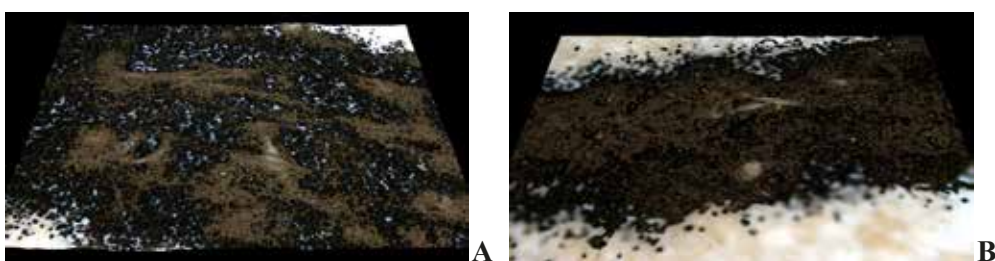


Fig. 6. 3D image of toner on printouts obtained from colour laser printer C734/C736w (A) and monochrome laser printer T650n/T652/T654n (B). Figgraphs in 200x of magnification, using a Nikon 80i microscope.

⁹ S. Szczepańczyk, U. Konarowska, *Zastosowanie mikroskopii optycznej w weryfikacji dokumentów przerobionych za pomocą drukarki laserowej*, „Problemy Kryminalistyki” 2012, No 276, pp. 65–73; A. Łasińska, *Badania mikrośladów*, in: *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, B. Hołyst (note ed.), Warszawa 2014, pp. 804–840; A. Łasińska, U. Konarowska, *Zastosowanie mikroskopii optycznej i elektronowej w badaniach autentyczności dokumentów*, in: *Dokumenty a prawo prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (ed.), Warszawa 2015, pp. 105–112.

A good method of imaging is also Raman Spectroscopy. This is a spectroscopic techniques used to observe the oscillation spectra of materials, similarly to infrared absorption spectroscopy. It can be used for the analysis of gases, liquids, and solids. As a source of excitation, in most Raman spectrometers the lasers are used. This technique is complementary to infrared spectroscopy. In practice, most of the spectrum is recorded with the Stokes maximum¹⁰, which have a higher intensity than anti-Stokes¹¹, because the number of molecules in the first excited state is less than in the basic state. As the temperature increases, the number of molecules in the first excited state increases, thus the intensity of anti-Stokes lines increases. The total Raman spectrum consists of: maximum Rayleigh¹² scattering (high intensity, wavelength the same as the excitation wavelength), Stokes maxima (lower frequencies, higher wavelengths) and anti-Stokes maxima (higher frequencies, lower wavelengths). Raman shifts in the Raman spectra are identical in magnitude with the position of the absorption peaks in the infrared spectra, however, their relative intensities differ. Some maxima can be seen in one spectrum, while the others cannot. Raman scattering is related to the distortion of the electron density distribution around the bond, followed by radiation rebinding combining bonds back to the original shape. Homonuclear molecules, inactive in infrared, give Raman lines, because the polarizability of bonds (i.e. the binding force of electrons in a molecule) changes periodically and in phase with the stretching stretches. In the spectrum, the Raman band appears when polarizability changes during normal vibration.

During the vibrations, also the polarizability may change periodically. Vibration causes periodic changes in atomic structures. This diversity of selection rules of the infrared and Raman spectra causes that some infrared inertial vibrations may be active in the Raman spectrum and vice versa. For example, the vibration of a two-atom homonuclear molecule (including O₂, N₂) is inactive in infrared, however, it appears in the Raman spectrum because the polarization changes in this oscillation. In the case of NaCl, KCl molecules, we do not observe Raman spectra even in the gas phase, where they are not dissociated. This is because they are ionic molecules, their valence electrons belong to the appropriate atomic frameworks and during the vibrations they move with their atomic framework. Movement of atomic frameworks has no effect on polarizability. In fact, the bonds in molecules are not ideally ionic and therefore it is possible to obtain

¹⁰ Stokes band – they arise when the molecule is transferred to higher oscillatory level (after interacting with radiation) and the *scattered* photon has energy lower by the energy difference of oscillation levels $h\nu$.

¹¹ Anti-Stokes band – if the molecule was on an excited oscillatory level, before interacting with radiation, then the interaction transfers it to the basic (zero) oscillatory level. The scattered photon has energy higher by the energy difference of oscillation levels $h\nu$. This band usually has a lower intensity than the Stokes band.

¹² Rayleigh band – they arise due to the interaction of photons of incident radiation with the frequency ν_0 , which do not correspond to the energy levels of the molecule. When the molecule returns to the same energy level, after interaction with radiation, this phenomenon is called Rayleigh's classic scattering.

the Raman band of such molecules. These bands have such a low intensity that they are practically invisible. Another example is the molecule of HCl which gives the Raman spectrum not only in a gas state, but also in a concentrated aqueous solution. The solution is so concentrated that the dissociation of acid is reversed. This shows a high proportion of covalent bond in H–Cl binding. In the case of strongly polarized ionic bonds, the electric dipole moment and its change over the time are quite large. High intensity of the bands corresponding to strongly polarized bonds in the infrared spectrum was observed, unlike in the Raman spectrum. As a result, the term appeared in the literature, called criterion spectroscopic polarity binding. It says that if the intensity of the infrared band increases, and in the Raman spectrum decreases, it means that the corresponding binding of the molecule becomes more polarized. And vice versa – if the intensity of the Raman band increases, and the intensity of the infrared band decreases, this means an increase in the covalence of the corresponding bond.

The advantage of Raman spectroscopy is the ease with which samples can be prepared. This technique does not require the use of chemically unstable KBr cuvettes. Measurements of aqueous sample solutions can be made. It is also possible to perform measurements at higher temperatures. Raman spectroscopy is particularly useful for measuring the frequency of oscillating metal-ligand complexes, which have vibration frequency is in the range of 100–700 cm^{-1} . Measurement of the infrared spectra are very difficult to carry out in this range. Another advantage of Raman spectroscopy is that the sources of excitation emit radiation in the visible range. This allows for precise tuning of the optical system of the Raman microscopes. Raman spectra can be used to identify unknown substances, detection in a molecule specific groups of atoms or types of chemical bonds, for determining the geometric structure of molecules and vibration analysis. A valuable modification of spectroscopy is **micro-Raman spectrometry** which also to apply in forensic studies. Procedures for determining the intensity of the bands is an important element of correct Raman image creation. Micro-Raman spectrometry is a combination of Raman spectrometry and optical microscopy.¹³ The microscopic image (at appropriate magnification) of the tested surface preparation is visible on the screen (fig. 7).

¹³ M. Bowden and others, *Thermal degradation of poly-urethane-backed poly (vinyl chloride) studied by Raman microline focus spektrometry*, „Polymer” 1994, No 35, pp. 1654–1657.

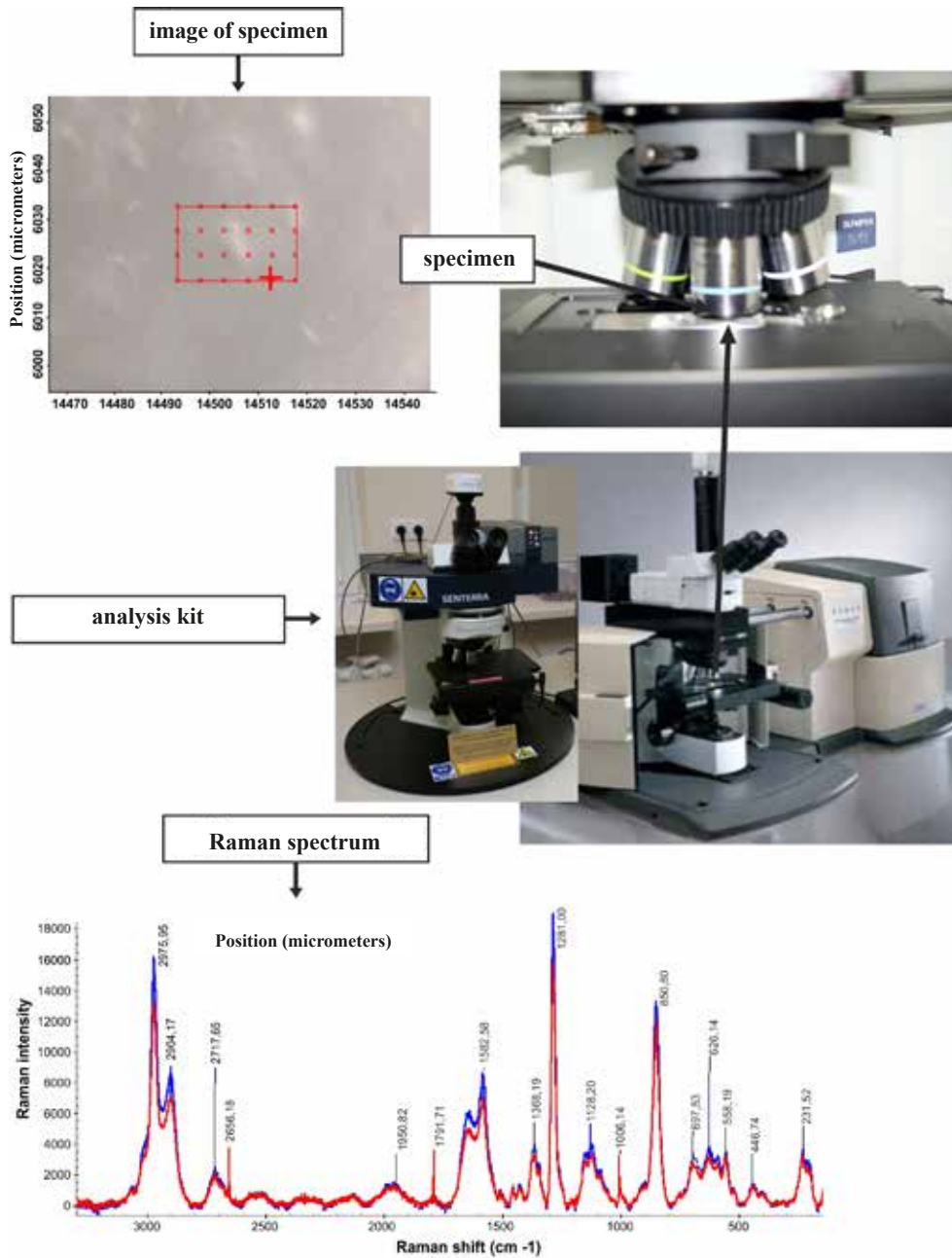


Fig. 7. Surface analysis scheme of unburned gunpowder grains by using micro-Raman spectrometry.

Motorized microscope table allows to choose the right position for Raman spectrometry analysis. Micro-Raman spectroscopy is considered as a non-destructive method. It allows to obtain information about the chemical composition of the sample

in a microscale. Research of toner cartridges carried out by Raman spectroscopy showed the presence of carbon molecular structures based on bands originated from amorphous carbon or (and) graphite, and amorphous silica. Depending on the excitation lines, the band was observed in 1574 cm^{-1} i 1332 cm^{-1} (fig. 8) and 1375 cm^{-1} , 1253 cm^{-1} and 2693 cm^{-1} .

It is possible to collect spectra from several points of the upper or lower surface of the sample and to make maps based on the size, chosen for spectral comparison, by coupling the Raman spectrometer with a microscope equipped with a scanning movement. The appropriate image is presented in the form of maps with colored squares. Thus, the distribution of the discrete function is obtained. To the distribution of the continuous function approximated by the program using the appropriate polynomial.

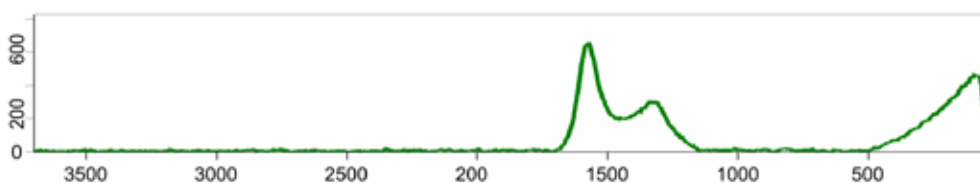


Fig. 8. Raman spectrum of the toner sample in the form of powder taken directly from the cartridge of the Lexmark C780 device – replacement, made by excited by a 532nm laser.

Raman maps of several gunpowder have been made to examine the homogeneity of the particles of unburned or partially burnt gunpowder. Only some grains showed the presence of sharp characteristic bands. The bands corresponding to the groups of NO_2 and CH_2 , nitroglycerine and nitrocellulose are the most evident in the Raman spectrum of gunshot residue. Fig. 9. show map of the intensity change of the stretching vibrations band of the NO_2 group and the band of symmetric stretching vibrations of the CH_2 groups. In the case of micro-particles originated from the residue of ammunition Fiocchi G.F.L 9×19 mm containing nitroglycerin and nitrocellulose, the intensity of the bands NO_2 group changes from 0.10 to 5.50. This change suggests that the mixture is not homogeneous. There are areas which are almost devoid of chemical compounds containing NO_2 groups.

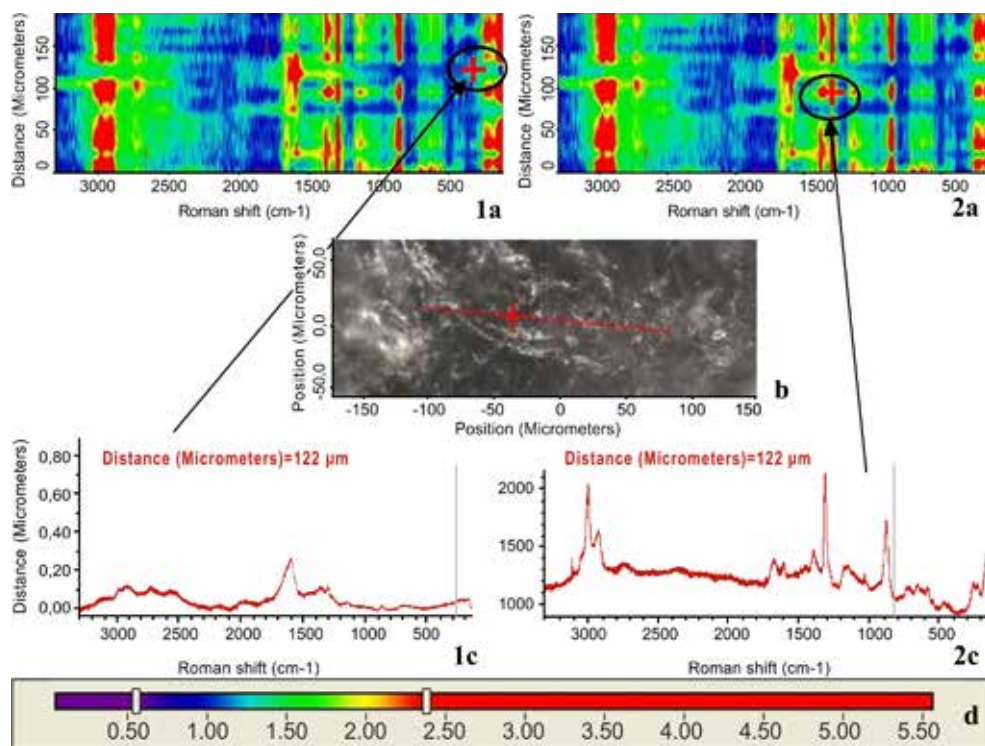


Fig. 9. Intensity change maps of stretching vibrations band of NO_2 group in unburned gunpowder originated from Fiocchi G.F.L 9×19 mm ammunition (1 a, 2 a); image of the analyzed area of the sample obtained from confocal microscope (b); Raman spectra in points marked with a red cross on maps, respectively (1 c, 2 c); the scale of the color assignment of the change values of the NO_2 group band intensity (d).¹⁴

Fig. 9 shows spectra and the nature of the micro-particles in terms of chemical composition, in one point on the map. Depending on the color distribution on the map, changes of the band intensity were observed. At the point marked on the map with a red cross in the light green area (fig. 9.1 a), the spectrum mainly shows the band corresponding to the C–C stretching vibrations (fig. 9.1 c). However, at the point marked on the map with a red cross in the red area (fig. 9.2 a) all bands associated with the presence of nitroglycerine and nitrocellulose are visible in the spectrum (fig. 9.2 c).¹⁵

The analytical method showed the possibility of identification of some organic compounds contained in the gunshot residue, and the possibility of imaging (mapping) changes in the band intensity of some functional groups of organic substances

¹⁴ A. Łasińska, *Analiza nieorganicznych i organicznych pozostałości po wystrzale z broni palnej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, No 16, pp. 157–189.

¹⁵ Ibidem.

presented in a single grain. The morphology and inorganic components study of the typical particles of gunshot residue provide full identification evidence.

In Raman spectroscopy, many new techniques are currently used, which primarily increase the sensitivity of this method. Resonance Raman Spectroscopy, RRS is a technique in which the frequency of a monochromatic laser beam is tuned to the frequency of electron transitions of the analyzed compound. This leads to a selective increase of the intensity of Raman bands 10^2 – 10^6 times, in relation to classic Raman dispersion spectroscopy.

A Surface Enhanced Raman Spectroscopy, SERS, is also applied in examinations where Raman scattering of molecules adsorbed on the surface of a metal or metallic sol (mainly silver) is measured. The phenomenon of amplification is explained by two different mechanisms: chemical and electromagnetic. In the SERS method, the intensity of the Raman signal increases 10^3 – 10^7 times in relation to the signal obtained in the classic Raman experiment.¹⁶ Spectra can be obtained from a very small, precisely selected sample area (about $1 \mu\text{m}^2$), using confocal Raman microscopy. The possibilities offered by the confocal microscope, obtain optical cross-sections of the examined materials, three-dimensional images and visualization of cells and fragments of tissues, varnish coatings from various cars, gunshot residues, detection of trace amounts of substances or contaminants, documents that are difficult to forge (hard-to-forge) security documents.

Using some types of the modern light microscopy, a very high resolution images were obtained. In the past, the primary limitation of the quality of the obtained microscopic images, were a defect lenses (chromatic aberration, spherical aberration). This problem was overcome, at least, in the most expensive models, in the second half of the 19th century. However, another barrier was encountered – diffraction and interference phenomenon, that cause the appropriate image sharpness can only be obtained for objects with sizes many times larger than the length of the wave used. Objects smaller than $1/2$ of the wavelength are not visible at all. Objects, in a distorted form, with a wavelength order of magnitude appear in the microscope image: surrounded by colored rims. Therefore, even the best optical microscopes that work in the visible spectrum, give maximum magnification of the order of 1500x. The maximum magnification up to approx. 3500x is achieved by microscopes working in the ultraviolet range. The development of electron microscopy was determined in order to obtain large magnifications of objects, impossible to obtain in optical microscopes. If we see something very small with very high resolution, and to know the elemental composition of the tested substance, should be used the technique of **electron microscopy coupled with an X-ray microanalyzer** (fig. 10).

¹⁶ B. Sharma and others, *SERS: Materials, applications, and the future*, “Materials today” 2012, No 15, pp.16–25.

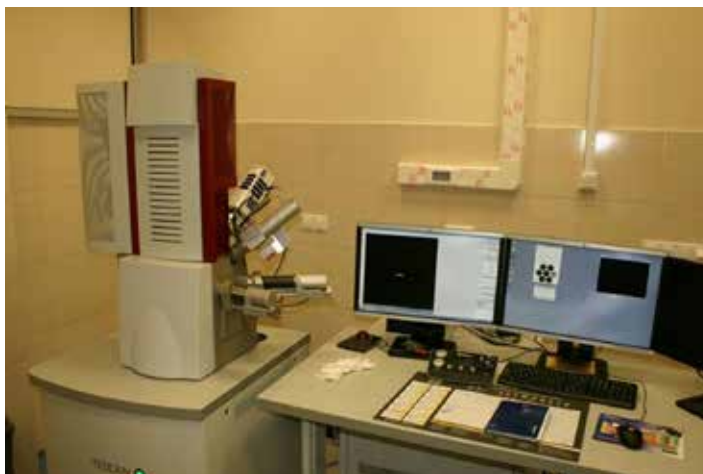


Fig.10. Scanning electron microscope with an X-ray microanalysis detector.

For 70 years the **electron microscope** has become a commonly used device in science, industry, and forensic science. Electron microscopes differ from light microscopes. They form the sample image using electron beam but not the light. Electrons have a much shorter wavelength than visible light. Electron microscopes allow to obtain images with a higher resolution than the standard images obtained in light microscopes. The electron microscope offers a wide range of research possibilities for microscopic samples of chemical substances and complex materials in the form of solids state, after the development of appropriate analytical methodology. The microscope enables simultaneous studies of their chemical composition and morphology. An additional advantage is that, in many cases, it does not require destruction of the sample, neither in the process of preparing it for analysis, nor during the measurement.

In the scanning electron microscope (SEM) the image is obtained as a result of detection of secondary and (or) reflected electrons with which the sample is bombarded. Imaging techniques such as: BSE (back-scattered electrons), SE (secondary electrons), CL (cathodoluminescence), LVSTD (in a variable vacuum) and X-ray microanalysis allow to analyze samples – except gas – both conductive and non-conductive. For the imaging of samples, secondary and backscatter electrons are commonly used. Secondary electrons are the most valuable for showing the morphology and topography of the samples. On the other hand, backscattered electrons are used to illustrate the contrast of multiphase samples. Secondary electrons are emitted from the area which is very close to the specimen surface. Therefore, the images from this detector clearly show the topography (shape) of the sample surface. They are characterized by a large depth of field. Back-scattered electrons – or reflected electrons emerge from deeper locations within the specimen and consequently the resolution of BSE images is less than SE images. BSE images are characterized by a smaller depth of field and they do not show the topography of the sample well,

but they provide information about the density of the observed surfaces. They show qualitative phase (chemical) differentiation of the sample surface. Higher or much lower number of electrons in the primary beam are backscattered, depending on the atomic number Z of the element. The number of protons in the nucleus describes the atomic number Z of the element. This means that the signal coming from heavy elements is much stronger than from the light elements. This allows the detection of metallic inclusions or heavy elements in the observed samples. The contrast characteristic of BSE imaging is proportional to the square of the mass number and instead of the topographic contrast (for SE imaging), the material contrast can be observed (fig. 11).

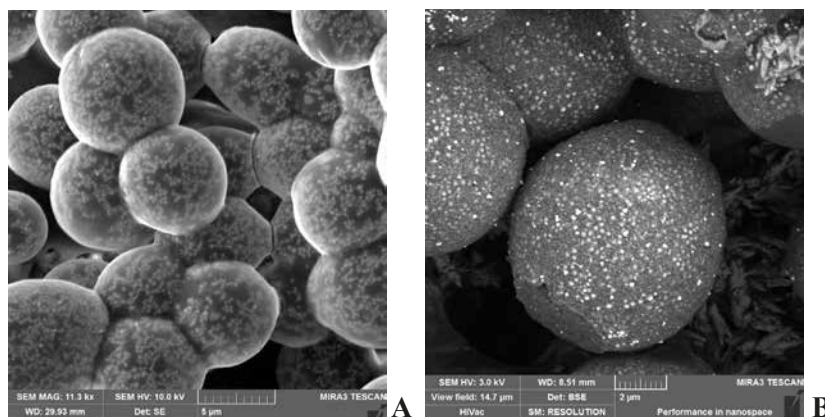


Fig. 11. SE (A) and BSE (B) image using a scanning electron microscope.

Another very useful technique is EDS spectroscopy. The EDS spectrometer's functionality is based on detection of the radiation. Characteristic radiation is emitted by atoms of the samples excited by the electron beam. During the bombardment of a sample with the primary electron beam, electrons are ejected from elements present in the sample. After ejection of the electrons the empty spaces are replaced by electrons from higher orbitals. In order to compensate for energy differences between electrons during this transition, X-rays characteristic for the given element are emitted. X-rays are analysed by EDS detector, as a result the elemental composition of the tested sample is determined. In addition, a semi-quantitative test was performed and the various samples were examined not only in terms of diversity, which are visible in BSE image, but also to determine the qualitative and quantitative changes in their composition. Study of the surface of the samples also allows to perform linear analysis and map content. This research are carried out, in order to capture the subtle changes in the elemental composition, which are not visible in the BSE image. The elemental composition can be easily interpreted and converted into percentages of cells. Considering composition, in terms of atomic percentage, conclusions can be read about the stoichiometry of compounds in the sample (fig. 12 and tab. 2).

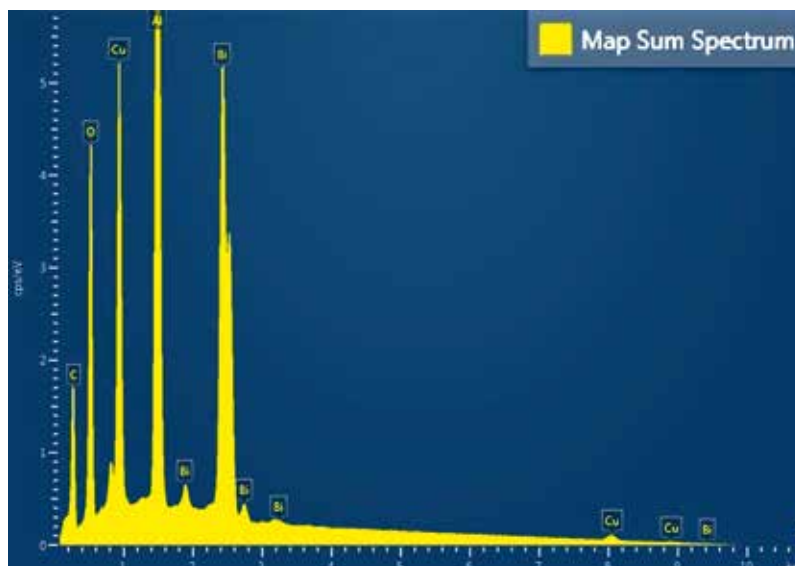


Fig. 12. EDS spectrum obtained during the SEM observation. The characteristic line K, L, M of the characteristic x-rays radiation by using symbols of the elements of the aluminium, copper, oxide and bismuth were marked.

Tab. 2. Quantitative results of x-ray microanalysis. The table of the results was generated using the Aztek program included in the SEM Mira 3XMU microscope software.¹⁷

| Element | Line type | k Ratio | Wt% | Wt% Sigma | Compound |
|---------|-----------|---------|-------|-----------|--------------------------------|
| O | K | 0,00576 | 10,38 | 0,05 | SiO ₂ |
| Al | K | 0,01818 | 19,11 | 0,06 | Al ₂ O ₃ |
| Cu | L | 0,01357 | 18,53 | 0,08 | Cu |
| Bi | M | 0,04348 | 51,97 | 0,12 | Bi |

The results of the quantitative analysis contain the following information:

- Wt % – weight percentage of the element in the sample
- Wt% Sigma – weight percentage error
- k-Ratio – the ratio of the radiation intensity of the characteristic line of the element in the sample to the intensity of the pure element under the same conditions.

The characteristic X-rays radiation is used to obtain maps of distribution of the elements' concentrations (called mapping). Analytical beam scans the tested area point by point. The spectrometer is set to automatically record a point in tested

¹⁷ A. Łasińska, *Badania mikrośladów...*, pp. 804–840.

area when it detects X-ray pulse with the characteristic energy for the corresponding element. In this way, a map of the elemental distribution was created. Colorful maps in appropriate shades are created by modern EDS systems, which show the most probable value of the pulse intensity at each point. However, it may require application with a sufficiently long time of the beam stop for each analytical point. During the one run of the analytical beam, distribution maps for several elements were recorded (fig. 13). The map is a bag of spots corresponding to pulses of X-rays. The degree of the spots concentration corresponds to the concentration of the element. Collection time of pulse have a significant implications for the assessment of distribution of the element concentration. However, the maps do not allow to capture small differences in concentrations and low concentrations (due to the presence of background spots – continuous radiation).

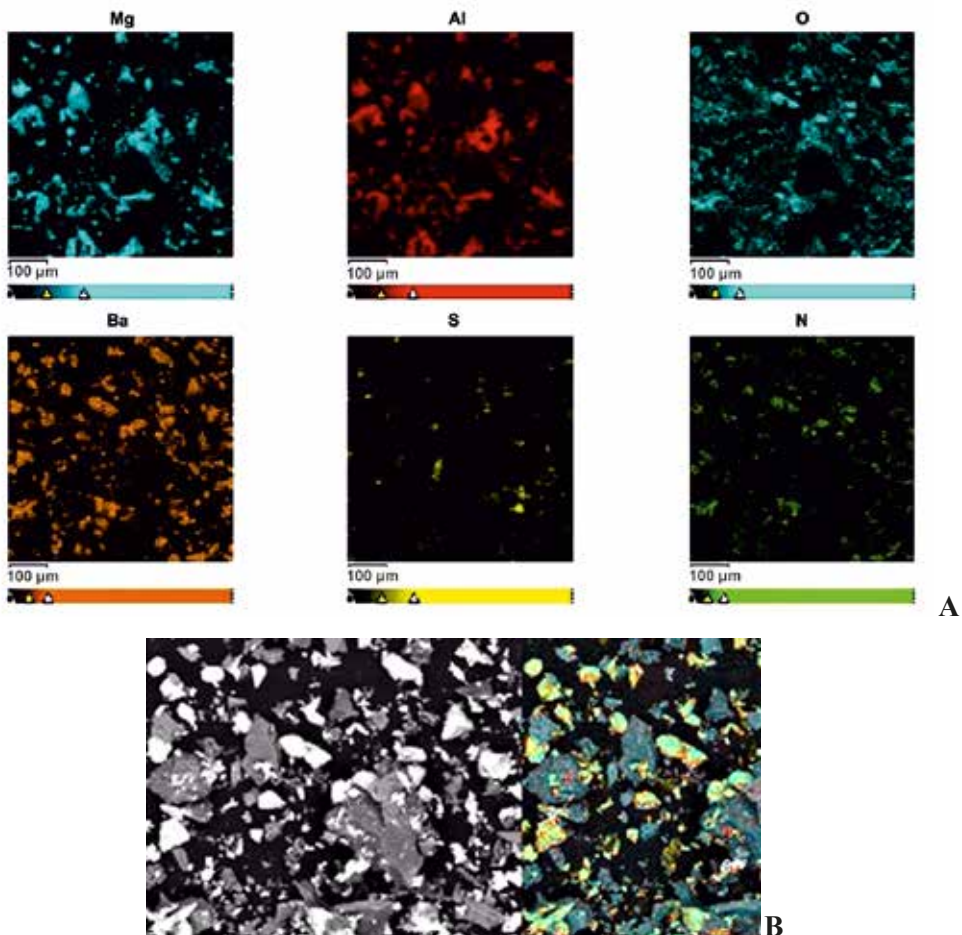


Fig. 13. Examples of elements concentration distribution maps (A); BSE image and the total image overlay maps of concentrations of elements (B). The maps were generated using the Aztek software included in the SEM Mira 3XMU microscope, based on the measured spectrum of EDS.

The chemical compounds and the percentage of these compounds in tested material are initially determined on the basis of the maps, using appropriate software. A sample map of the phases distribution and their percentage are shown in the fig. 14 and tab. 3.

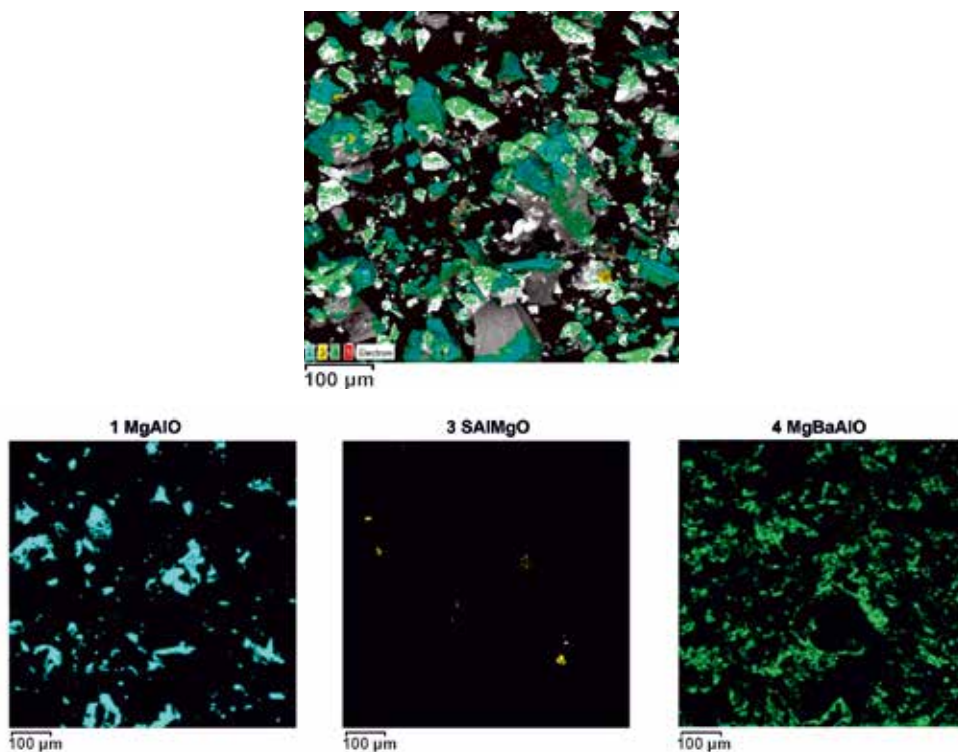


Fig. 14. Examples of maps of the distribution phase. The maps were generated using the Aztek software included in the SEM Mira 3XMU microscope.

Tab. 3. The values of the founded fractions percentage.

| Compound | Fraction (%) | Number of pixels |
|-----------|--------------|------------------|
| 1 MgAlO | 9,1 | 23 849 |
| 3 SAlMgO | 0,2 | 553 |
| 4 MgBaAlO | 11,9 | 31 172 |

In the X-ray microanalysis the technique of linear analysis can also be applied. It involves scanning with an electron beam, along a defined line on the surface of the sample with simultaneous recording of changes in the intensity of the emitted X-ray radiation. A linear analysis of chemical composition shows the changes

in the concentration of defined element, along the line, selected on the surface of the tested sample. In the diagrams in fig. 15 an example of a line analysis is presented.

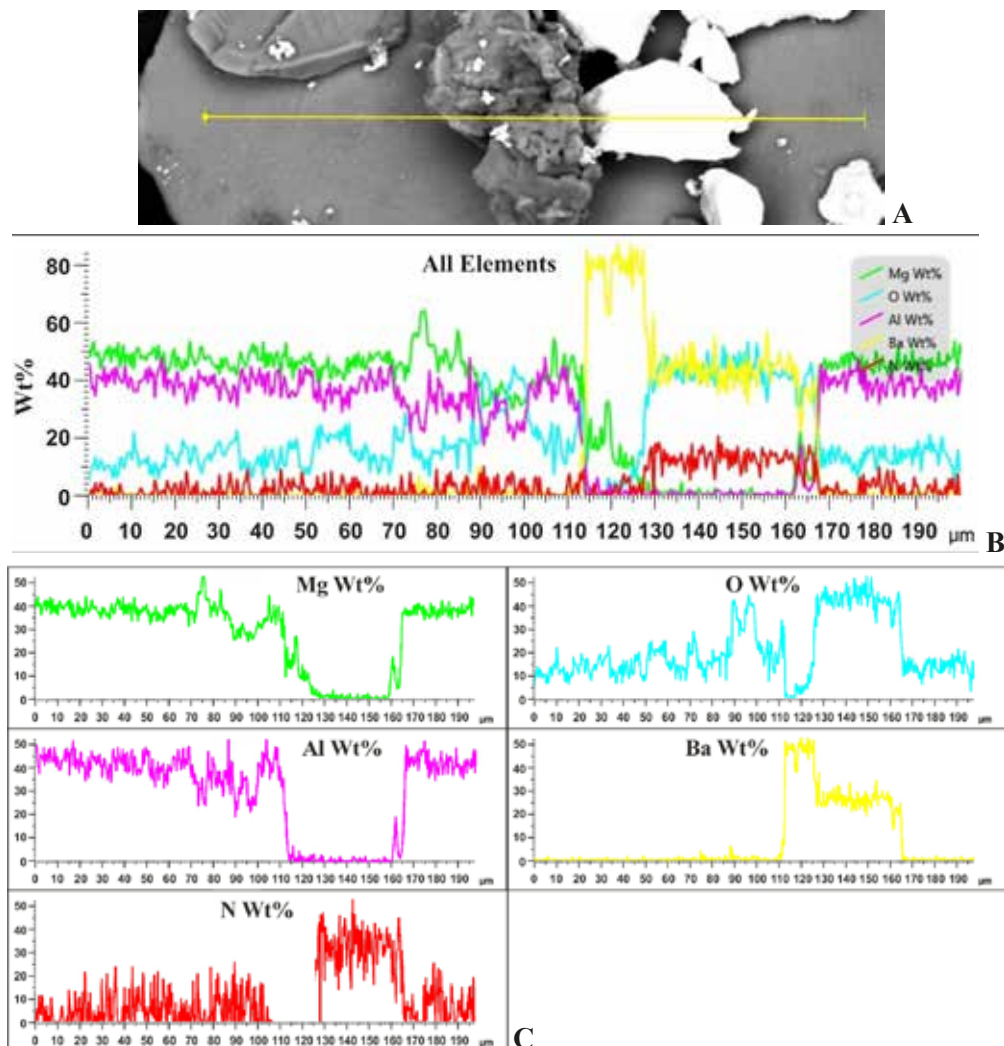


Fig. 15. BSE /SEM microFiggraphy of the grain surface with the scan line marked (A); curves: summary result of the EDX line analysis along the line (B); EDX line analysis of the elemental distribution (Mg, O, N, Al, Ba) in single grain (C) The line analysis was generated using the Aztek software included in the SEM Mira 3XMU microscope.

One of the most attractive features in electron microscopy is its wide range of applications in various fields of forensic science. It is used for identification tests and comparative evidence, such as: glass particles and varnishes, metals, toners for printing devices, fiber morphology, pyrotechnic mixtures and their residues, pyrotechnic devices

and gunshot residues (GSR). SEM is used to analyze micro-traces of solid substances found on clothes at the micrometer level (plant pollen, soil grains), paint splashes from the crime scene, and even to determine if the car had headlights turned on at the time of the accident. Electron microscopy allows us to analyze poorly visible or invisible microscopic traces by using imaging, image comparison and X-ray microanalysis.

From the point of view of the forensic science one of the essential problems faced by analysis, among others, appears to be the identification of the implementation device. Within the framework of the present research project extended research has been conducted aimed at obtaining the individual identification of printing and copying devices. In this study, 134 printouts from laser printers from 10 manufactures were analyzed. For this purpose, toners and their replacements were used. Microscopic images obtained allowed us to allocate characteristic features of toners to specific groups of devices: monochrome laser printers, color laser printers, monochrome multifunction devices and color multifunction devices. Clear criteria were established for individual assessment, which allowed to assign and select distinctive features of toners to the printouts obtained from the respective printer devices. Based on the SEM images and established criteria the details of topography of the toner structure were revealed. Based on this study, the differences or similarities of toners on tested printouts were determined. In case of printouts obtained from different laser printing devices the conducted analysis of the toner surfaces showed that not in every case toner layer on the printouts has solid or granular form. If both appear, the difference between the two consists in ratio of one layer to the other and the form of their distribution within the area of one sign, depending on the kind of device.

In some cases, certain features such as: straight rod structures and irregular structures (*T650n/T652/T654n* Lexmark), (fig. 16), bent rod structure (*X264/X363/X364* Lexmark), a single spherical structure resembling balls scattered about on the surface of a toner (*X940e/X945e* Lexmark), clearly the same size (*MX410* Lexmark), spheres and cubes on the grain surface (*Canon iRAAdv C9070*) or only cubes on the grain surface (*OKI MB461/MB471/MB491*) are individual for a specific print job. Some features may appear only in a few cases, such as: rod structures characteristic for two models of laser devices (*Dell 5310n* and *Dell 5350dn*), for one color laser multifunctional device *OKI C5550MFP* and for a few models of Lexmark monochrome laser devices.

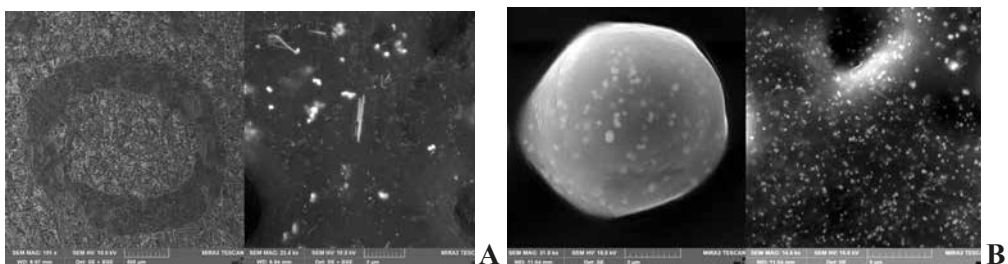


Fig. 16. SEM image of the solid surface (A), grain and grain surface (B) of toner on the printout obtained from Lexmark T650n/T652/T654n.

On the other hand, alternative features may be unique for a given type of printer device. For example, irregular or spherical structures under the grain surface and solid surface of the toner, were distinguished by different contrast in SEM image. This type of structure occurred in monochrome laser printers and monochrome laser multifunctional devices. Toners, creating text on the printouts are characterized by a number of features that allow you to distinguish among them but only within certain limits. Unfortunately, many of these features are repeated in different models, which significantly impedes their individual identification. However, these features allow you to specify the exact group of printing devices (monochrome, color).

Electron microscopes for forensic examinations can be also equipped with additional software for analysis of gunshot residue particles (GSR), with characteristic morphology and specific elemental composition. The software allows to analyze the residue found on clothing or skin of a firing person and particles originated from pyrotechnic reactions¹⁸. In forensic science, the analysis of gunshot residue is a frequently used method of research in order to explain the circumstances of the events with the use of firearms. Traces after firing from a firearm are routinely collected on a microscopic stub. Based on the high average atomic number (Z) of the GSR particles originated from the composition of the primer mixtures, the screening of such particles is carried out on the basis of their brightness on the backscattered electrons image (BSE) (fig.17).

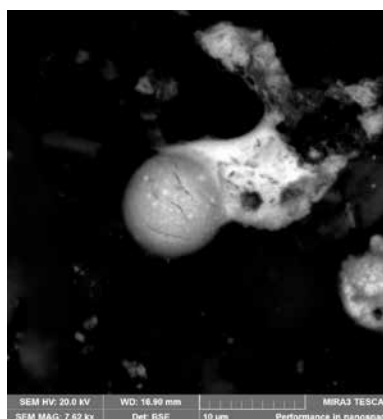


Fig. 17. SEM image of the characteristic particle of gunshot residue on the surface of microscope stub.

The elemental composition of the particles is analyzed by the EDX system, in which a common type of detector is a silicon detector doped with Si (Li) lithium in the solid state. Over 25 years ago, automated search systems were introduced, which

¹⁸ H. Krüsemann, *SEMs and forensic science*, „Problems of Forensic Science” 2001, No 47, pp.110–121.

replaced the manual search of gunshot residue particles originated from the primer.¹⁹ Such automatic search systems locate particles, analyze their elemental composition and identify them. Due to the small size of the GSR particles (e.g., 0.5–10 µm) in relation to the area of the sample (120–480 mm² depending on the size of the SEM microscope stub) and the large number of environmental particles with a high average atomic number (*Z*) usually found in the analyzed samples, the time needed to carry out the automatic search is long. The result of the GSR analysis is an automatically generated test report, which contains the number of particles, including the defined classes. The possibilities of automatic systems in the field of detection of a larger number of particles and of smaller sizes, carried out in shorter time, are increased by the continuous technological development of computer hardware and software.

Another technique of imaging is to obtain a surface image with a resolution capability in the order of dimensions of a single atom. For this purpose, atomic force microscope (AFM) is used. Among the many devices associated with nanotechnology, none is as well recognizable and simple in its construction as the atomic force microscope, also called the microscope of close interactions. Over the past few years, field of the applications of the AFM has expanded, mainly due to enormous potential, not available for other research techniques. The large resolution allows the testing of individual molecules, their groups and elements of supramolecular structures. The AFM consists of a cantilever with a sharp tip (probe) at its end that is used to scan the specimen surface, above or below the surface of the sample. AFM uses the intermolecular forces. The cantilever bias allows to determine the intermolecular forces between the atoms of the tip and the tested surface. The force map for each surface point of the sample is computer-processed into an image. Cantilever deflection measurement is made by optical methods. The sensitivity of the cantilever it is tenths of angstrom.²⁰ The tip consists of several hundred atoms to even one atom. The tips are usually made of silicon and silicon nitride. In contact atomic force microscopy mode, the cantilever is held from the surface of the sample at a distance of less than a few tenths of a nanometer, and repulsive forces are present. In non-contact atomic force microscopy mode, the cantilever is held from the surface of the tested material at a distance of a few to several dozen nanometers.

In this case, the probe-sample force of attraction can be found (van der Waals interactions). The appropriate choice of the research method using the AFM is important, because the correctness of the results depends on it. The AFM control computer must be characterized by high speed and large memory capacity.

¹⁹ R.S. White, A.D. Owens, *Automation of gunshot residue detection and analysis by scanning electron microscopy/energy dispersive X-ray analysis (SEM/EDX)*, „Journal of Forensic Science” 1987, No 32, pp. 1595–1603; M. Germani, *Evaluation of Instrumental Parameters for Automated Scanning Electron Microscopy/Gunshot Residue Particle Analysis*, „Journal of Forensic Science” 1991, No 36, pp. 331–342.

²⁰ Ångström (Å) – unit of length equal to 10⁻¹⁰ m. It is used for numerical expression of values of very small lengths, comparable to the sizes of atoms.

Computer programs used to generate of sample images and to determine their properties are constantly improved. Their development requires knowledge, not only in the field of mathematics and computer science, but also on the physical and chemical properties of the tested materials. It is also important to study the type of the material, the dimensions of the tip and the effect of the AFM on the force appearing between this tip and the tested sample. The research procedures and methods of statistical calculations are also developed, which are the basis for determining the properties of the geometrical structure of the examined surfaces. Application possibilities of the AFM are very large in various fields of science, technology and forensics. First of all, they include the study of metals, ceramic and silicon structures and recently conducted biology research on an increasing scale. AFM's forensic microscopy technique is used to investigate the effects of fire, blood, hair, fibers, paper texture, depth of penetration of coatings (inks, pen pastes)²¹ and to investigate gunshot residue (fig. 18), including the determination of the shape, size and average density of particles around the bullet inlet opening.²²

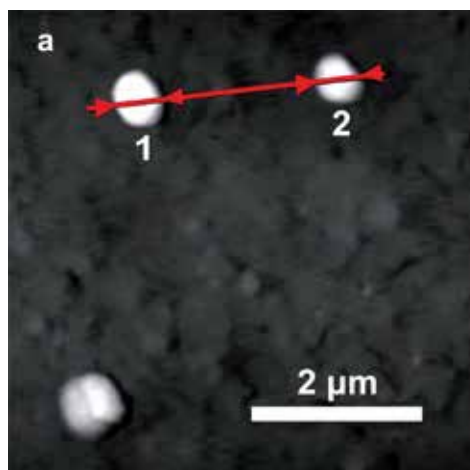


Fig. 18. AFM image of individual GSR particles.²³

A.J. Goddard et al used the AFM technique to study imaging fingerprint ridges on polished brass substrates. For the production of ammunition, brass is a very popular material. In this case the AFM microscopy technique was used to visualize the corrosion of metals, between fingerprints and metal, after heat treatment²⁴ on a nanometer scale.

²¹ S. Kasas, A. Khanmy-Vital, G. Dietler, *Examination of line crossings by atomic force microscopy*, „Forensic Science International” 2001, No 119, pp. 290–298.

²² Y. Mou, J. Lakadwar, J.W. Rabalais, *Evaluation of shooting distance by AFM and FTIR/ATR analysis of GSR*, „Journal of Forensic Science” 2008, No 58, pp. 1381–1386.

²³ Ibidem.

²⁴ A.J. Goddard, A.R. Hillman, J.W. Bond, *High Resolution Imaging of Latent Fingerprints by Localized Corrosion on Brass Surfaces*, „Journal of Forensic Sciences” 2010, No 55, pp. 58–65.

The AFM microscope was also used for the analysis of textile fibers. AFM images were used to quantify the surface texture parameters of fabrics exposed to environmental factors (different soil types, water) as a function of time. The tests showed the difference between fiber damage due to environmental factors and mechanical damage.²⁵

The AFM technique was also used to detect explosives. In order to determine the characteristics of explosives²⁶ more accurately, the surface morphologies of substances such as triamine-trinitro-benzene, ammonium perchlorate and PBX were analyzed. Due to the continuous work, both on the construction of the microscope and the physical basis of the method used, the possibilities of the AFM microscope are increasing. The interpretation of the results obtained by using AFM method is still a difficult and complex issue, despite continuous improvement of the atomic force microscope, the development of computer software and new achievements in the field of theoretical and experimental foundations.

Summary

The use of advanced technology to study the evidence allows extremely accurate analysis. Imaging of material in high magnification is necessary for the preparation of different samples documentation (the study of the morphology of the surface, determining the diagnostic features). The use of optical microscopy, electron microscopy or atomic force microscopy and integrated spectroscopic systems is a basic and powerful tool for the observation of various materials. Currently, such device systems should be available in every forensic laboratory. These systems should be used as basic devices, routinely used in court expertise, despite their high market value and high exploitation prices. They allow quick, uncomplicated and non-destructive testing of material. Therefore, in a short time, it is possible to obtain information about the tested samples, which can be easily processed and visualized by making Figgraphic documentation, with regard to various construction details, examining their optical properties and determining their chemical composition. The obtained results, enable preliminary classification of evidence before being passed to further research using other highly advanced instruments.

²⁵ E. Canetta, K. Montiel, A.K. Adya, *Morphological changes in textile fibres exposed to environmental stresses: atomic force microscopic examination*, „Forensic Science International” 2009, No 191, pp. 6–14.

²⁶ M. Tourne, *Developments in explosives characterization and detection*, „Journal of Forensic Research” 2013, No S12, pp. 002 (pp. 2–10); G.C. Yang, F. Nie, H. Huang, L. Zhao, *Pang preparation and characterization of nano-TATB explosive*, „Propellants Explosives, Pyrotechnics” 2006, No 31, pp. 390–394; A. Kumari and others, *Nano-ammonium perchlorate: preparation, characterization and evaluation in composite propellant formulation*, „Journal of Energetic Materials” 2013, No 31, pp. 192–202; A.E.D.M van der Heijden and others, *Energetic materials: crystallization, characterization and insensitive plastic bonded explosives*, „Propellants Explosives, Pyrotechnics” 2008, No 33, pp. 25–32.

Abstract

The article presents issues that include various imaging techniques used in forensics. Technology development observed in the modern world, implies changes in all areas of life, improving, speeding up and opening them to new research capabilities. The use of advanced technology allows precise analysis of the evidence. The opportunity to observe different samples at high magnification is necessary in the performance of their documentation (examination of the morphology of the surface, setting the diagnostic characteristics). The application of optical microscopy, electron microscopy or atomic force microscopy, and integrated spectroscopic systems is an essential and powerful tool for implementation observations of a variety of materials.

Keywords: imaging techniques, microscopy, SEM, X-ray microanalysis, EDS, Raman spectroscopy, atomic force microscopy, AFM.

Acknowledgments

In this article some of the results of the research were presented. The study was supported by NCBiR, Nr 0023/R/ID3/2012/02 and provided in pyrotechnic and structure of the toner surface range.

Slawomir Gladysz

Counter-terrorism powers of national authorities

With a provision of the Law on the Counter-Terrorism Operations of 10 June 2016¹ some criticism and anxiety aroused in concern with the powers assigned to the security services, especially the operational powers assigned to the Internal Security Agency. These powers – according to the skeptics of that regulation – have influence on rights and civil freedom and they breach the constitutional principles of protection of the citizen's right of free communication and privacy.

The most frequent foundation of the a/m statements is the anxiety for creation of the law that would justify breaching, by the state's apparatus, all rights constitutionally protected, that under any circumstances should not be touched. It is visible *a priori* to assess the situation from the perspective of the security, in which it is known that no one in their right mind will threat or violate it. Then, the assumption made at the beginning of this paragraph about the inalterability of certain freedoms, and no possibility of suspending them, would be right. Unfortunately, such an approach to security-related issues seems naive.

Rational and at the same time pragmatic attitude in these matters conveys the necessity of going beyond ideals and prepare the state and its institutions to act in the situation of the highest threat or counteract the effects of events that have already taken place. These preparations should include both formal aspects, specifying the basics and scope of actions, and real – by indicating how to use these tools in accordance with the law.

It should be noted that legal structures in the Polish legal system that allow limiting or suspending the use of full civil rights in certain situations have been already existing². They provide that in the event of particular threats preventing the normal functioning of the institution under specific constitutional measures, a state of emergency may be introduced, which may involve a restriction of freedom and human and civil rights.

According to the author, the catalogue of specific threat events shall be supplemented by threats of a terrorist nature, especially those bearing attributes of an offence. The given stance can be reassured i.a. by the regulation on broadly understood anti-terrorist activities discussed in this report.³

¹ Journal of Laws 2016, item 904.

² States of emergency include: martial law – Act of 29 August 2002 on Martial law and on the competences of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional organs of the Republic of Poland (Journal of Laws 2017, item 1932); state of emergency – Act of 21 June 2002 on the emergency state (Journal of Laws 2017, item 928); and natural disaster – Act of 18 April 2002 on the Natural disaster state (Journal of Laws 2017, item 1897).

³ It is possible to discuss whether combating terrorist offences is a “special threat” within the constitutional concept resulting from Journal of Laws art. 228 paragraph 1, nevertheless the logical

It is therefore logical that in order to save the common “greater good” as citizens, we will be ready to give up certain attributes of functioning in the state. No one has or at least no one should have any doubts about it. The common sense of threat felt by citizens, causes flexibility, thanks to which the use of even bothersome restrictions will be accepted by them.

Regardless of the necessity to point out the foundations and scope of the functioning of state institutions in identifying, preventing and counteracting terrorism, the arguments for the implementation of new regulations⁴, in the author’s opinion, are effective measures recognized by the legislator in the 90’s of the twentieth century used by the institutions that are responsible for ensuring security. Operational and procedural work based on “old”, proven methods, used for many years, has been supplemented by “new” solutions, i.e. the possibility of operational or process control of mobile communication means, no matter for a specific telephone number, but also for an individual number of the telephone (IMEI), the ability to track the spectrum of telecommunications frequencies or other information that can be obtained from the operational and technical security divisions.

Then, at the turn of 20th and 21st century, it seemed that the saying “criminals are always one step ahead of us” might be outdated for just a moment. At the beginning of the 21st century, while conducting one of the cases, the author determined the way of communication of suspected individuals, who were citizens of neighboring countries. They agreed on a kind of “security system” to keep their criminal activities covert. It consisted of using one SIM card for a maximum of one month, and one telephone did not support more than three SIM cards and after six months it had to be changed. And they were just simple criminals...

This example shows that the development of know-how, technology, communication, especially in relation to the globalization of every area of life, causes that the bodies appointed to recognize, counteract and fight crime will always be behind the criminals aiming for the hermeticity of their environments and the secrecy of their connections, hiding their real plans and intentions. The only question is how far they will be left behind.

It is obvious that the services aren’t (or weren’t – before June 10th, 2016) helpless in the implementation of their statutory competences, especially in terms of ensuring security. As shown by the various types of publications, the actions taken by the services ensure internal security at a certain, satisfactory level. The criterion of this assessment is based on the existence or not of terrorist incidents. At the same time, the borders between the citizens’ awareness that this security was assured, because

interpretation of related norms supports such a position. Well, in the regulation of the state of emergency, its introduction was indicated, among others, threat to citizens’ security and public order. It should be agreed that a possible terrorist attack would harm these goods. It will be an issue to assess whether a given terrorist, event can cause a situation in which ordinary constitutional measures are not enough to fight or counteract it.

⁴ Adapted to new times, technologies, and society, etc.

nobody planned anything, realizing that certain actions were broken by the services at the right moment, and that their potential continuators are deterred by the effectiveness of security services – is (or was) invisible.

The introduction presented above shows two basic points of view of the issues related to the powers of services perceived in the terms of civil rights and freedoms. On the one hand, they are based on the admissibility of certain tools, on the other hand they concern the scope and methods of using them.

Exposing issues related to the state domain in the field of security, in particular protection against terrorist threats, and legal regulations in this area may dispel doubts as to the legitimacy of equipment the state authority in specific instruments of action. The analysis shows that the regulations of this area arise from various legal acts, and their citation, even if signaled, may allow an objective and rational evaluation of the provisions of the Act on anti-terrorist activities.

1. General issues

In accordance with Article 5 of the Constitution of the Republic of Poland of April 2nd, 1997⁵ – The Republic of Poland safeguards the independence and inviolability of its territory, ensures freedoms and human and civil rights, and the security of citizens. This standard defines the basic, general functions of the state and its fundamental goals, which mainly consist in the protection of the territory, freedom and security of citizens. The mentioned values are also the basis for the functioning of the state apparatus, and especially its institutions, which were appointed to guard them, regardless of the source of the potential threat.

It is obvious that the most important goods to be protected are: the state as an independent entity with its territory and citizens with their rights, and thus, in fact, the most valuable element of the state. This protection means in fact ensuring a state of security, i.e. creating a situation in which regardless of the level of danger, actions taken by state authorities will rise citizens' trust and understanding of their necessity, and at the same time correctness and effectiveness. The concept of ensuring security, however, requires a narrow interpretation, because it should only be a certain reaction, although also of a preventive nature, to real or potential (but still plausible) threats and attacks.⁶

For the purposes of this article, the focus should be on defining the term *citizen security*. According to the definitions of the *Dictionary of the Polish language*, the term *safety* is understood as a state of non-hazard, functioning in the normal mode without the threat of a specific event, negative in its consequences. On the other hand, *public safety* means all conditions and institutions protecting the state and citizens from dangerous phenomena threatening the legal order, and

⁵ Journal of Laws 1997, No 78, item 483.

⁶ P. Sarnecki, *Artykuł 5*, in: *Konstytucja Rzeczypospolitej Polskiej. Komentarz I, Wstęp*, Art. 29, L. Garlicki, M. Zubik (scientific editing), Warszawa 2016, p. 234.

protecting the system against attacks on the basic political institutions of the state.⁷ However, this definition – excluding from its scope “other people” staying or functioning in the structures of a given state – would be an unauthorized restriction of this concept. “Other people” are also protected; they are also element of public safety.

In the author’s opinion, the above entitles to claim that the determination of the security of citizens is a kind of *lex specialis* of public security, which the state has taken upon itself a special legal obligation to protect it.

Another duty of the state under the Article 5 of the Constitution of the Republic of Poland is to ensure freedom and human and civil rights, which expressly lead to the second chapter of the Constitution of the Republic of Poland. It is worth citing here the French *Declaration of Rights of Man and Citizen of August 26th, 1789*⁸, especially its article IV, saying that: *Freedom consists in the possibility of doing everything that does not harm another; in this way, the exercise of the natural rights of every human being has no limits other than those that ensure that the same rights are enjoyed by other members of society.* These limits can only be determined by statute. Despite the passage of almost 230 years from this regulation, the commentary to its record is in fact unnecessary.

In Polish legislation, freedom is generally understood as the sphere of rights that law does not create, but only defines their limits. In this case, it is the state’s duty to prove that the individual has violated these limits. On the other hand, in the case of *law*, the catalogue of which is established by the State, the entity must invoke a specific legal basis in the course of their investigation.⁹ It means the freedom of human action wherever the law allows that. This is a total reversal of the situation existing in relation to the state and its organs. The state body operates where it has been authorized by law and acts, citing the legal basis. A citizen can act wherever the law did not introduce bans, and did not forbid certain acts.¹⁰

Referring to the earlier definition of public security, in which its qualified form was pointed in reference to “citizens”, a similar procedure should be indicated, establishing the general rights common for all people, as well as those closely related to formal state affiliation. It is the result of a special obligation of the state to provide protection and a sense of security especially to its citizens, without ignoring the basic, necessary rights belonging to all people residing on the territory of the Republic of Poland, regardless of their state, nationality, racial, religious or political status.

The manifestation of this is the Article 31 of the Constitution of the Republic of Poland, in which legal protection of human freedom was established, but at the same time it was indicated when, and on what basis the indicated rights and freedoms

⁷ <http://sjp.pwn.pl/slowniki>.

⁸ Text of the *Declaration* was published on web page <http://libr.sejm.gov.pl/tek01/txt/konst/francja-18> [access: 23 I 2017].

⁹ W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej, Komentarz*, Warszawa 2013, p. 42.

¹⁰ *Ibidem*, p. 45.

may be limited. It is obvious that the rights, especially the rights of freedom, cannot be unlimited. The Article 31, paragraph 3 of the Constitution of the Republic of Poland provides guidance on how to determine these boundaries and how far limits can be allowed.¹¹ These guidelines result directly from the editors of the norm and specify that restrictions that can only be established in statute, and only when they are necessary in a democratic state for its security or public order, or for the protection of the environment, public health, morality or the rights and freedoms of others.

The above provides guarantees for the protection of rights and freedoms, at the same time by introducing clauses limiting these rights and freedoms – the formal ones, setting the minimum rank of a legal act¹² constituting a limitation, and the material ones, dependent on the implementation of a specific task by the state. The tasks listed have been divided into three groups, including: security and public order; environment, public health, public morality; freedom and rights of other people. Restrictions introduced of any of these reasons do not violate the principles of a democratic state ruled by law, but on the contrary – they are necessary.¹³

When discussing constitutional norms, it is worth paying attention to the relevant provision from the point of view of this article, namely Article 37 of the Constitution of the Republic of Poland. It introduces the principle of equal use of freedoms and constitutional rights by all people, both citizens and foreigners in the area covered by the authority of the Republic.

A foreigner, according to the definition of the *Act of 12th December 2013 on foreigners*¹⁴, is anyone who does not have Polish citizenship¹⁵, regardless of whether one has any foreign citizenship (stateless person). Exceptions from the above-mentioned rule, particularly referring to foreigners, can be regulated in statutes. The legislator did not indicate a specific legal act, which could impose restrictions on the enjoyment of rights and freedoms by foreigners, but defined its rank, confirming¹⁶ the necessity of these regulations by means of statutes.¹⁷

Summing up, the Constitution of the Republic of Poland imposes on the state a special obligation to ensure public safety while guaranteeing the respect of freedoms and human and civil rights. These freedoms may be limited, however, by the legal act issued by the parliament .

One of the reasons for introducing restrictions on the rights of human and citizen freedom is the necessity to ensure security which may jeopardized, among others,

¹¹ P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997*, Warszawa 2008, p. 48.

¹² As indicated above, this act should have the status of a law, a generally applicable legal act issued by the highest legislative body, in a special mode and having a high position in the structure of sources of law.

¹³ P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej...*, p. 49.

¹⁴ Consolidated text: Journal of Laws 2017, item 2206.

¹⁵ Article 3 (2) of the Act on Foreigners.

¹⁶ Article 37 (2) of the Constitution of the Republic of Poland.

¹⁷ Article 31(3) of the Constitution of the Republic of Poland.

by various phenomena and threats of a terrorist character. This threat is important especially now that it defies traditionally understood definitions, and their potential perpetrators act out of the box, often targeting random people, infrastructure or simply striving to make the greatest damage.

To counteract this, the state must comprehensively prepare itself by equipping the competent authorities with instruments and tools that allow to undertake immediate and adequate measures to respond to threats and – in the time of attack – also to remove its consequences.

Precise regulation of the activities of state authorities in the face of terrorist threats, regardless of their level, should be the standard adopted by the state, independently of the political environment from which the ruling party originates.

The effectiveness of such regulations will depend on the close and comprehensive cooperation of all services, bodies and institutions involved in broadly understood anti-terrorist activities with approval – and even support – of the mass media, non-governmental organizations and the whole society.

2. Competent authorities in matters of terrorism

In Poland, bodies appointed directly under the Act to deal with broadly understood issues related to terrorism are the special services: the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service and the Military Intelligence Service, as well as the Military Police and the Police. The leading role in the issue of recognition, prevention and detection of terrorism-related offenses has been assigned to the Internal Security Agency, which is reflected in the force-based provisions of competence. The mentioned Article 5 contains a relatively broad approach to the tasks of the Internal Security Agency in the area of terrorist crime.

In fact, it is difficult to overlook also other bodies, whose significance at various stages of phenomena related to terrorism cannot be overestimated, but their tasks do not result directly from the rules, but rather from the logical or systemic interpretation of their powers. Among others the State Fire Service¹⁸, the Polish Border Guard¹⁹, or the Government Protection Bureau²⁰, however, due to the generality of the subject,

¹⁸ The State Fire Service is the main service responsible for conducting rescue operations in the field of saving lives and human health and protecting property and the environment in the event of an emergency. The tasks of the State Fire Service include undertaking activities in the field of hazard identification, including contamination with chemical and radiation substances, as well as conducting preliminary biological reconnaissance operations. The entities undertaking rescue tasks operate within the framework of the National Rescue and Firefighting System. All rescue operations during a terrorist threat are based on maintaining the priority of saving lives and health and the technology of actions aimed at minimizing the effects of an event.

¹⁹ These activities include protection of state borders, including maritime borders, organization and control of border traffic as well as prevention of illegal crossing of state borders and prosecution of perpetrators of such offenses. The Border Guard also carries out tasks in the area of ensuring security in international communication, including on board aircraft performing air transport.

²⁰ The Government Protection Bureau is competent in the protection of statutory defined persons,

the author focused on the main organs appointed to deal with the phenomenon of terrorism and the instruments of action assigned to them. Presentation of these tasks and tools, in which the legislator provided organs for their implementation, will create a starting point for discussing and assessing the provisions of the Act on anti-terrorist operational actions.

2.1. Internal Security Agency (ABW)

Article 5, paragraph 1, point 2 of the *Act of 24th May 2002 on the Internal Security Agency and the Foreign Intelligence Agency*²¹ indicates that the recognition, prevention and detection of crimes, including terrorism is a part of the tasks of the Internal Security Agency. In this respect, the Agency's activity can be carried out both in the country and abroad.

They consist of activities undertaken on four levels, which the legislator has grouped in the terms.²²

- recognition – according to the definition, it means identification of someone or something, research and undertaking activities aimed at obtaining information about an opponent²³,
- detection – stands for establishing facts about someone's participation in something, disclosing things that were supposed to be secret²⁴,
- prevention – taking actions aimed at preventing something bad to happen.²⁵

In addition, the legislator indicated that the Internal Security Agency is obliged to prosecute the perpetrator of crimes remaining in its material jurisdiction. This means that the Internal Security Agency has the option of legal utilization of its operating materials.²⁶ This is important at the stage of operational and procedural cooperation, as officers from specific departments can often afford to conduct free dialogue and a loose, informal exchange of comments and needs, aimed at determining the appropriate directions of both the given operational case and the criminal proceedings.

The indicated tasks are the ABW's ability to identify, confirm and taking preventive and procedural measures. The above-mentioned four action plans can occur selectively, individually, and cumulatively. The model situation would be to

facilities and equipment that may become the potential target of terrorist attacks.

²¹ Consolidated text: Journal of Laws 2016, position 1897 – therein: the Act on the Internal Security Agency and the Foreign Intelligence Agency.

²² Perhaps they are obvious, but in the context of the fundamental purpose of this article, i.e. the analysis of the law on anti-terrorist activities, it is worth defining and defining their foundations of meaning.

²³ <http://sjp.pwn.pl/szukaj/rozpoznawanie.html>.

²⁴ <http://sjp.pwn.pl/szukaj/wykrywanie.html>.

²⁵ <http://sjp.pwn.pl/szukaj/zapobieganie.html>.

²⁶ The author met with numerous voices of representatives of other services who do not have these capabilities, indicating that the investigations frequently conducted on their operational materials did not have proper operational support, which put the unsatisfactory process results.

have operational and analytical capabilities that would make the recognition process the fastest, the most effective and the most accurate. It depends on further activities of an operational nature, and actions taken in the last phase of the process. Recognition gives the advantage, time and possibilities to take effective and adequate responses to a specific threat. The next stage, detection, is the consumption of identification activities. It is at this stage that the Internal Security Agency will confirm the existence of reasonable suspicion of committing a crime. Then the verification of the collected operational material and its possible process of legal utilization take place. Depending on the type of threat identified, its scale and timeliness, further activities of the Internal Security Agency may take the form of a response adequate to the threat aimed at its leveling or liquidation. This can be achieved both by the dynamic use of force²⁷ and in long-term activities of a preventive nature. Such activities should, however, lead to a certain goal – which means either to prevent the escalation of the threat or to gather evidence to apprehend the perpetrators and prepare the charge indictment for the court.

According to the Article 21 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, to perform their duties, i.a. in the CT aspect, officers conduct operational, as well as investigate activities. Despite the fact that these three kinds of activities are basically different from and dependent on each other, such division of work is fundamental for the functioning of ABW. To sum it up briefly: the more information is gathered at the operational stage, the better assumptions can be made later by the investigators which results in more effective legal proceedings.²⁸

The described relation resulted in granting investigative powers (similar to these used by the Police, resulting from the provisions of the Code of Criminal Procedure) to the ABW officers.²⁹ The importance of this provision was already mentioned at the beginning of this chapter. It is systematically linked with the Article 22a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, which – if the gathered material indicates the probability of a perpetration of a crime – allows the Head of ABW to present it to the prosecutor to decide if any further legal proceeding should be initiated. Therefore, it can be supposed that ABW should be the first institution tasked by the prosecutor's office to conduct an investigation³⁰, whenever the presented material is considered valid and the investigated crime lies within the remit of the Agency.

A certain exception from the rule stipulated in Article 22a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency has been made by the legislator. Whenever the Head of ABW gets in possession of information indicating

²⁷ That is why it is so important to be able to use them, and according to the author, within the framework of criminal proceedings or directly at the disposal of the Head of the Internal Security Agency.

²⁸ Interesting is that his “obviousness” is not so clearly visible for the ABW officers.

²⁹ Art. 21 (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

³⁰ According to art. 303 of the Code of Criminal Procedure this happens when there is a good reason to suspect that an offence has been committed, and the act can be described, as well as its legal classification can be set forth.

a possible terrorist activity he may – for national security reasons – renounce from informing the prosecutor about the justified suspicion of this crime or its suspected perpetrator.³¹

Another amendment allows the ABW officers³² to cooperate with a person suspected of committing a crime of a terrorist nature. It can be done only if all circumstances of the committed crime or conducted activity have been deliberately and voluntarily revealed by the mentioned person, and a commitment to cooperate with ABW was signed.³³

The decision of the Head of ABW of not informing the local prosecutor must be reviewed by the General Prosecutor, as well as by the member of the Cabinet competent in the matters of coordination of special services.³⁴ The mentioned exceptions are first tools provided by the act of law that can be used by ABW to perform its duties, especially to investigate, detect and prevent crimes of a terrorist nature.

As it was mentioned earlier, the legislator created an exact catalogue of activities that can be done by the state (represented in this case by the officers of ABW) to fulfill its tasks. The analysis of the service's competences shows that they can be divided into three fields: administration and public order³⁵, covert operational activities, and investigative powers.³⁶ Due to the fact that the goal of this publication is to describe the provisions of the Law on the Counter-Terrorism Operations, the author focuses only on these covert operational activities of ABW which are essential in fighting terrorist crimes, this means:

- to request blockade of telecommunication;
- to request blockade of accessibility of certain data in IT system;
- to perform a security check of IT system;
- to initiate operational control;
- to collect personal data (also in a covert manner);
- to make use of information described as bank secrecy and information from agreements on cash accounts, insurance or other agreements related to financial instruments, money services or investment funds;

³¹ Art. 22b (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, added by the Law on the Counter-Terrorism Operations. Such exception cannot be executed when the suspected terrorist committed a crime against a person resulting with death or serious detriment to the health of a person, was involved in committing such crime or instigated to commit it. It involves also a person who – while being a covert informant – has not revealed all relevant information and continues to conduct activities against the Republic of Poland, or committed any of the above-mentioned offences despite his covert cooperation with the service.

³² There has been no such possibility since the establishing of the UOP and, later, the ABW, neither in the CI nor in the CT field.

³³ It remains unclear how such cooperation should be initiated – by the person, as a “walk-in” or by the officers of the Agency, after the person was identified and offered to cooperate (“to cooperate or to be persecuted”).

³⁴ Art. 22b (4) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

³⁵ A right to issue an instruction to behave in a requested manner, to check a person's identity, to conduct personal searches, to photograph and record fingerprints, and to use firearms and means of coercion.

³⁶ Based upon the legal procedure code, supported by an internal “instruction on investigation”.

- to covertly buy or seize objects from an offence;
- to request a covert oversight of production, transport, storing and trading of subjects from an offence;
- to accept the assistance of informants who are not officers of ABW.

The first of means presented above, the blockade of telecommunication³⁷, is used as a reaction on a high threat level in a certain field. The indicators of such threat are listed in the empowering measure of the Internal Security Agency; they are: threats to internal security of the state and its constitutional order, as well as most serious offences threatening the state. Despite such broad definition of conditions allowing to use the blockade of telecommunication this procedure seems to be related exclusively to the defined and probable threats, like an act of violence directed against the constitutional institutions of the state or an attempt of a terrorist attack. In such a situation (like in the case of a terrorist attack) the blockade of telecommunication becomes a tool enabling to gain time for mobilization of means and powers which can be later directed to the venue to perform the official duties. It is not difficult to imagine that using this power could mitigate the spreading of potential destruction or prevent the criminal activities aimed at public security.

To use this power the Head of ABW first defines its territorial range and then informs of this fact the President of the Office of Electronic Communications. The lack of precise definition of the time period for which such decision may be valid, seems significant here. The legislation uses only an unclear expression “for the time necessary to perform the duties” which is a result of an unpredictable nature of situation when the blockade of telecommunication is vital. The only limitation in such activities is minimization of the results stemming from the lack of possibility to use means of telecommunication.

The activities described above are linked with an ability to block the accessibility of certain data or services in IT system, in case of a terrorist incident.³⁸ It can be performed on request of the Head of ABW to block the accessibility to “prevent, counter and detect offences (...) and to pursue the perpetrators”³⁹ which should be addressed to the District Court in Warsaw, entitled to decide in this matter.

To formalize the request there is a need to obtain a written permission of the General Prosecutor. There is also an option to put the request into power immediately. In such a case the Head of ABW may request to establish a blockade of accessibility after receiving the permission of the General Prosecutor, and in the same time the request is passed to the court to get the final approval. If the court refuses to approve the request within five days since the blockade has been put into power, these activities must be stopped. The blockade of accessibility can be requested for no longer than 30 days with a single option of extending this period for three months.

³⁷ Art. 26a of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

³⁸ Art. 32c (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

³⁹ The quotation marks were used intentionally, due to the opinion of the author that a legal inaccuracy happens here – according to Art. 5 (1) (2) the tasks of ABW are “to investigate, prevent and detect offences”. “Countering” is a new kind of tasks described by the Law on the Counter-Terrorism Operations. The issue will be elaborated later on.

Another IT tool that remains at the disposal of the Head of ABW is the ability to perform a security check of mentioned IT systems, allowing to verify the vulnerability to attacks which may harm their integrity, confidentiality, accountability and accessibility.⁴⁰ Interesting is that the legislator granted ABW the right to design or acquire devices or software mentioned in Art. 269b of the Criminal Code⁴¹, as well to use them.

The operational control is defined as acquiring and recording: communication with use of technical means, including IT networks; video footages or sound recordings from means of transport or places other than public; correspondence (also from the electronic channels); information from IT data carriers, terminals, informational and IT systems, as well as acquiring access to postal letters and packages to control their content.⁴²

After years of discussions, the mentioned power was adjusted to follow the reality. The operational control gives a lot of opportunity to intrude into someone's privacy, however in the first place it should be assumed that national entities uphold the rule of law. A hypothesis – known to the author from the case of introducing the “posteriori approval” procedure – saying that “it is easily imaginable that an officer illegally uses acquired data” is, in the author's opinion, inadmissible. The main rule is to use granted powers accordingly with their intention, after fulfilling appropriate criteria and with due diligence. The author's experience from his service in ABW allows to conclude that such standards (sometimes even more restricted ones) are being met whenever the power of Article 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency is executed. In other words, it cannot be imagined that an officer misuses information acquired by the operational control.⁴³

To perform its duties related to investigate, detect and prevent crimes, i.a. of a terrorist nature, the court, on a written request made by the Head of ABW, may issue the decision to start the operational control.⁴⁴ An additional criteria to fulfil while requesting the operational control is to prove the ineffectiveness or uselessness of other covert means.

⁴⁰ Art. 32a (1) and (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁴¹ The described provision seems inaccurate – the referred point of the Criminal Code relates to destroying, deleting or changing IT records that have a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information. It may be assumed that this provision may allow to perform simulation of potential results of an attack, however the point 8 of the article stipulates: “(...) to acquire access to data (...) by breaking or passing by its electronic, magnetic, IT or any other means of protection”, which suggests a possibility of using more offensive actions.

⁴² Art. 27 (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁴³ To avoid idealization, the violation of the mentioned rule cannot be fully excluded, but it remains exceptional. It is commonly thought that the surveillance materials (especially stemming from tapped wires) are sensational, uncover the deepest secrets and keep the thrill from the beginning to the very end. In real life these sensational recordings are rather a tedious, exhausting and psychically-burdening toil, demanding to listen, re-write and verify enormous amounts of data to gain a potential result.

⁴⁴ Art. 27 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

The request for operational control must be verified at two stages. First, the request of the Head of ABW needs the approval of the General Prosecutor, made in written form. Such legitimization of the request for the operational control entitles the Head of ABW to reach the court. The court may, however, deny such form of control, if the operational materials used as the basis for the request deem insufficient.

There is also an urgent mode of this procedure. According to the Article 27 (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, in case of a risk of losing the information or of destruction of evidence the Head of ABW may run the surveillance – the need to acquire a written agreement from the General Prosecutor is in such a case still pending, and the request for the decision must be presented to the court at the same time.⁴⁵

As it was earlier mentioned, the operational control gives the opportunity to i.a. tap telephone lines, install hidden video cameras and microphones in buildings⁴⁶ and vehicles⁴⁷, control the correspondence (also electronic one), acquire and store data on electronic carriers, as well as to get access to the content of postal letters and parcels. Despite the fact that some of the mentioned covert means of surveillance are formally incomplete, they seem to allow to record activities of an ABW's person of interest in a multidimensional way – from traditional means of communication to the contemporary ones, including Internet and personal electronic devices. In the era of global network services the legal provisions of data access in different countries are not always compatible, however in Poland this question has been, in most part, formalized.⁴⁸

While discussing the matter of operational control, the ABW's ability to acquire and process communication data⁴⁹, i.a. telephone billings⁵⁰, postal packages⁵¹, internet

⁴⁵ If the court does not allow the operational control in the five-day period since the procedure has started, the Head of ABW stops the surveillance immediately and any acquired materials are to be formally destroyed.

⁴⁶ Differently from the regulation of Art. 23 (1) (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, these activities are conducted in private spaces.

⁴⁷ Executive provisions are still lacking.

⁴⁸ There are still some misunderstandings with Polish Internet services' providers but the current practical cooperation positively influences the level of mutual understanding.

⁴⁹ Art. 28 (1) and art. 34 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁵⁰ Especially when there is a need to obtain information on network terminal, IT terminal, end user, call initiator, call receiver, date and time of connection and its duration, kind of connection or localization of the terminal – art. 180c and 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2017, item 1907).

⁵¹ To get information about the postal operator, provided services, as well as information allowing to identify the clients, to acquire the packages for communication or content control, to seize the package in case of a suspicion that it contains objects from a crime (for a formal inspection procedure), to admit a crime-related package for the further transport (either untouched or after substituting the content completely or partly, according to other regulations – Art. 82 (1) (1) of the Postal Law of 23 November 2012 (Journal of Laws 2017, item 1481).

data⁵², as well as any personal information⁵³ related to the Agency's persons of interest in the context of its tasks enumerated in Article 5 of the Act on the Internal Security Agency and the Foreign Intelligence Agency should also be mentioned. In such cases, especially in those related to telecommunication, postal or Internet data, the judicial review was also introduced. This means that the proper court has the right to be provided with all materials justifying the ABW's access to this kind of information.⁵⁴

The scope of information ABW is entitled to acquire has recently been broadened by the access to information protected by the bank secrecy and derived data.⁵⁵ Such information can be acquired to effectively prevent crimes enlisted in Article 5 (1) (2), to detect them or to establish their perpetrators and gather evidence. The access procedure includes a formal agreement made by the District Court in Warsaw determining the kind and the scope of provided data, as well as the entity obliged to grant the access.⁵⁶ It needs to be pointed out that the Head of ABW has 120 days to inform the entity about the fact of obtaining the data related to it. If such information could harm the ongoing covert actions⁵⁷ the court – on the Head of ABW's request – can postpone this date⁵⁸. The ability to pass to an entity information about acquiring data related to it and protected by the bank secrecy and derived data also depends from gathering material allowing to initiate legal proceedings – or the lack of such possibility.⁵⁹ If the material has been gathered the prosecutor informs the entity before the investigation closes (it can also be done by the Head of ABW, on the prosecutor's request) or – with no hesitation – after it had been closed. If there is no sufficient material it is done immediately after the local prosecutor's office rejects to open the investigation.

Whenever ABW obtains credible information concerning a crime that remains within its remit, it may initiate activities to covertly buy or seize objects from an offence or other objects that cannot be legally produced, owned, transported or traded. Such procedure also relates to controlled acceptance or giving a material benefit.⁶⁰ These activities cannot be understood as playing leading role in the criminal process – they are designed to detect perpetrators and gather sufficient evidence.

⁵² Especially when it relates to surname and family name(s) of the client, personal identification number or the passport number, personal ID or other identity document, permanent or postal address, verification data of client's e-signature – Art. 18 (1-5) of the Act on Electronic Services of 18 July 2002 (Journal of Laws 2017, item 1219).

⁵³ Especially the personal identification number and data related to racial or ethnic background, political opinions, religious or ethical beliefs, religious or political or trade-union affiliations, health data, DNA, addictions or sexual relations, information concerning previous convictions, penalties and fines, as well as other decisions issued in court or administrative proceedings – Art. 27 and 28 of the Act on the Protection of Personal Data of 29 August 1997 (Journal of Laws 2016, item 922).

⁵⁴ Art. 28a (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁵⁵ Art. 34a (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁵⁶ Art. 34a (6) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁵⁷ Such risk must be considered probable.

⁵⁸ Art. 34a (9) and (10) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁵⁹ Art. 34a (11) and (12) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁶⁰ Art. 29 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

The Head of ABW is designated as authority to order the a/m measures, after being granted a written permission by the General Prosecutor, who is also provided with all covertly acquired material, if the fact of crime perpetration has been confirmed.

Covert oversight of production, transport, storing and trading of subjects from an offence can be initiated in the same manner – after receiving a permission from the General Prosecutor.⁶¹ The only condition in this context is to prevent any risks to human life or health. In this case the legislator obliges national entities (especially the custom entities and the Border Guard), as well as postal and cargo entities to cooperate closely with ABW.

The ability (stemming from a major rule named *argumentum a maiori ad minus*) to apply the operational control both by “covert acquisition” and “covertly supervised package”, needs additional attention.⁶² The reason for that is the high probability of the fact of a crime and the need of an efficient control of all participants of such activities. It allows to obtain evidence from multiple sources that confirm the reason of criminal inspiration or perpetrators’ motivation, often leading to discovering the true principals and initiators of the transactions.

All of the a/m activities are based on the cooperation with informants⁶³ assisting the ABW officers in performing their duties. It is considered an essential element of building the informational competence of a service. The activity is – paradoxically – underestimated by “newcomers” and overrated by the “old hands”. The true power of this operational tool is its apparent simplicity and directness of obtaining knowledge. This form of work can also be easily modified and planned: from individual tasking to long-term undertakings concerning multiple aspects.

The presented instruments may be used by officers to investigate, prevent and detect i.a. terrorist crimes. Additional means are the ABW’s analytical abilities, as well as its coordination powers, directly pointed in Art. 40 of the Act on the Internal Security Agency and the Foreign Intelligence Agency: (...) *the Head of the ABW coordinates all covert activities of special services that may influence national security.*

2.2. Foreign Intelligence Agency (AW)

According to Art. 6 (1) (5) and (7a) of the Act on the Internal Security Agency and the Foreign Intelligence Agency, the tasks of AW are: (...) *to investigate international terrorism, extremism and international groups of organized crime, as well as (...) to investigate, counter and prevent terrorist incidents aimed at citizens or property of the Republic of Poland abroad, with exclusion of terrorist incidents aimed at personnel or property of the Polish Armed Forces.*

⁶¹ Art. 30 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency – according to provisions of Article 27.

⁶² Art. 31 of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁶³ Art. 36 (1) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

In addition to the previously described and defined terms (while describing the tasks of the ABW), “to investigate” and “to prevent” terrorist incidents or other incidents of such a nature, AW undertakes activities aimed at countering them.

To counter, according to the definition, means to prevent a negative phenomenon by undertaking certain activities⁶⁴. In the context of the AW’s competences it can be understood as gathering data and analyzing it for further distribution and utilization by other entities.

The main criteria enabling the AW activity is the threat for Polish citizens or property abroad. In this context, officers of AW initiate covert actions and conduct analytical activities.

As far as the activities related to administration and public order, as well as strictly informational ones⁶⁵ are common for both of the described Agencies, the very AW has only limited possibilities to engage in covert operations.

What is more, the operational activities of an offensive nature⁶⁶ can be undertaken on the territory of the Republic of Poland, however (...) *only through the Head of ABW*.⁶⁷

The obligation imposed on the governmental authorities to inform the Head of AW about events relevant to the external security and international position of Poland, especially regarding international terrorism, extremism and international groups of organized crime⁶⁸, seems to take an increasingly central place.

2.3. Military Counterintelligence Service (SKW) and Military Intelligence Service (SWW)

Article 5 (1) (2a) and Art. 6 (1) (2b) and (3a) of the Act on the Military Counterintelligence Service and the Military Intelligence Service of 9 June 2006⁶⁹ concern duties imposed on the services in the field of counter-terrorism.

SKW is in charge of identifying, preventing and detecting crimes connected with terrorist activities threatening security of the defence potential of the country, the Armed Forces of the Polish Republic and organizational units of the Ministry of National Defence. On the other hand, SWW is designated as the authority for the identification, counteracting and prevention of terrorist threats to personnel and property of the Armed Forces of the Polish Republic outside the country, as well as dealing with the consequences resulting thereof.

⁶⁴ <http://sjp.pwn.pl/szukaj/przeciwdzialanie.html>.

⁶⁵ Consistently with the role of AW – they are: gathering (also in a covert manner) any kind of personal data.

⁶⁶ Thus: operational control, purchase, in an implicit manner, or the takeover of objects, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence.

⁶⁷ Art. 6 (9) (3) (editorial note).

⁶⁸ Art. 41 (1) (3) of the Act on the Internal Security Agency and the Foreign Intelligence Agency.

⁶⁹ Consolidated text: Journal of Laws 2017, item 1879.

In analogy to the civil security services operating in Poland, SKW⁷⁰ is the competent authority to carry out the a/m tasks, whereas SWW fulfills them outside the country. The operational capacity of SKW was regulated similarly to ABW – however, with a few exceptions.⁷¹ The first and probably the major difference concerns the way of execution of appointed tasks by undertaking operational and exploratory activities, as well as analytical and informative, but excluding investigative activities. Thus, SWW plays an active role in recognition of the given issue remaining its responsibility until information justifying the suspicion that a crime has been committed becomes available. The next step – pursuant to Art. 27 of the Act on the Military Counterintelligence Service and the Military Service – is to inform the competent Prosecutor’s Office or pass on the information to other competent authority.

The exceptions concerning the a/m similarity are: no access to data provided by banks, falling under the category of bank secrecy and tools used to block accessibility of specified IT data. The other activities i.e. the power to block telecommunications, operational control, obtaining telecommunication, mailing and internet data, collection (also in a covert manner) of all personal data, purchase, in an implicit manner, or the takeover of objects from an offence, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence, request for assistance from any person, as well as the procedure of their implementation, fall within the remits of ABW.

SWW is the military counterpart of AW in the area of competences, which also performs operational and exploratory, as well as analytical and informative activities. The offensive operational activities might be undertaken on the territory of the Republic of Poland only by SKW or ABW.

2.4. *Military Gendarmerie and Police*

The given uniformed services are a part of the governmental administration system established for the purpose of dealing with CT issues. Both, Military Gendarmerie and the Police, were granted the competences pursuant to the Law on the Counter-Terrorism Operations.

The powers of Military Gendarmerie are regulated by Art. 4 (1) (3a) of the Act on the Military Police and the Military Law Enforcement Bodies of 24 August 2001.⁷² Pursuant to the Law, Military Gendarmerie is entitled to perform counter-terrorism operations

⁷⁰ Military Counterintelligence Service is in charge of identifying, preventing and detecting crimes committed by soldiers fulfilling the active military service, officers of the Military Counterintelligence Service and the Military Intelligence Service, as well as the staff of the Armed Forces of the Republic of Poland and other organizational units of the Ministry of National Defence, as well as collaborates with i.a. Military Gendarmerie but only in performing the a/m activity. Interestingly, this new competence (referred to in point 2a) lacks the possibility to carry out the given tasks, whereas ABW has been granted such a possibility.

⁷¹ These are of crucial importance for identifying the position of the service within the CT system.

⁷² Consolidated text: Journal of Laws 2016, item 1483, as amended.

over areas or facilities owned by offices and agencies subordinate to the Minister of National Defence or supervised by him, or administered by these offices and agencies.⁷³

Noteworthy is the range of activities undertaken by Military Gendarmerie within their statutory powers, which include operational and exploratory, as well as investigative activities.⁷⁴ Those powers, exercised to fulfill own duties, correspond to the competences of SKW i.e. the power to block telecommunications, operational control, obtaining telecommunication, mailing and internet data, collection (also in a covert manner) of all personal data⁷⁵, purchase, in an implicit manner, or the takeover of objects from an offence, power to order covert surveillance of the manufacturing, transportation, storage and trafficking of objects from an offence and request for assistance from any person.

According to the author⁷⁶, granting investigative powers to Military Gendarmerie means in effect that the service has a leading role among entities under the Ministry of National Defence. Interestingly, it is not one of the special military services mentioned earlier, which in the light of the rules and powers perform strictly informative duties.⁷⁷

On the other hand, pursuant to Art. 1 (3a) of the Act of 6 April 1990 on the Police⁷⁸, police is carrying out counter-terrorist activities and therefore becomes the executive authority responsible for the physical elimination of threats.

3. The Law on the Counter-Terrorism Operations

Thus far, in this paper the author described the government administration bodies with appropriate competences, which pursuant to the Law were granted with certain measures and tools for identification, detection, prevention and countering of terrorist threats. The new powers, despite the interference with particular human and citizen rights and freedoms, were adopted with the aim of providing the national security in the widest meaning of the term. Granting the power to use these measures in order to execute statutory tasks by security services should not raise any doubts.

The general picture which emerges from the a/m observations is that security services are authorized to perform operational and exploratory, as well as investigative activities, hence are equipped with instruments enabling identification of a given issue at all stages

⁷³ The definition of counter-terrorism operation, as well as the source will be provided in the further part of the report.

⁷⁴ Art. 4 (2) of the Act on the Military Police and the Military Law Enforcement Bodies.

⁷⁵ Taking into account constraints deriving from the Act on the Protection of Personal Data.

⁷⁶ The author is aware that there are many opponents of the given stance.

⁷⁷ It is difficult to assess whether it is a disadvantage or advantage. There are many different opinions on the given matter, thus the saying "one's point of view depends on where one is sitting" seems accurate. However, experience shows that the farther apart the source is, the more distorted information or the emphasis put in an improper manner. This in turn reinforces the likelihood of its incomplete or improper use. In this situation, not only the structure of one institution at the operational level will be horizontal, but also the procedure will be repeated at the further procedural stage, however from top to bottom.

⁷⁸ Consolidated text: Journal of Laws 2017, item 2067.

and its further proceedings. At the same time, taking operational and exploratory, as well as analytical and informative measures – thus, oriented only at obtaining information and its appropriate operation. The same selection and ranking of government institutions have been set out in the specific provisions relating to terrorist offences.

With regard to the Laws stipulating the competencies of the Internal Security Agency, Foreign Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service, Military Gendarmerie and Police, on 10 June 2016 the Law on the Counter-Terrorism Operations was adopted – a *lex specialis* in the context of terrorist threats. The Law is the response to a long-expected legal regulation in the given matter, adopted to provide a solution to be used in a situation of a real threat, mobilize forces and resources and to respond effectively in the event of a terrorist incident and counteract its impact.

It should be noted, that the act of law regulating the identification, detection and prevention of terrorist threats helped to stipulate the roles and responsibilities of authorities, their capacities and actual tasks by putting the emphasis on the effective functioning of the state in a situation of a real threat.

The need for this regulation can be reaffirmed by *de lege ferenda* arguments put forward a few years ago by collegial bodies of the Criminal Proceedings Department of ABW.⁷⁹ At that time, it was proposed to consider taking up steps towards establishing new rules of statutory ranking, providing for a comprehensive regulation on identification, prevention, counteracting, neutralization and dealing with the effects of terrorist attacks, as well as specifying tasks and responsibilities to be taken immediately at the scene of incident by authorized services and institutions.

In order to discuss the content of the Law on the Counter-Terrorism Operations several definitions need to be clarified, thus confirming the validity and relevance of the regulation.

3.1. Definitions

Terrorist offence (Art. 115 par. 20 of the Criminal Code)⁸⁰ – a terrorist offence is a prohibited act with a sentence of imprisonment for at least five years, committed with the aim of: 1) seriously terrorizing a large number of people, 2) forcing a public authority of the Republic of Poland, or another state or international organization, to take or not to take a certain course of action, 3) cause a serious disturbance in the political system or economy of the Republic of Poland or another state or international organization, – or a threat to commit such an act.⁸¹

Such definition of a terrorist offence can be also found in other definitions of the offences embodied in the Criminal Code, i.a. in sections XVI-XXII, in which

⁷⁹ Task Force for developing a proposal for cooperation and management of tasks to be undertaken at the scene of a terrorist incident, established in 2013.

⁸⁰ Act of 6 June 1997 – the Criminal Code (Journal of Laws 2017, item 2204).

⁸¹ The motives of a potential perpetrator can be various i.a. religious, political or racial.

the most characteristic crimes are described in Art. 163⁸², 164⁸³, 165⁸⁴, 165a⁸⁵, 166⁸⁶ and 167⁸⁷. The given offences may or rather, as a rule, will include the actual concurrence with other crimes. Thus, there is no possibility to commit a terrorist crime without any connection to other illegal activity stipulated by criminal law provisions. However, it may occur only after a certain period of time that the given criminal offence was committed in relations to a terrorist crime.

Terrorist incident⁸⁸ refers to a situation when there are sufficient reasons to believe that it has arisen from a terrorist offence or a threat of such a situation.

While describing an incident, we can specify a scene of the event of a terrorist nature, which can be understood as an open or closed area where an event of a terrorist nature has taken place, or where its effects have taken or were to take place, as well as a space where threats related to the event of a terrorist nature are present.⁸⁹ The activities undertaken at a scene of the event by particular services immediately after the incident will represent very significant, but only a part of all measures to be taken by the competent authorities in relation to the incident that might have been of a terrorist nature. According to the a/m definitions, a scene of the event, as well as activities undertaken on site, are only components of a greater whole related to the complex examination of a terrorist offence (i.e. operational and exploratory, as well as investigative).

The act in question regulates the activities of the organs of public administration which are aimed at preventing events of a terrorist nature, preparations to take control over such events by means of planned undertakings, reaction in case such events occur and removal of their effects, including the recovery of the resources aimed at reacting to such events, referred to as antiterrorist activities.⁹⁰

The list of tasks includes also counter-terrorist activities mentioned before. The term should be understood as activities against perpetrators, as well as persons preparing or assisting in committing an offence of a terrorist nature, performed with the aim to eliminate the immediate threat to life, health or property, with the use of specialist forces or means, as well as specialist operational tactics.⁹¹

3.2. Terrorism – identification, prevention and counteracting

The Head of ABW and the minister competent for internal affairs have been given the central role in the provisions. By working together, the authorities are responsible for

⁸² Causing a life-threatening event.

⁸³ Immediate endangerment.

⁸⁴ Other endangerment.

⁸⁵ Financing terrorist activity.

⁸⁶ Piracy.

⁸⁷ Dangerous devices or substances.

⁸⁸ Art. 2 (2) of the Law on the Counter-Terrorism Operations.

⁸⁹ Art. 2 (6) of the Law on the Counter-Terrorism Operations.

⁹⁰ Art. 2 (1) of the Law on the Counter-Terrorism Operations.

⁹¹ Art. 2 (2) of the Law on the Counter-Terrorism Operations.

prevention of terrorist incidents, as well as taking control over events of a terrorist nature in case of the occurrence of such events by producing response adequate to the threat.

By increasing emphasis on combating terrorism, the legislator imposed on the a/m authorities the responsibility for the effectiveness and professionalism of activities undertaken by services and institutions in a threat situation or in case of a suspicion of committing an offence of a terrorist nature.⁹²

While discussing certain stages of an operation, we have to focus on those resulting from the Law on the Counter-Terrorism Operations, which are: identification, prevention and counteracting. The legislator designated the Head of ABW as the authority responsible for the prevention of terrorist incidents. The Law on the Counter-Terrorism Operations is a specific law referring to threats and incidents of terrorist nature, thus the majority of activities that can be carried out by ABW have been regulated in the Law on the Internal Security Agency and the Foreign Intelligence Agency. Designating the given powers to ABW supports the argument that there is a need for one centre responsible for gathering all information concerning terrorist incidents and giving instructions, in order to ensure efficient, quick and adequate response. The given responsibilities were assigned to the Head of the Internal Security Agency, who within the remits of analytical and informative, as well as operational and exploratory activities gathers information and coordinates activities undertaken by other authorities and public institutions, while at the same time conducting operational activities against individuals suspected of being involved in terrorism.⁹³

The Head of ABW is authorized to coordinate analytical and informative activities of Polish external and internal security services i.a. Military Counterintelligence Service, Foreign Intelligence Agency, Military Intelligence Service and Central Anticorruption Bureau, as well as other authorities i.a. Police, Border Guard, Government Protection Bureau, State Fire Service, Customs Service, General Inspector of Financial Information, General Inspector of Fiscal Audit, Military Gendarmerie and Government Centre for Security. The coordination arrangements include exchange of information on possible terrorist threats⁹⁴, as well as persons associated with terrorist activities.

Individuals of particular interest are divided into four categories:

- persons involved in activities on behalf of terrorist organizations or organizations connected with terrorist activities or members of such organizations;

⁹² Art. 3 (1) and (2) of the Law on the Counter-Terrorism Operations.

⁹³ Particular attention should be drawn to categorical statements, such as: “the Head of ABW coordinates”, which impose the obligation to take such actions. There is no room for an independent decision to take certain actions. This implies a need for taking coordinating measures by the Head of Internal Security Agency in the event of threat.

⁹⁴ In particular, incidents described in the catalogue of incidents and events of a terrorist nature included in the Directive of the Minister of the Interior and Administration of 22 July 2016 on the open catalogue of terrorist incidents (i.e.: Journal of Laws 2017, item 1517).

- wanted persons involved in terrorist activities or persons suspected⁹⁵ of committing offences of a terrorist nature, with regard to whom an arrest or a search warrant has been issued or a wanted letter has been decided on, as well as persons who are wanted and subject to the European Arrest Warrant;
- persons with regard to whom there is a justified suspicion that they are involved in activities aimed at committing an offence of a terrorist nature, including persons who might present a threat to civil aviation;
- persons participating in a terrorist training or undertaking journey with the aim to commit an offence of a terrorist nature.⁹⁶

The Head of ABW maintains a register including the a/m information.

Officers of ABW, Police and the Border Guard are entitled to take fingerprints or record the face image of individuals included on the list or a person who is not a citizen of the Republic of Poland in case when there is a doubt as to the identity of this person or there is a suspicion that the border of the Republic of Poland has been crossed illegally, or there is a doubt as to the declared purpose of the person's stay on the territory of the Republic of Poland. The organ, which has taken the fingerprints or recorded the person's facial image, shall transmit to the Commander in Chief of the Police the obtained data which are then entered in the Police databases.⁹⁷

In order to prevent events of a terrorist nature, the Head of ABW has free access to the data and information gathered in public registers and records that is kept in particular by: Military Counterintelligence Service, Foreign Intelligence Agency, Military Intelligence Service, Central Anticorruption Bureau, Police, Border Guard, Government Protection Bureau, State Fire Service, Customs Service, General Inspector of Financial Information, General Inspector of Fiscal Audit, Military Gendarmerie, Government Centre for Security, Head of the Office for Foreigners, President of the Office of Electronic Communication, President of the Office for Civil Aviation, President of the National Atomic Energy Agency, Social Insurance Office, President of the Agricultural Social Insurance Fund, Financial Supervision Authority, Land Surveyor General, local authorities and General Prosecutor.⁹⁸ The scope of the data includes also the image of events recorded by image recording equipment located in public venues, by public roads and other public places.⁹⁹

Pursuant to Art. 4 of the Law on the Counter-Terrorism Operations, organs of public administration, owners and holders of facilities, installations, and equipment of public administration infrastructure, as well as critical infrastructure¹⁰⁰, are obliged

⁹⁵ Whereas the Act refers to presumed suspects, what was probably meant were suspects toward whom there was sufficient evidence to issue a decision to present charges (not necessarily announced to the a/m persons).

⁹⁶ Art. 6 (1) of the Law on the Counter-Terrorism Operations.

⁹⁷ Art. 10 (1–6) of the Law on the Counter-Terrorism Operations.

⁹⁸ Art. 11 (1) of the Law on the Counter-Terrorism Operations. It should be emphasized, that this power encompasses also units subordinated and supervised by the a/m organs.

⁹⁹ It is worth mentioning that it concerns on-line streams.

¹⁰⁰ In particular, any potential threat to the functioning of energy, water and sanitation, heating and

to convey to the Head of ABW information they possess about terrorist threats to the infrastructure of public administration or the critical infrastructure and the Head of ABW can issue orders¹⁰¹ to them aimed at counteracting, removing or minimizing the threats.

Another area of activities imposed on the Head of ABW includes coordination of operational and exploratory activities undertaken by the special services and authorities mentioned in the previous paragraph, as well as activities performed by customs officers of observing and recording vision and sound of events in public spaces¹⁰². The operational and exploratory activities have to concern incidents of a terrorist nature. The Head of ABW can issue recommendations¹⁰³ to the entities, with the aim to remove or minimize the terrorist threat which has occurred.

Article 9 of the Law on the Counter-Terrorism Operations deserves particular attention. It refers to the extended scope of activities of ABW and includes, apart from prevention, also identification and counteracting of terrorist offences. The new competence of the Head of ABW, which has not been indicated previously, is counteracting, which according to a dictionary definition means any action against a person or object, overcoming an obstacle by taking long-term steps.¹⁰⁴

The given regulation stipulates that the Head of ABW may order covert activities (such as obtaining and recording the content of conversations by technical means, including with the use of telecommunication networks; image and sound of persons from premises, means of public transportation and other venues from public spaces; content of correspondence, including correspondence kept by means of electronic communication; data from data storage devices, telecommunication terminal devices; as well as information and IT systems and finally obtaining access and controlling the content of consignments)¹⁰⁵ with regard to a person who is not a citizen of the Republic of Poland, and with regard to whom there is a fear of possible involvement in terrorist activities.

The Head of ABW shall, without delay inform the Minister Coordinator of Special Services, as well as the General Prosecutor about the undertaken actions, who may order to stop the activities¹⁰⁶. These actions might be ordered for a period of no longer than three months with a possibility of extension, however under Art. 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency.¹⁰⁷

IT systems and networks, relevant for the national security.

¹⁰¹ These will likely be legally binding notices to take specific actions.

¹⁰² Art. 8 (1) of the Law on the Counter-Terrorism Operations.

¹⁰³ Although it is only a "recommendation" it is difficult to imagine a situation in which either authority – not having a comprehensive view of the situation – would refuse to follow such a recommendation.

¹⁰⁴ <http://sjp.pwn.pl/szukaj/zwalczanie.html>.

¹⁰⁵ These bring about associations with the operational control described in Art. 27 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, which make complete sense.

¹⁰⁶ Art. 9 (4) of the Law on the Counter-Terrorism Operations.

¹⁰⁷ It refers to judicial control of the validity of the extension.

The decision to undertake activities equivalent to the operational control¹⁰⁸, which is a single-stage procedure, comes to the fore. What is more, it should be emphasized that the procedure has been limited to foreigners who are not citizens of the Republic of Poland, and the powers of the Head of ABW were granted by a legal act of statutory rank. Thus, there are no grounds for questioning this legal basis and powers to carry out the given tasks.

By defining a specific threat, the legislator provided the Head of ABW with a possibility to undertake offensive operational activities. Having in mind that it refers to the concern for undertaking terrorist activities by foreigners¹⁰⁹, the normal procedure of initiating the operational control, on the basis of Art. 27 of the Internal Security Agency and the Foreign Intelligence Agency, could be hampered or even impossible. In order to apply the given procedure, any other operational measures would have to be ineffective or useless. The ever-evolving nature of terrorism makes it impossible to apply the standard operational activities that include a variety of actions from simple methods and measures to more sophisticated solutions, which very often require complex combinations or operational games. Time is of the essence¹¹⁰ when it comes to the implementation of the procedure. There is no place for hesitation when intelligence on a possible terrorist threat is obtained and an immediate and rational decision has to be made.¹¹¹ That is one side of such statutory solutions.

On the other side, the common perception of terrorism as homogenous is not always that obvious.¹¹² Terrorist activities include also logistical actions related to individuals against whom further procedural steps are to be taken and evidence is to be collected in order to take the case to court. Therefore, it gives possibility to identify the actual masterminds and other participants, as well as clarify their roles and identify potential targets. This, in turn, as it was mentioned before, gives advantages and possibilities to security services.

The aforementioned arguments indicate that the decision to grant the Head of ABW with the ability to undertake offensive operational activities in the light of the terrorist threat was correctly taken.

¹⁰⁸ Although supervision over the proper application of these activities is the responsibility of the General Prosecutor by the power to finish them, according to the provisions, the Head of ABW has the duty to immediately inform about the taken actions, which in practice might mean that they will be in force for a certain period of time.

¹⁰⁹ It refers to individuals, whose identity is very difficult or even impossible to be verified, as well as other data such as place of residence or criminal records.

¹¹⁰ Truly, the author did not want to mention that argument but that is the reality of any public administration body. In order to introduce certain actions, time in organization unit first is needed, then its implementation must be accepted by the unit, department and appropriate documents have to be passed to the other institution etc. Before sending a motion concerning the implementation of surveillance procedure to the Regional Court in Warsaw documents goes through a few organizations units (not even mentioning the supervisors, who have to accept these documents).

¹¹¹ This includes also taking responsibility for the decisions made.

¹¹² A suicide bomber, one faith believer, armed with explosives attached to a specified uniform.

Another approach, which is also significant in the given matter, cannot be ignored. As is was stated by Mr. Lech Paprzycki, who is the President of the Criminal Chamber of the Supreme Court (...) *for many years security services were operating (...) under limited prosecutor and judicial control*, he also added that the aspect of control should be in the interest of officers in order to ensure that activities (i.e. of an operational nature), undertaken by them, including counter-terrorist, are conducted in conformity with the law.¹¹³ Giving the Head of ABW the power to execute actions described in Art. 9 of the Law on the Counter-Terrorism Operations, without obtaining the prior consent of the court, may raise certain controversies, in particular in relation to the general obligation of judicial checks on applications for operational control imposed on all security services.

Considering the above, it can be assumed that specific circumstances require specific competences, and these require exceptional professionalism, accuracy and diligence. These qualities will guarantee appropriate and effective use of tools granted to the Head of ABW.

After finishing activities described in Art. 9 the Head of ABW passes all gathered materials to the general prosecutor, who decides about the scope and the way the materials will be utilized. An assessment, if the materials have enough evidence to initiate a criminal proceedings, is conducted by the general prosecutor¹¹⁴, who, if there is not enough evidence orders destroying the material.

The rules in the Act on anti-terrorist activities refer in a visible way to the proceeding field, which was extended to special opportunities as far as information obtained during conducted operational activities is used, which caused the appropriate reaction to the threat of terrorist nature. The author emphasizes that in case when the operational officer recognizes the terrorist threat it will be almost the end of the potential case at his level, whereas – as far as prevention and combating the above-mentioned threat, including gathering and securing the evidence in the legal process, and further arresting the perpetrators are concerned – the case will just begin.

A novelty in the criminal proceeding regulations are rules allowing to search at any time of day and night premises, including individuals staying in the certain rooms or in the certain premises.¹¹⁵ The decision is made by the prosecutor, who acts on the basis of the notion containing materials describing the suspicion, attempts to commit a crime or preparation to commit a crime of terrorist nature and justified suspicion basis, that the above mentioned things are there prepared by the appropriate ABW's unit. In an analogical situation the prosecutor can issue a decision to detain the suspected person.

¹¹³ L.K. Paprzycki, *Czy Polsce potrzebna jest ustawa antyterrorystyczna?*, in: *Terroryzm – materia ustawowa?*, K. Endecki, P. Potejko (ed.), Warszawa 2009.

¹¹⁴ It is indicated in Art. 27, para.15 Act on the ABW and AW, according to which the Head of ABW decides if material gathered from surveillance procedure has enough evidence to initiate a criminal proceeding, and if it has, it can be passed to the General Prosecutor.

¹¹⁵ Article 25 (1) of The Act on anti-terrorist activities.

Analyzing the above regulation it can be assumed that information concerning what or who needs to be found must be limited to justified suspicion¹¹⁶ and describe precisely according to which criminal case must be gathered and verified. These knowledge not necessarily contains the grounds on the basis of which the investigation may be initiated, in which it is crucial to justify the suspicion of crime¹¹⁷. It seems that result of performed activities will set grounds to take the decision of initiating or refusal of instituting a preparatory proceeding. The said activities will be carried out, using trade law terminology, “in organization investigation” that is before the decision about its formal initiation.

If during surveillance and intelligence activities a gathered material indicates the suspicion of committing a crime, the prosecutor, with due regard for the investigation of the alleged offence, can issue a decision on presentation of the charges, based on the operational materials.¹¹⁸ Furthermore, in case the possibility of committing, attempts to commit or preparation to commit a crime of terrorist nature the prosecutor can issue a decision for provisional detention of the suspected person.¹¹⁹

The regulation allows to present charges in a case of “only” suspicion of committing a crime, not necessary justified suspicion, under the condition of activities with regard of further purpose of pre-trial proceedings. Whereas, in case of its probable suspicion¹²⁰ it can be a premise for provisional detention.

The above-listed activities of proceeding character before formal investigation begins may have its source in Art. 308 Code of the Criminal Proceedings that is a proceeding in the essential scope, “adjusted” to reality of the terrorist threat. It can be true, especially, when applying to materials gathered accordingly with Art. 9 Act on anti-terrorist activities. It would be more difficult if the mentioned decision were taken on the basis of vague, ambiguous terms, not consulted objectively with ABW’s units responsible for cooperation with the prosecutor.

¹¹⁶ It is worth noticing that it is a challenging construction.

¹¹⁷ As W. Grzeszczak stated that the basis on which the investigation may be initiated can be only such data, which impartially makes committing a crime more likely to happen, whereas subjective emotions arise high suspicion of its appearance. The said basis is a minimum condition, thus the obviousness of crime committing is even more likely to fulfill the condition to initiate the proceeding. The Act on anti-terrorist activities describing justified suspicion of a perpetration of a criminal offence requires it to be based on a rational premise. This condition is not fulfilled by rumor, thought or not close related suspicion regarding the crime because such suspicion would be arbitrary. The justified suspicion must refer to the certain crime, an act, which can be qualified from certain regulation of the Criminal Code or other specific act, but it goes with stadial forms and phenomenal crime, see: W. Grzeszczyk, *Postępowanie przygotowawcze w kodeksie postępowania karnego*, Kraków 1998, p. 48

¹¹⁸ Article 26 (1) The Act on anti-terrorist activities.

¹¹⁹ Article 26 (2) The Act on anti-terrorist activities.

¹²⁰ The legislator uses not precise phrase “probable suspicion” avoiding a code phrase “reasonably assumed”. It seems that before the motion for provisional detention would be better to obtain materials justifying the suspicion of a perpetration of a criminal offence, giving the basis for initiating the investigation as it is stated in Art. 303 of the Code of Criminal proceedings.

Due to variability of methods used by the terrorists, the Services should have adequate instruments that would enable them proper recognition and evaluation of threats and effective counteracting of possible situations of terrorist nature. The instruments, so that they were effective, considering development, need to be adopted to the realities and updated systematically.

At the end the author quoted a fragment of one of the operation cases analyzed a few years ago, in which long before regulation of the Act on the anti-terrorist activities he indicated that:

(...) in the context of current situation concerning terrorism development in Europe, in the Middle East, Asia and both Americas, the decision whether the given occurrence poses a threat should be made with no presumption of innocence, with any doubt being treated as detriment, at least in terms of verification necessity [and possibilities]. Actually, accordingly to media information, this strategy was accepted in practice with various countries that are particularly exposed to terrorism (the USA, England, Israel, etc.) and this is currently accomplished.

This approach gives an opportunity to fight against organizations and their members, which are aimed at widespreading feeling of threat.

A thorough familiarity with the Act on anti-terrorist activity and other legal acts related to it, gives an answer to the raised question concerning legitimacy of equipping state bodies with certain tools regarding possible special threat to the state security and its citizens and legitimization of the activities in the Polish legal system. In both cases – although, one could say that some regulations are controversial – the answer is “yes”.

Obviously, minor and more serious mistakes were not avoided, however, they will not be verified until situation of direct necessity to use regulations of the Act on anti-terrorist activities appears.

Events of last years, months and even days have reflected the significance of the subject and its regulation requires special attention and accuracy. Increasing number of terrorist acts, including activities supporting such organizations, requires an immediate and effective reaction¹²¹ that simultaneously should be legal.

Since June 10, 2016 we have had a starting point thanks to which the mentioned at the beginning of the article “a step behind the criminal” may become much more shorter.

¹²¹ With a wide range of effective accomplishment of goals imposed to state authorities.

Abstract

Issues concerning terrorism appear to be highly popular and prone to public discussion. This concerns both comments of incidents and occurrences with terroristic backgrounds including looking for reasons of such a situation and attempts to prepare our state for pushing the attack and prevent it.

Unfortunately, as one can notice this discussion takes place, in my humble opinion, in the atmosphere of unnecessary tense and commotion each time evoked by the peculiar character of the commented occurrence and relating it to a current situation in Poland, very often with political connotations. What is noticeable is the lack “cold blood and common sense”, which is significantly crucial to assess a particular threat, let alone real actions in the face of it.

This article include a multitude of answers posed by potential participants, observes and listeners of such discussions. These questions especially concern designated organs fighting terrorism and their tasks. Moreover, they concern more advanced issues regarding a range of means and methods f work of operational and reconnaissance as well as investigation teams.

The above considerations were preceded by an attempt to define the role of the state to assure public safety and the significance of this role for both administrative organs and the society itself.

The issues included in this article shall constitute a possibility of, hopefully, objective adjudication of numerous issues cited in the comments in the introductory part.

Keywords: safety, terrorism, counter-terrorism action, operational control, covert activities.

Marcin Gołaszewski
Paulina Markowicz
Justyna Jastrzębska

Social perceptions of polygraph examinations in Poland, their utility in security agencies and other fields of activity

1. Polygraph examinations in Polish literature

In Polish scientific literature one can come across a heterogeneous position on the assessment of polygraph examination usefulness. Many authors stress that criticizing the method is associated with insufficient understanding of the essence of examinations done by the means of polygraph. In a significant proportion of psychology environment, also in Poland, there is a popular misconception of polygraph examinations, connected to works by Paul Ekman, dealing with the nature of emotions and methods of dishonesty detection on the basis of microexpression.¹ The author indicates that lies can be detected in situations when people feel fear, feel guilty, feel joy, and other emotions. He also stresses that while looking for clues about lying, one should remember about the risk of the so called Othello error² and the possibility of mistakes resulting from the failure to include individual differences in emotional behavior of the examined person. As far as polygraph examination is concerned, Ekman admits that his assessment of the polygraph is based on other scientists' works. In his own works it can be noticed that there are no scientific proofs confirming reliability and precision of the method.

There is a lot of works by Polish authors indicating the high accuracy of polygraph examination and a wide range of its application. J. Widacki and J. Konieczny are the precursors in the field. The results of one of the experiments by Widacki proved that polygraph examinations are as valuable as other methods of criminal identification.³ Nevertheless, part of the legal community shows skepticism when it comes to using polygraph examination as legal proofs in Polish penal proceedings. P. Herbowski points out that polygraph examinations during lawsuits are often perceived as a method to directly assess truthfulness of an examined person, i.e. detecting lies.⁴ The situation has been clarified by the decision of the Supreme Court of January 29, 2015 (I KZP 25/14), in which the possibility of polygraph examination of a suspect, defendant or

¹ P. Ekman, *Kłamstwo i jego wykrywanie w biznesie, polityce i małżeństwie*, Warszawa 2006.

² In Shakespeare's *Othello*, Othello falsely believes that his wife, Desdemona, has been cheating on him with another man. Seeing his wife's emotional distress, Othello interprets it as her reaction to hear of her alleged lover death.

³ J. Widacki, *Badania poligraficzne w Polsce*, Kraków 2014, pp. 135–138.

⁴ P. Herbowski, *Wykrywcze wykorzystanie wyników badań poligraficznych*, „Problems of criminalistics”, No 267, 2010, pp. 12–14.

witness was confirmed. The decision stated also that a formal expert's opinion based on the examination, treated both as incriminating evidence as well as rebutting evidence (according to Article 199a of the Code of Penal Proceedings of 6 June 1997 – Journal of Laws 1997, No 89, item 555, as amended⁵).

2. Perceiving of polygraph examination by different environments in Poland

According to analyses by J. Moszczyński published in 2011 (see the table) basic recipients of polygraph examinations, i.e. prosecutors and judges – assessed them very low (on a scale from 1 to 10 – respectively: 2,9 and 3,2). Two times higher was assessed even the next type of criminalistics examination, which had gained also very low notes, i.e. osmology identification (6,0 and 5,9).

Table. Prosecutor's and judge's preferences on criminalistic examinations.

| PROSECUTORS | |
|-----------------------------------|--|
| Criminalistic examinations | Value assessment (scale of 1 to 10) |
| Genetic identification | 9,82 |
| Dactyloscopic identification | 9,81 |
| Pchysicochemical identification | 9,0 |
| Firearm identification | 8,9 |
| Handwriting identification | 8,8 |
| Car accident rekonstruction | 7,7 |
| Mouthprint identification | 7,6 |
| Audio forensics identification | 7,5 |
| Toolprints identification | 7,4 |
| Ears Prints identification | 7,3 |
| Shoes prints identification | 7,0 |
| Osmology identification | 6,0 |
| Polygraph examination | 2,9 |
| JUDGES | |
| Criminalistic examinations | Value assessment (scale of 1 to 10) |
| Genetic identification | 9,7 |
| Dactyloscopic identification | 9,5 |
| Firearm identification | 8,8 |
| Handwriting identification | 8,3 |

⁵ *The Act of 6 June 1997 Code of penal proceedings* (Journal of Laws 2017, item 1904).

| | |
|---------------------------------|------------|
| Pchysicochemical identification | 8,3 |
| Car Accident rekonstruction | 7,7 |
| Audio forensics identification | 7,4 |
| Toolprints identification | 7,2 |
| Mouthprint identification | 7,2 |
| Shoes prints identification | 7,1 |
| Ears prints identification | 6,7 |
| Osmology identification | 5,9 |
| Polygraph examination | 3,2 |

Source: J. Moszczyński, *Subjectivism in criminalistics*, Olsztyn 2011, p. 206, University of Warmia and Mazury Publishing Company in Olsztyn.

Several years after the study by Moszczyński the preferences have changed slightly in favor of polygraph examinations, but their position in the hierarchy has not changed at all. According to a study by K. Niziołek, at present, prosecutors and judges assign polygraph examination a value of 4/10 (for comparison: genetic identification – more than 9/10, dactyloscopic identification – almost 9/10, firearms identification – slightly more than 8/10, osmology identification – slightly more than 5/10).⁶ The surveyed attitude towards polygraph examination has differed according to personal experiences. Those, who had anything to do with polygraph in the past, assessed its value more than one point higher than those who based on a common opinion only.

There is a lack of Polish surveys on the level of polygraph examination acceptance in the scientific environment. To compare – such analyses were conducted in the early 21st century in the USA.⁷ Among surveyed there were members of Society for Psychophysiological Research – SPR, and American Psychology-Law Society – APLS. More than 90% of the surveyed said *yes* to a question – whether materials on polygraph examination published in independently reviewed scientific magazines are based on commonly accepted methodology. Around 70% of scientists assessed that polygraph examination is as much, if not even more, useful evidence as psychological opinion whether a certain person is dangerous or not. 72% of APLS members and 61% of SPR members claimed that in case of reception of evidence from the expert's opinion on polygraph examination in judicial proceeding, the relevance of judicial decisions will increase or will remain unchanged. The minority of the surveyed claimed that the relevance will decrease.

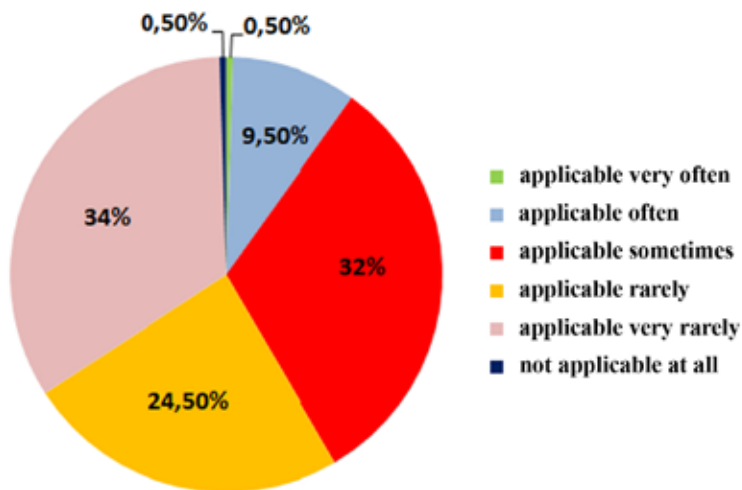
⁶ K. Niziołek, *Ocena trafności badań psychofizjologicznych w odniesieniu do polskiego procesu karnego* presentation from the Nationwide Scientific Conference „The role of psychophysiological examination in a human understanding and corrections of human's functioning”, 18 May 2017, UKSW, Warsaw.

⁷ C.R. Honts, S. Thurber, D. Cvencek, W. Alloway, *General acceptance of the polygraph by the scientific community: Two surveys of professional attitudes*, paper presented during APLS meeting in Austin (Texas) in 2002.

In order to establish how Polish society (different social groups, not only representatives of judiciary) perceives at present polygraph examination, there was a survey prepared with questions concerning, among other things, the knowledge of polygraph examination, experience with regard to the method or thoughts on its practical application. 200 persons between the ages of 16 to 67 took part in the pilot study. The average age in the group was 25. With respect to gender, the majority of the surveyed were women. Highly educated individuals or in the course of their studies (mainly from the faculties of law, psychology, criminology, internal security) dominated in the group. 33,5% of the surveyed declared full time employment at the time of the survey. They declared the Ministry of National Defense, the Armored Cavalry Brigade, Police, Customs Service, Army, Social Services, public administration, medical and psychotherapy centers, foundations, security companies and HR companies as their work places. 3,5% were self-employed, 2% had agricultural businesses, 4,5% were unemployed, 2,5% were pensioners. The rest were students.

In the surveyed group 63,5% declared that they had known the notion of polygraph examination, 22% admitted direct or indirect contact with polygraph. In most cases the picture of the method came from the knowledge gained during studies, at a workplace or personal interests and mostly from the media (especially from TV documentaries or entertainment – for example “The moment of truth”). 8% of the surveyed have had the polygraph, 36% declared at least basic knowledge how the polygraph testing run and 64% did not know how the whole procedure.

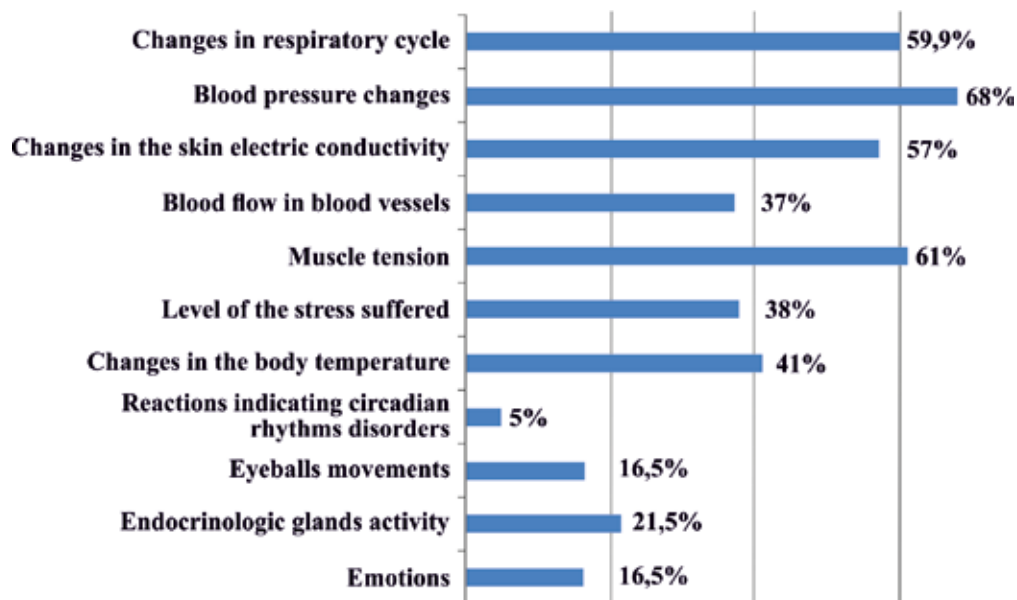
The following chart (pic. 1) shows how the surveyed had imagined the frequency of polygraph examination in Poland.



Pic. 1. Application of polygraph examination in Poland.

Source: private study.

Next chart (pic. 2) presents the answers regarding psychophysiological reactions measured by the polygraph.



Pic. 2. Answer for the question about psychophysiological reactions measured by the polygraph.

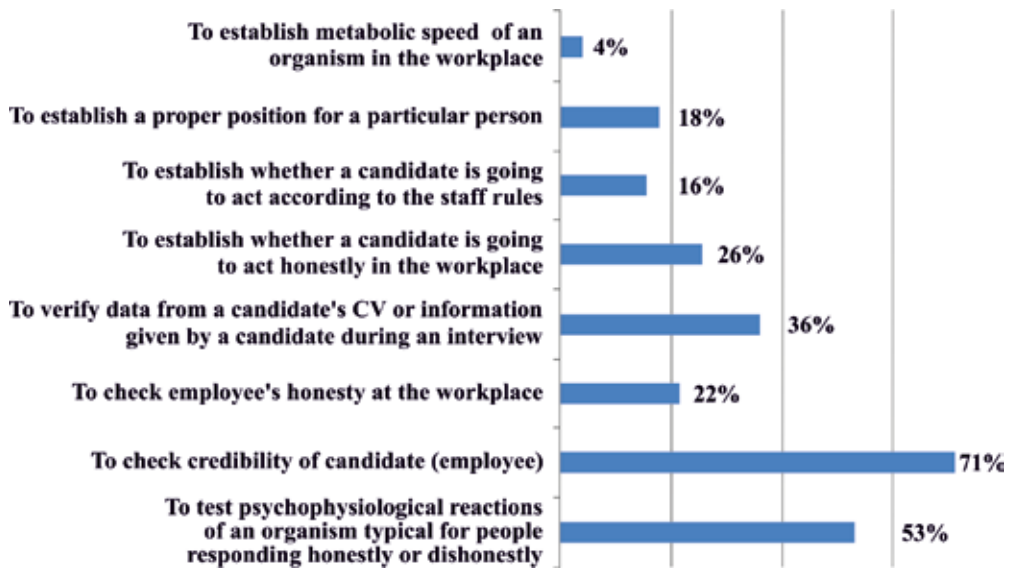
Source: private study.

Among answers given there are correct options, i.e. changes in the respiratory cycle (indicated by 59,5% of the surveyed), changes of the blood pressure and pulse changes (68%), changes in the electric conductivity of the skin (57%), changes in the volume of blood in blood vessels (37%) and muscle tension, i.e. movements of the tested person (61%).

Incorrect options concerned the following: level of stress (38%), changes of the body temperature (41%), reactions showing circadian rhythm disorders (5%), movements of eyeballs (16,5%), activity of endocrine glands (21,5%), emotions (16,5%). The answers regarding level of stress and emotions of the tested are connected with the common myths in the society. For example, P. Ekman claims that on the basis of polygraph examination one can notice whether a person feels certain emotions (anger, fear) during the procedure.⁸

Next chart (pic. 3) shows opinions on the possibilities to use polygraph examination during job recruitment procedures:

⁸ P. Ekman, *Kłamstwo i jego wykrywanie...*, pp. 171–216.



Pic. 3. Answers on a question regarding the application of polygraph in HR assessments. Source: private study.

Apart from those answers consistent with reality – for example checking the credibility of a candidate (71,5% of the surveyed), verification of CV data or verification of information given during a job interview (36%) – there were also answers that indicated the possibility of tracing the candidate's intention⁹ of acting honestly at a new workplace (25,5%) and even to establish the speed of people's metabolism in a workplace (4%).

Functions of polygraph examinations

51% of respondents considered that polygraph examinations on a broader scale would contribute to improving both state apparatus (including law enforcement services) and private companies sector. Nevertheless, 49% of the respondents were of the opposite opinion.

Representatives of the first group claimed that polygraph examination allow to eliminate inappropriate candidates for the service or for the job (*It is especially important as far as services are concerned. It would also be an additional method of confirming the loyalty of employees and of verifying their activities*). They stated also their preventive value (*for example thanks to them the number of frauds and thefts was smaller and inappropriate individuals were discouraged to apply for certain positions*).

The preventive role of polygraph examinations is reflected particularly in studies done in the USA and in the UK on people convicted for offences against sexual freedom and on conditional release. 75% of the surveyed indicated that such studies

⁹ Poligraph is not a crystal ball!

would be useful also in Poland¹⁰. It was supported by the view that (...) *it would make it easier to get to know whether such persons still threaten the security of others, check their activities being at large (in order to verify whether the person has not committed any other offences or breaching conditions of the parole)*. 25% of the surveyed answered that polygraph examinations should not be used in this context because this solution (...) *would be unlawful and limiting personal freedom*. One of the surveyed touched a question of privacy of those examined: (...) *through polygraph testing of the people who were convicted for sexual offences it would be possible to monitor everyday activity of such people and prevent possible committing of other sexual offences by them in the future. Nevertheless, such examination should be applied only when psychiatric evaluation indicate the possibility of returning to criminal activity or the possibility of psychic perversion of the former person sentenced. Such supervision during post-penitentiary stage can appear as too far-reaching and treated as intervention interference into rights and freedoms of a person (right to privacy)*. Some of the surveyed paid also attention to the costs.

Polygraph examinations supporters see also the possibility of gaining important information during investigations (*I am a supporter of polygraph examination especially in courts. There is a bunch of cases regarding for example falsified signatures, last wills, anonymous letters and so on. After such examinations there would be no doubts or polygraph examination during preparatory proceedings could steer investigative organs to a proper direction – circumstantial evidence*). 76% of the surveyed were pro polygraph examinations during criminal proceedings, and 24% were against. Supporters regarded polygraph as “valuable evidence”, and they perceive it as particularly useful in most complex cases, or in a word against one’s word cases. A demand of “careful interpretation” was also added (for example: *No doubt that it is a method giving certain view over certain situation. Despite some doubts about 100% credibility of the method, it can be very useful although it should not be taken for granted and its results should be verified by other methods*).

Simultaneously, it was demanded that polygraph examinations should be treated as a subsidiary method (for example: *They can be a useful source of knowledge if they are combined with other methods, for example interview, or: testing with such tool would be helpful in assigning proper candidates for important state posts or for posts in business companies. It is not the point to focus only on polygraph examinations but to treat them as a guideline or improvement of recruiting process, which could tell what to check more or what to pay particular attention to*).

On the other hand the opponents of polygraph examinations stated that reportedly they are “non-authoritative”, and their results can be associated with (...) *the health condition, drugs, age, stress connected with the testing and so on, and former preparations for the testing makes it possible to deceive device*. This group of surveyed

¹⁰ More in: M. Gołaszewski, *Użyteczność badań poligraficznych w ograniczaniu recydywy wśród sprawców przestępstw przeciwko wolności seksualnej*, „Prosecution and Law” 2016, No 12, pp.5–22.

states that polygraph examinations should not be used in criminal proceedings because (...) *accuracy of the testing is dubious, (...) emotional situation connected with the testing do have influence on the result, (...) the expertise is costly.*

3. Polygraph examinations in state institutions

When it comes to polygraph examinations in law enforcement agencies, 85% of the surveyed stated that they are useful (they responded for example: *It is an exceptionally responsible and demanding job, that is why there is a need to be sure that the candidate does not have any links, for example to groups dealing with drugs. The job is also exceptionally burdensome, that is why it is worth testing during the service whether a person does not break and goes to the dark side; I think that during a recruitment process in services important for the state defense and security polygraph examination is an outstanding and adequate way of candidates verification (it is true that it enters private sphere of the recruited person but it is justified by the specific situation).*

Polygraph examinations in services have not been supported by the minority of the surveyed (15%). There were statements like: *In my opinion polygraph examinations cannot be a source of information about recruited person, the error rate is too high; In my opinion it is additional and unnecessary stress for a candidate who is under a very meticulous verification, anyway.*

The first Polish service that owned polygraph device was Military Internal Service (WSW) – a service that combined competences of military police and military counterintelligence. It bought Keeler polygraph (model 6308) in the late 1960s. A bit later the then Ministry of Internal Affairs (including civil intelligence – Department I and counterintelligence – Department II) bought polygraph devices.

In both institutions polygraph devices were used mainly for training purposes. Probably intelligence agents were also accustomed with such testing, assuming that they might be tested by the American services in the future. In WSW polygraph examinations were used in criminal proceedings, during investigations conducted by the military prosecutors, especially in weapons theft cases. WSW experts were asked by common prosecutors to conduct polygraph examinations in different most serious criminal proceedings, including mostly murder cases.

Up to 1989 the Citizens' Militia had not got any polygraph examinations unit. They had been using WSW experts or university experts. At that time there had not been any polygraph examinations for candidates to the police nor special services.

A major change happened after 1989, after the communism had collapsed. Independence from the USSR, special services and police reorganization and starting unbound cooperation with western countries in different areas, including the USA, which allowed broader use of polygraph testing and using western patterns.

The Police, which replaced the Citizens' Militia, bought first polygraph devices and organized both central facility for polygraph examinations in Warsaw and its four

regional branches. The Office of the State Security established in 1990 started its own polygraph examination unit. Such units started also in the Border Guards and in the Military Gendarmerie (Military Police). After special services reconstruction, The Office of the State Security was transformed into the Internal Security Agency (ABW) and the Intelligence Agency (AW), and the Central Anticorruption Bureau (CBA) was also established, the Military Information Services (WSI) was transformed into the Military Counterintelligence Service (SKW) and the Military Intelligence Service (SWW).

Polygraph examinations are used in recruitment procedures and screening procedures of most police and special services. Recruitment procedures for the particular service are described in acts and anticipate obligatory polygraph examinations for candidates. The procedures are also used to check loyalty of officers and soldiers. The number of examinations for internal use of police and special services is unknown, nevertheless, it can be assessed that it is at least few times higher than in criminal proceedings.

The loyalty means for example obeying the law, mutual commitment between people who trust each other, honesty in everyday activities.¹¹ It manifests itself by fulfillment of commitments and respecting the rules of honor and rightness.¹² The employee loyalty means that an employee wants to stay in an organization and performs duties with commitment regardless of temporary problems at a workplace.¹³ Loyalty in law enforcement environment is based, on the one hand, on pragmatic circumstances, i.e. on a relatively permanent working bond and desires to be promoted in the hierarchical structures. On the other hand, it is based on values, patriotic attitude and citizenship, and personal satisfaction of the officers in a service. It comes from the surveys made between 2015–2016 among employees of Polish companies that a loyal employee is described as an honest, sincere person who performs professional duties carefully and fairly¹⁴. Conformist subordination to an organization does not come to the fore although, indeed, it is of greater value in services than in a private sector. Before starting their duties in different institutions, officers take an oath of office connected to loyalty. It contains such promises like: service to a nation, loyalty to constitutional organ of the Republic of Poland, diligent obeying the law and discipline of the service, following orders, protecting honor, dignity and a good name of the service.

Candidates for the service in Police, Central Anticorruption Bureau, Intelligence Agency, Internal Security Agency, Border Guards, Military Gendarmerie, Military Intelligence Service, Military Counterintelligence Service, National Revenue Administration as well as officers and workers of those institutions undergo polygraph examinations during the recruitment process.

¹¹ M. Jarosz and others, *Słownik wyrazów obcych*, Wrocław 2001.

¹² M.S. Szczepański, *Lojalność*, in: *Fundamenty dobrego społeczeństwa. Wartości*, M. Bogunia-Borowska (ed.), Kraków 2015.

¹³ A. Lipka, A. Winnicka-Wejs, J. Acedańska, *Lojalność pracownicza. Od diagnozy typów pracowników do zarządzania relacjami z pracownikami (Employee Relationship Management)*, Warszawa 2012.

¹⁴ E. Robak, *Lojalność pracowników a zarządzanie potencjałem społecznym współczesnych organizacji*, „Scientific Notebooks of Polytechnic in Częstochowa. Management” 2016, No 24, Vol 2, pp. 82–95.

The goal of such examinations is to check whether the officer is useful for the service on a particular post or in particular organizational unit and elimination among those from candidates, who should not perform a service or work on a particular position from certain reasons. In case of ABW, AW, SKW and SWW¹⁵, CBA and Border Guards¹⁶ polygraph examinations can be done for candidates to a positions that require particular skills or predispositions (these are *de facto* all positions).

It is the heads of special services who decide about polygraph examinations. Usually, they are not obliged to justify their decision. It is treated as an element of supervision over the officers. It should also be pointed out that a refusal to undergo the examination would be treated as refusal of following an order, which means disciplinary tort. More precise procedure about polygraph examination exists in case of Border Guards. It is possible only in connection with referral for a training and in cases prosecuted as offences in connection with performing service activities.¹⁷

In the National Revenue Administration polygraph examinations are applied to candidates for the service in most organizational units of the Customs and Revenue Service¹⁸. In order to check usefulness for the service on a particular position such testing can be applied also to officers (mainly those who are entitled to perform operational and investigative activities). It is worth to pay attention to criteria for experts carrying out polygraph examinations in the National Revenue Administration. In accordance with the Regulation of the Ministry of Development and Finance of 10 April 2017 on psychophysiological examination, physical fitness test and psychological examination of the Customs and Revenue Service officers¹⁹ – polygraph examiner (...) *holds master's degree, graduated from a specialized course and obtained proper certificate authorized or recognized by the American Polygraph Association (APA), or a course on polygraph examinations at least on a basic level, or does have proper – gained other way – skills to correctly conduct polygraph examinations and to give interpretation of its results, authenticated by Polish polygraph organizations, including the Polish Polygraph Association*. The above mentioned Regulation is the most up-to-date document of this kind in Poland that regulates the qualifications of polygraph examiners.

¹⁵ *The Defense Minister Regulation of 26 July 2006 on the qualification procedure for candidates to service in the Military Counterintelligence Service* (Journal of Laws 2006, No 137, item 978). *The Defense Minister Regulation of 26 July 2006 on the qualification procedure for candidates to service in the Military Intelligence Service of 26 July 2006* (Journal of Laws 2006, No 137, item 979).

¹⁶ *The Act on the Border Guard of 12 October 1990* (Journal of Laws 2017, item 2365).

¹⁷ According to Article 1.2a of the Act on Border Guard, it is the Border Guard which carries out proceedings in cases of recognizing, preventing and detecting crimes described in Article 228 (passive bribery), Article 229 (active bribery) and Article 231 (abuse of rights, failure to fulfill the obligation) of the Penal Code, committed by Border Guard officers in connection with official duties. (*In such cases it is the Border Guard Commander in Chief who is capable to order for such examination*).

¹⁸ *The Act on National Revenue Administration of 16 November 2016* (Journal of Laws 2016, item 1947).

¹⁹ *Minister of Development and Finance Regulation of 10 April 2017 on the procedure and conditions of establishing physical and psychological abilities, physical fitness and psychological tests of the Customs and Excise officers* (Journal of Laws 2017, item 805).

For the recruitment of Police officers polygraph examinations are to establish predispositions of candidates for the service on particular positions or in particular organizational units, particularly to establish loyalty to the service, reaping unauthorized benefits from the former service and to establish any pathologies and undesirable dependencies in the service. During polygraph examinations there are no questions regarding faith and sexual or political preferences. The examination is recorded (picture and sound), and if the examination result is inconclusive such examination can be repeated only once in 30 days time²⁰. A check test is to check whether since the last examination officers did not reveal any secret information, whether they did not make any undesirable contacts or they did not commit any offences or disciplinary misconducts.

Among all services performing their tasks within the scope of the state security, it is only the Government Protection Bureau that had no legal regulations regarding the obligation and – even more – possibility to carry out polygraph examinations to candidates for the service and its officers. In 2018 the Government Protection Bureau was replaced by the Service of the State Protection (SOP). Psychophysiological tests for candidates to the service are obligatory and optional for officers, SOP employees or personnel of other state institutions being brought to the service in SOP.

There is no doubt that if polygraph examinations regarding candidates for services and officers of services are based on legal acts, no other state officials cannot undergo such tests unless the proper act states so.

Police and special services that perform operational and intelligence tasks can also do polygraph examinations to individuals who help services by such tasks.

Polygraph examinations are also allowed in disciplinary proceedings of prosecutors. The Act on Prosecutors²¹ (chapter about criminal, disciplinary and work responsibility) states that during disciplinary proceeding in order to limit the range of people suspected of disciplinary misconduct having features of offence if the secret or top secret information from criminal proceedings disclosure disciplinary officer can appoint an expert to use - against the prosecutor with access to such information – technical means of unconscious reactions of the organism, with his consent.²²

Many years of experience of the rest of Polish law enforcement services prove the high quality of psychophysiological examinations with the use of polygraph device. Since it is the tool that enables to obtain valuable information which is often very difficult or even impossible to obtain via other available procedures. Nevertheless, examinations performed in some state institutions rise sometimes different controversies. First area of controversies is connected to admissibility of such examinations in a legal, formal and ethic sense and doubts about it are reported from outside services with an emphasis

²⁰ *Minister of Internal Affairs Regulation of 20 March 2007 on the procedure and conditions of establishing physical and psychological abilities of policemen for the service on certain positions or in certain Police units* (Journal of Laws 2007, No 62, item 423).

²¹ The Act of 28 January 2016 The Law on Public Prosecutors (Journal of Law 2017, item 1767).

²² *Ibidem*, Article 154.

on a reportedly high degree of mistakes when it comes to polygraph examinations. Second area of controversies embraces topic of examinations standardization and quality assurance policy. This part of discussion goes on an inter-ministerial level as well as among officers inside the services and institutions.

The topic of polygraph examinations admissibility has been a subject to considerations of the Constitutional Tribunal²³ that stated that the provisions of acts allowing such examinations in Police are not unconstitutional. State organs are allowed to do only what legal acts order or allow. The scope of such competences are mentioned above for all institutions and should not rise any doubts.

By the way, in private sector there is a general rule that what is not prohibited by the law, should be regarded as allowed. Polygraph examinations in companies are usually performed in the course of recruitment process, and in situations when employee is suspected of any wrongdoing for the employer. A. Drozd points out some labor law representatives who pay attention to possible rights of personality, freedoms, dignity and private life violations²⁴. According to him HR examinations with the use of polygraph device can be accepted only when clear legal norms are established and if a candidate or employer accepts the testing. These conditions are in line with the American Polygraph Association²⁵ and The Polish Association of Polygraph Examinations standards. J. Pietruszka and R. Rogalski admit that polygraph examinations are very often invaluable source of knowledge for employers. The testing allows to obtain information which could not be obtained in any other way.²⁶

The opponents of the polygraph examinations require very often an unreal demand of absolute accuracy, citing underrated data (for example 75%).²⁷ Meanwhile, it should be stressed that polygraph examinations have relatively high and most probably the best diagnostic value comparing to other methods used in criminalistics. An average accuracy of all types of polygraph examinations confirmed by scientific research is 87,1%.²⁸ In case of diagnostic tests (one-problem test) it is 92,1% and for screening test (multi-problem) – 85%. Data regarding accuracy of polygraph examinations techniques come from different scientific research done in 20th and 21st centuries. Only those of scientific standards and which were published in independently reviewed magazines or scientific works are taken under consideration. In the result of meta-analysis

²³ Decision of the Constitutional Court of 23 February 2010, K. 1/2008 LexPolonica, No 2144497, OTK ZU 2010/2A, item 14

²⁴ A. Drozd, *O dopuszczalności wykorzystywania wariografu w stosunkach pracy*, „Labor and Social Security” 2003, Vol. 4, pp. 9–14.

²⁵ *Code of Ethics*, [online extract], American Polygraph Association, <<http://www.polygraph.org/assets/docs/Misc.Docs/2015%20code%20of%20ethics.pdf>> [access: 25 V 2017].

²⁶ J. Pietruszka, R. Rogalski, *Nie odbierać prawa do obrony- artykuł dyskusyjny o poligrafie*, „Labor and social security” 2004, vol. 11, pp. 15–21.

²⁷ Inter alia P. Słowik, *Rekrutacja do Straży Granicznej: Wariograf wątpliwy, ale nie dla MSWiA*, „Legal Journal” [online], <<http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1026987,rekrutacja-do-strazy-granicznej-badanie-wariografem-w-sadzie.html>> [access: 26 III 2017].

²⁸ *Meta-Analytic Survey of Criterion Accuracy of Validated Techniques*, „Polygraph” 2011, Vol. 40, No 4.

of data from numerous research there were two important reports summing up average accuracy of polygraph examinations in general and also different types of research and individual research techniques. One of the mentioned reports was issued by the American National Research Council in 2003. At that time the indicator of polygraph examinations accuracy in “concrete and particular cases” was confirmed as ca. 90%. The second report was prepared by the American Polygraph Association in 2011 and currently it is regarded as the best point of reference. As in any other field of science, data from the report should be treated as binding until possible new results of scientific proofs basically change the view.

Much more justifiable in terms of accuracy of texts used in polygraph examinations is a demand for minimalization of error risk formulated in March 2017 by a member of the Helsinki Foundation of Human Rights.²⁹ Such demands meet professional standards. If any testing, much less, a whole polygraph examination occurs at some stage inconclusive, additional examinations are needed (in the framework of the same testing or next one, replicated). In turn, the so called „successive dealing with obstacles” attitude requires that diagnostic testing is done in order to verify remaining doubts in case of unfavorable results of screening tests for the examined person. Technically, it means that in case of examinations with relatively less accuracy (average 85%), a more accurate examination (average 92,1%) should follow.

It should also be clearly stressed that equating posts in governmental institutions and law enforcement with workplaces in regular institutions or usual workplaces is not possible. There is no need to explain anybody that from the perspective of a state security it is better to reject some percent of candidates – even if not correctly assessed – than, to allow even one person, who is capable to do harm to the state interests, to be let in. The interests of the country, state’s security and protection of classified information shall have priority over anything else.³⁰

The rules of polygraph examinations are set out by publicly available standards of professional and standardization international organizations (American Polygraph Association, ASTM International) as well as national organizations (including Polish Society of Polygraph Examinations). Furthermore, there are internal rules and procedures in different state institutions which do polygraph examinations. Standards have been described in Polish-language scientific literature³¹ so they are commonly known and accessible, and a language barrier is not a sufficient reason to ignore them.

²⁹ P. Słowik, *Rekrutacja do Straży Granicznej: Wariograf wątpliwy, ale nie dla MSWiA*, „Gazeta Prawna” [online], <<http://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1026987,rekrutacja-do-strazy-granicznej-badanie-wariografem-w-sadzie.html>> [access: 26 V 2017].

³⁰ Article 24.4 of the Act of 5 August 2010 on the Protection Of Classified Information (Journal of Laws 2016, item 1167).

³¹ *Współczesne standardy badań poligraficznych*, M. Gołaszewski (ed.), Warsaw 2013, „Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego” Warszawa 2013; M. Gołaszewski, M. Widacki, *Aktualny standard badań poligraficznych a praktyka polska*, in: *Badania poligraficzne w Polsce*, J. Widacki (ed.), Kraków 2014.

In HR examinations, like screening testing, scientifically proved techniques with the accuracy level higher than statistic chance, are recommended. They can be used together with the so called „successive dealing with obstacles”.

Separate examinations, in connection with a certain system of testing data analysis, differ between each other not only with an average accuracy but also with sensitivity and specificity. It seems that the optimal solution would be choosing such technique with balanced parameters. Policy of a certain institution may, however, stipulate that the overriding aim is as much sensitivity to deceiving, even at the expense of examination ability to confirm truthfulness of the examined person. Also decision-making thresholds by numerical notes can be regulated – depending on the accepted error tolerance. Normally, error tolerance is accepted, for example, by favorable results for the examined at the level of 0,1. The system could be tightened, however, by lowering the level of tolerance to 0,05 (like in case of results indicating artificiality).

The possibility of choosing from a dozen of test should not mean a total freedom. Also worthy of note is the R/I test (classical), which goes into history books slowly, and relatively short accuracy (at the level of ca. 75%) in combination with alarmingly small specificity and exclusively qualitative (global) method of charts evaluation call into question the meaning of its application anyway. In some conditions it can be useful, but in ordinary situations it is hard to understand the arguments in favor of it (apart from its simplicity and comfort of the examiner) – if other, more effective, exist. Similar objections can also be aroused by peak tension tests (POT) because their results provide the basis for credibility opinion about a person examined. At this point it is worth recalling that the POT examination type with required solution version are only subsidiary.

On the ground of such concerns there comes a subject of the so called “quality control” or – more softly – „quality assurance policy”. In the USA such procedures operate successfully. They contribute to eliminating pathologies (for example custom-made results), limiting subjectivity of examiners, enhancing professional development, and, on the other hand, they guarantee examiners protection from external pressure. In Poland, there have been introduced internal procedures in different institutions. The procedures shall include, inter alia, the so called blind polygrams assessment, checking chosen examinations in full (live or restored) and professional supervision. What is lacking is a supervision and control authority to coordinate polygraph examinations programs on the central and inter-ministerial level, and at the same time it would be responsible for experts training process and scientific research, like the National Center for Credibility Assessment in the USA. There are similar problems in assessments during criminal proceedings. In view of the lack of license procedures the activities of forensic experts are only under formal courts supervision or alternatively under scientific supervision of the environment. Some experts are, however, outside professional associations and are not interested in contacts with other professionals and experts.

Nevertheless, no matter the controversies or problems are, one can sum up that polygraph examinations in Polish administration institutions have quite a long history of practice. It also seems that polygraph examiners have well-established presence and reputation within the respective services. It is only a high quality of expertise (especially for criminal proceedings) and activities in the public sphere that will allow polygraph examinations perceiving in the society to be consistent with the picture of the examinations in services and adequate to real diagnostic possibilities.

Abstract

The issue of psychophysiological examinations utilizing polygraph causes many discussions for scientific and social reasons. Usually, this is connected with limited access to knowledge in this area and consequently – common beliefs operating in Polish public opinion. The article presents the results of a survey, including such variables as: knowledge of the concept of polygraph examination, experience in using this method, opinions about practical application of polygraph examinations (both during recruitment and at the stage of employment in specific positions or in criminal proceedings). The results indicate a miserly range of knowledge about such examinations in the society, largely based on an inadequate or insufficient presentation of this method in the media, press and literature (also covering specialist issues). These perceptions were correlated to the actual utility of polygraph examinations in different fields of practice – particularly in public institutions (uniformed services and others).

Keywords: polygraph, psychophysiological examinations, detection of insincerity, utility, officers, public institutions, loyalty, society, survey.

Marek Świerczek

**The internal sources of the defeat
of the Second Department of Polish General Staff
in the confrontation with the State Political Directorate
under the People's Commissariat of interior affairs
of the Russian Soviet Federative Socialist Republic
during the disinformation operation of the Soviet counterintelligence
known as the "MOCR-Trust affair"**

It remains an open question, as it came to be that **Department II of Polish General Staff** (further DII) came into contact with an organization managed by the KRO GPU¹ in 1921 which lasted for almost six years. And when the truth came to light, DII, instead of looking for explanations and remedies, in fact resigned of intelligence activity in the east, replacing it with the observation method, the weaknesses of which were well known to many espionage officers² and an ineffective activity of radio monitoring and analysis of Soviet media – which were under full censorship control – so practically worthless for intelligence analysis and still offering Russians the possibility of disinformation.

In fact, the involvement of Polish intelligence into a disinformation operation conducted by the Soviet counterintelligence should not be considered in the category of tactical failure, but rather strategic defeat. For the first years of our intelligence operations in Soviet Russia, they were "transparent" to the Chekists and Polish spies were misinformed by Soviet agents-provocateurs. And when DII understood its mistake, it first gave up the recruitment of agents in Russia to avoid provocations, and then, when it turned out that the observation method was not enough, it failed to recover. At the end of the day, Poland in the East was "blind", what became sadly clear on September 17, 1939, when Poland was attacked by the USSR, which according to the leadership of DII – was not only to remain neutral, but even to provide material support in case of the war with Germany.

Given the extent of the Polish intelligence failure in the years 1921–1927 (and their consequences in the following years), it is not enough to describe the operation, it is also necessary to formulate hypotheses answering the fundamental question about the **reasons for** such a serious failure of the Polish intelligence. To explain the causes that brought about this intelligence defeat in the secret war with the Soviet services, first of all, we need to realize their **multiplicity and complexity**.

¹ Soviet counterintelligence GPU. Trust Operation was carried out by the Soviet counter-intelligence in spite of organizational changes, i.e. by VCheKa, GPU and OGPU. There is only one term used in the text to make things easier.

² W. Michniewicz, *Wielki bluff sowiecki*, Chicago 1991, pp. 268–269.

There was not one key element or event that would become the cornerstone of the process of submission to the Soviet disinformation by the Polish intelligence service. Even remembering that formally the beginning of cooperation with the organization MOCR³ Trust (established by the VChK/GPU), and at the same time the initiation of the great disinformation operation, was contact of the Trust's missionaries with Cpt. Wiktor Tomir Drymmer, who headed the intelligence post in Reval, it must not be forgotten that this was just a single event, which – in different circumstances, and with other personnel and organizational solutions – would not have to lead to intelligence losses at the strategic level and could have ended at the level of penetration of Reval intelligence post.

Contact established by Cpt. W.T. Drymmer and subsequently taken over by the DII HQ and sending Polish officers as the Trust's liaisons in Moscow, which in turn led to the Trust's monopoly of the Polish reconnaissance in the east, were the result of a combination of many factors that caused the DII to fall victim to the Soviet disinformation.

One can risk a statement that, considering the multiplicity and complexity of the reasons behind this cooperation, DII was the ideal object of such activities. Even if there had not been contact in the Reval with Soviet emissaries, it is very likely that sooner or later the Polish intelligence (as well as services of other limitrophic states) had to get involved in this type of situation. It was only a matter of time.

Trying to understand this phenomenon, it is necessary to distinguish the main factors behind the multiannual activities of Polish intelligence, which consistently facilitated the GPU activities from 1921 to 1927, without practically undertaking any verification or offensive operations that could provide insight into the nature of operations conducted by the Soviet counterintelligence and intelligence. Providing that the list does not have to be complete, the following groups of factors can be distinguished that affected the level of readiness for self-deception in Polish intelligence structures.

I. Internal factors

1. Psychological factors, occurring universally (a participating lie, the phenomenon of cognitive dissonance, which makes it difficult or impossible to recognize a lie, especially in its co-participation version, group thinking syndrome, usually based on uncritical reproduction of superiors' sentences⁴).

2. Factors generated by the organization of Division II (the authoritarianism and conformism of a military institution⁵) based on the order and transmission information in the "top-down" structure, basically excluding the reverse direction of information flow (especially critical one) and object-oriented feedback; group

³ The Monarchic Union of Central Russia (note ed.).

⁴ T.H. Bagley, *Wojny szpiegów*, Poznań 2014, p. 281.

⁵ G. Bailey, *The Conspirators*, London 1961, p. 66.

interests of a large institution of military bureaucracy, phenomenon of a participating lie; lack of team work, promotion depending on personal success, voluntary decisions of superiors, whose favor – acquired in a variety of ways – played a key role in the careers of intelligence officers; the relationship between the intelligence success, measured by the number and quality of information obtained by the agent for the career of his desk officers⁶; the degree of identification of officers with the service (in the vulgar version the tension between ethos and careerism⁷); a combination of organizational and psycho-social factors generating deficiencies in the professionalism of at least some of the officers⁸; adopted organizational model, character of interpersonal relations, capacity of promotion channels, etc.⁹; the level of responsibility and courage of the civilian executives who in the situation of symptoms of infiltration and disinformation must choose between decisive actions that must cause serious repercussions from society and government and silence over the scandal combined with hiding uncomfortable facts).

II. External factors

The internal policy of the government towards the army till 1926 drastically increasing – due to financial cuts and pauperization of the officers – counterintelligence risk level in the Polish Army and a close relationship between disinformation and infiltration of the deceived service (agents of influence, “moles”).¹⁰

I will try to elaborate upon the first group of reasons, i.e. “internal factors”, which affected the failure of the Polish intelligence in war against Soviet counterintelligence.

Ad I.1. Psychological factors

- **The phenomenon of participating lies** is common and has been known to mankind for centuries. It is a situation, when a victim of a lie *does not pay attention to mistakes made by the deceiver; interpreting the ambiguous behavior as much positively as possible for a liar*¹¹. Such phenomena can be observed in all areas of social life. People often want to believe in false information when they have their own, usually hidden motives, and detecting a lie could have negative consequences (mainly in the psychological dimension) for a deceived person. On the level of everyday life, we

⁶ See: J. Masterman, *Brytyjski system podwójnych agentów 1939-1945*, Warszawa 1973, p. 42.

⁷ T.H. Bagley, *Wojny szpiegów...*, p. 139.

⁸ See: M. Romeyko, *Przed i po maju*, Warszawa 1985, p. 512.

⁹ It can be said that well-paid, well-managed institutions that maintain open promotion paths for talented and dedicated officers are usually much less susceptible to infiltration than poorly managed organizations, in which cliques and groups with access effectively block the promotion paths, putting aside all who may threaten the advancements of the chosen ones.

¹⁰ See M. Romeyko, *Przed i po maju...*, p. 160.

¹¹ P. Ekman, *Kłamstwo i jego wykrywanie w biznesie, polityce, małżeństwie*, Warszawa 1997, p. 22.

deal with this type of participation, for example, when we accept someone's excuses, not wanting to break the relationship for reasons more or less trivial, or when a betrayed husband prefers not to notice evident symptoms of betrayal of a spouse¹² or when someone's lies correspond to previously accepted assumptions of the deceived person.

In special services, this phenomenon occurs very often: ambiguity of information, multiplicity of often conflicting data and difficult verification process favor the acceptance of situations when an officer (or the whole organization) *de facto* facilitates deceiving himself (and his organization), because it is in the group interest, allowing the deceived officer to fulfill his tasks and guaranteeing him a career.

The co-founder of the British system of double agents, J. Masterman, analyzed this phenomenon very carefully.¹³ On the other hand, perhaps the most synthetic characteristic of the co-participant's lie is Bagley's quotation from the Abwehr officer Herman Baun¹⁴ who, after the war, was interrogated by Americans, he:

(...) was aware that every one of his informers on the Soviet territory was controlled by the Soviet counterintelligence. Because he was unable to get better results, and because the German Supreme Command (OKH) liked his reports, questioning them would be a political suicide for him. That's why he preferred to pretend that everything was fine.¹⁵

In short, in the special services, a situation can easily arise when it is much better to believe in agent's lies than to discredit him, undermining his enunciations. Accepting disinformation (especially in areas badly recognized so far) guarantees rewards, rapid promotion and recognition of the management, which, in turn, is interested in quick intelligence success, not tedious procedures that check agent's loyalty and credibility of information. In every intelligence institution in which the individual's success is linked to his personal information contribution, i.e. the more agents and information, the more praises and promotions), being at the same time detached from the interests of the team or the entire service, there is a huge scope for the phenomenon of a participating lie.

It can be deduced from the documents of Division II that most officers, more or less involved in the Trust scandal, avoided any activities that could shake their confidence in the Soviet agents and the information they brought.

For years of stay in Warsaw of an evident OGPU agent, Yury Artamonov, no one in the entire Division II had come to an idea of even briefly checking what the young Russian really was doing and from where he got funds for a sumptuous life.

¹² Ibidem.

¹³ J. Masterman, *Brytyjski system podwójnych...*

¹⁴ See: http://www.foia.cia.gov/sites/default/files/document_conversions/1705143/CIA%20AND%20NAZI%20WAR%20CRIM.%20AND%20COL.%20CHAP.%201-10,%20DRAFT%20WORKING%20PAPER_0010.pdf.

¹⁵ T.H. Bagley, *Wojny szpiegów...*, p. 139.

Explanations of Cpt. W.T. Drymmer and Edward Czyżewski's reports show that Division II was aware that there was a Pole appearing in the so called Trust Board known as Kijakovski (in fact Viktor Steckiewicz), but there is no information in the preserved materials that DII tried to identify this character and to collect any information about him, despite the fact that Steckiewicz, as Kosinski, supervised the Soviet spy-rings in all *Pribaltica* and often stayed in Helsingfors¹⁶, where the Polish Military Attaché was active. Even after unsuccessful recruitment of Bohdan Jarociński by W. Steckiewicz, no one in Warsaw tried to determine, who he really was, what he had done before, where he really stayed, and who he met (or could have met), although a comparison of Kijakovski and Steckiewicz's descriptions would allow Polish analysts notice that it was the same person.¹⁷

Explanations of Aleksander Niedziński clearly show that – while being in Moscow, he had the opportunity even partially to verify the enunciations of Trust members – instead he relied entirely on their intelligence.

During the long years, when Polish officers met with the agent of the Soviet counterintelligence Eduard Opperput, no one even tried to get any information about him, although materials on this subject had to be stored in the archives of Division II, because E. Opperput as Paweł Seljeninow came into contact with Polish intelligence in 1921, during an operation against Boris Sawinkow. In 1921, E. Opperput had contact with Józef Beck and Colonel Stanisław Dowoyno-Sołłohub, in the company of which he carried out negotiations with the British military mission.¹⁸ DII, in addition, issued him a passport under the name Paweł Iwanowicz Spektorskij – and therefore his real name (because in contact with B. Sawinkow he was to reveal how he was really called), and appearance¹⁹ should be known to Polish intelligence officers. It should be added that the recognizing E. Opperput was not difficult. In 1927, in Finland, immediately after Opperput's escape from the USSR, former officer of B. Sawinkow, a certain Aleksandr K. Rudin did it and then published under the pseudonym A. Karin an article on this topic in a Riga newspaper "Sevodnya"²⁰.

Simplifying the issue, DII officers effectively avoided all activities that could potentially jeopardize the credibility of their informants, even the most basic ones, such as making detailed checks in files, which had to fall within the scope of their official duties. It should be remembered that the "legend" created by GPU agents was not perfect and generated questions for which there was no good answer for example – the question asked by the gen. Yevgeny Klimowicz during a meeting with a representative

¹⁶ E. Opperput's letter to „Sevodnya” newspaper of 17 May 1927.

¹⁷ What's worse he introduced himself to B. Jarociński with his real name, revealing his past, and yet no one considered it appropriate to carry out more extensive searches on him that would reveal his participation in the organization "M".

¹⁸ P. Seljaninow, *Narodnyj sojuz zaszczyty Rodiny i swobody. Wspominanija*, Berlin 1922, p. 66.

¹⁹ See: A. Baczyńska, *Historia dowodu osobistego w Polsce*, <http://wiadomosci.onet.pl/kraj/historia-dowodu-osobistego-w-polsce/sd95s>.

²⁰ Centralne Archiwum Wojskowe (CAW), Oddział II, sygn. I.303.4.2090, „NORD”, intelligence post letter.

of the Board of the Trust, gen. Nikolai Potapov (...) *as he manages to travel for so long in Europe, being an officer of the active service of the Red Army*²¹. The problem was that almost no one asked such questions on the Polish side.

• **Cognitive dissonance** is defined as a *state of tension that occurs when a person has two cognitive elements (ideas, attitudes, beliefs, opinions) that are psychologically incompatible with each other*.²² If the cognitive elements mentioned above *are found in dissonance* (i.e. they are incompatible with each other), there is a sense of discomfort that motivates the individual to reduce it, because one of the basic human characteristics is the belief that life makes sense, and accepting two conflicting ideas deletes the assumed *a priori* logic of existence.²³ The more someone is involved in some action resulting from the accepted belief, the greater the resistance to information that threatens this view.²⁴ The reduction of dissonance results from the process of distorting, discrediting and selecting of information, thanks to which one's own convictions are protected. This is a process that has been tested in both laboratory conditions²⁵ as well as on historical examples, the most famous of which are analyzes of Jewish population behavior during the *Shoah*, who, despite more and more information about the genocide taking place, consistently tried to discredit the threat.²⁶

The activities of Division II, after contacting the Trust and signing agreements with monarchists (first by the DII intelligence post in Reval and then by the HQ in Warsaw), had all the features of the classical reduction of cognitive dissonance. From 1921 to 1927 – not counting the so-called W. Michniewicz's report – there are no traces in the archives indicating that anyone from DII had seriously considered the possibility that the MOCR-Trust representatives could be GPU agents.

Throughout his stay, Y. Artamonov in Warsaw was not checked. No one has ever wondered where he gets his money for a good life from, although this is a question that is crucial for any person who is in constant contact with the intelligence service, especially if this person is a foreigner from a country considered as the main opponent. The same situation took place in DII posts in Moscow: no one was struck by the thought that Opperput regularly visited Polish diplomatic mission and – despite this – did not become the object of interest of the GPU, although the implications of this fact were so obvious that informant of W. Michniewicz, Colonel W. Drobyszewski automatically recognized this as symptoms of a GPU provocation, and the Polish liaison officer with the Trust, Władysław Michniewicz, after a conversation with Colonel W. Drobyszewski, also discovered this obvious truth and was so impressed with it that, without any solid evidence, beyond the sense of the obvious lie in the face

²¹ This case illustrates well that the legend of GPU agents had “holes” that were relatively easy to spot and – using the capabilities of the intelligence organization – to verify suspicions.

²² E. Aronson, *Człowiek – istota społeczna*, Warsaw 1987, p. 134.

²³ *Ibidem*, p. 134.

²⁴ *Ibidem*, p. 137.

²⁵ *Ibidem*, pp. 134–190.

²⁶ *Ibidem*, pp. 147–148.

of the Soviet realities, he went to Warsaw with a report on the subject. It should be noted here that the fact of writing a report on the Trust by W. Michniewicz should be considered highly probable – despite the lack of the document in archives – for four reasons:

1. In 1923, Michniewicz had indeed suffered harassment from the leadership of DII, as a result of which he went to the line service in the regiment in Rivne, although there was no indication in his previous career that he deserved such a penalty.
2. The source of information (i.e. Col. W. Drobyszewski) existed.
3. About his report from 1923, a deputy head of the “East” Department in 1922–1923, Władysław Kowalewski wrote in the letter.²⁷
4. W.T. Drymmer’s article from 1965 is not a direct confirmation.²⁸ However, the course of events given by him corresponds roughly to the version presented by W. Michniewicz, which may mean that this story was known to Drymmer. We also know that Cpt. W.T. Drymmer did not report his suspicions about the Trust in 1923. In his written explanations regarding the scandals of the organization “M” from 1927, he did not mention a word about such an event, although he acted under pressure as an external service officer accused by E. Opperput of cooperation with the GPU. It may result from the fact that he attributed others merit to himself, which, it seems, corresponded to his psychological profile. This probably means that Michniewicz’s report was known to him, so it can be assumed that the report existed and could be discussed in the environment of the officers of the DII and W. Michniewicz did not lie in his memories.

The course of discussing the contents of the report with Michniewicz’s superior Cpt. M. Talikowski fully complies with the assumptions of cognitive dissonance theory:

(...) Drobyszewski scares us with GPU, probably out of fear, he sits like a mouse under a broom. In Warsaw – Talikowski argued – we have comprehensive sources and wide possibilities of their control. We have contacts with General Klimovich and Kutepov who have their own agents network in the Soviet Union. We have a MOCR delegate here, Captain Artamonov, not only a brilliant guard officer whom you know from Reval, but a groomed and intelligent man. He is of the best opinion on Trust and announces the imminent arrival to Warsaw of a special mission from Moscow for political-military negotiations at the highest level! Levels to which you do not grow up, constantly communicating with Kasatkin, both in the role of postmen.²⁹

From the memoirs of W. Michniewicz it is clear that the head of the “East” Department used all known strategies, to reduce cognitive dissonance: he ridiculed

²⁷ W. Michniewicz, *Wielki bluff sowiecki...*, pp. 135–136.

²⁸ W.T. Drymmer, *Trust*, „Kultura” 1965, No 11.

²⁹ W. Michniewicz, *Wielki bluff sowiecki...*, p. 132.

and underestimated the thesis of Colonel W. Drobyszewski, he relied on (non-existent *de facto*) opportunities to verify Trust information from independent sources, and finally, when W. Michniewicz did not stop talking about the case, he got rid of him, assuring himself a psychological comfort by eliminating the source of unpleasant information. Behavior of Cpt. M. Talikowski³⁰ also points out to reducing dissonance in the situation of emotional involvement, namely, the decisive removal of the source of information contrary to the adopted position. M. Talikowski, it seems, was an active co-victim of the Soviet lie. Accepting Soviet disinformation was beneficial for him: it favored his career (despite bad opinions of the management about his intelligence and abilities), what gave him the money needed to finish his villa and allowed him to play the role of the *wizard of espionage* among snobbish aristocrats from the Ministry of Foreign Affairs who, in the hope of regaining property in the east, were eager to hear information about the impending break-down of the Soviet state.³¹

Another example illustrating the effect of cognitive dissonance among DII officers involved in cooperation with the Trust are explanations of A. Niedziński. For example, an extremely characteristic description of the GPU's apparent failure, when in the autumn 1925 Trust agents provided the Poles with false information about the alleged maneuvers of Soviet troops:

Fortunately, however, our intelligence has noticed this inspiration; I therefore demanded a categorical explanation and a thorough examination of this case. I exactly remember this conversation with members of "M" – Fiodorov, Potapov, Denisov and Kasatkin, upon whom my statement that the documents were inspired by the GPU made a strong impression (...). It was not difficult to refute this assumption, because this document was provided simultaneously by 3 sources: from R7 / I, from post "Bałt" and, if I am not mistaken, from the "Szperacz" (...) it should be noted that the "Szperacz" received this document from an agent as inspired one by the GPU. After this statement, there was nothing else to left for them, but, to say, after some time that indeed their man in Kiev came across a GPU agent from whom he acquired the document. I was, therefore, informed that they had one organizational link with them, and that unfortunate intelligence officer was shot. I reported at the right time about the above, being of the opinion that such an accident is possible under the conditions of conspiratorial work.³²

It is not difficult to notice that the Polish side ignored the extremely clear symptoms of being a victim of disinformation. The motives for which the GPU transferred the same document to a few intelligence units of DII at the same time – as if making sure that the Polish side will surely understand – adding in one instance the information that it was inspired – is unclear. It should be presumed that the Soviets had a sense of full

³⁰ Who fired W. Michniewicz from the military intelligence.

³¹ W. Michniewicz, *Wielki bluff sowiecki...*, p. 100.

³² CAW, Oddział II, sygn. I.303.4.1781, the annex 130 to *Arkusz obserwacyjny org. „M”*.

control over the Division II and, perhaps, they wanted to check the verification procedures used by Poles in a situation of obvious disinformation. If this hypothesis is correct, it should be emphasized that Division II did not use ANY methods of verification, apart from telling GPU agents not only the information that the document is false, but also the knowledge of how the Polish intelligence came to such beliefs.

The same situation took place in the case of a mobilization document provided by the Trust, which was questioned by Polish analysts. A. Niedziński described the matter in the following way:

Speaking in this matter with the organization [MOCR] I informed them on the accusations that had been made to the above document and I pointed out that they were inspired by the source providing them with the above document. For my part, however, I could not reconcile myself with the idea that the organization “M” was exposed to the GPU, coming to this conclusion on the basis of the known GPU work systems, and a whole range of data arguing with the impossibility of similar supposition.

Explaining, why he was not persuaded by the arguments of the Polish analysts, he added: (...) *the institution did not have and could not have a test, using only logical arguments stemming from the knowledge of the area and based on moral conviction.*

In order to fully grasp the stupidity of the above sentence, one should realize that the Soviet document was falsified extremely ineptly, because it suggested that mobilization plans in the event of war with Poland predicted an attack from the south, from Ukraine – which was inconsistent with all previous general staff plans anticipating the dislocation of troops by the so-called Smolensk Gate. This was absolutely unrealistic due to the lack of a dense network of rail and road connections.³³ Thus, the “moral conviction” evoked by A. Niedziński was, in fact, an iron logic that excluded this direction of dislocation.

Symptoms of continuous reduction of dissonance can be observed in the behavior of the Polish officers both in the initial stages of operations and after the self-disclosure of the Trust, when it was no longer possible to maintain the illusion that the Polish intelligence in the east had a powerful and influential organization providing a wealth of intelligence information.

One can see them on the example of the Lt. Col. L. Bociański’s reaction to the revelations of E. Opperput³⁴ and finally in the course of the so-called Bociański’s commission, in which *strictly* political motifs overlapped with multi-level denials generated by the reduction of cognitive dissonance.

• **Group thinking syndrome** – (...) *group thinking refers to the decline of psychic efficiency, realism and moral judgment caused by intra-group pressure.*³⁵

³³ W. Michniewicz, *Wielki bluff sowiecki...*, p. 248.

³⁴ CAW, Oddział II, sygn. I.303.4.2090, a letter from 25th May 1927.

³⁵ W. Domachowski, S. Kowalik, J. Miluska, *Z zagadnień psychologii społecznej*, Warszawa

When such a phenomenon occurs, the following defects of the information flow process in the group take place: limiting the discussion, to consider a limited number of alternatives, avoiding re-analysis of the original solutions, neglecting the solutions rejected at the beginning, resigning from external expertise that can evaluate alternative ways of acting, accepting only facts and assessing the adopted direction and ignoring the influence of negative factors on the expected results.³⁶ An important factor in the occurrence of group thinking syndrome is a group cohesion (*esprit de corps*), isolation from qualified associates and experts, and preference given by the management (group leader) of a specific solution.³⁷

Based on the research of Irving L. Janis on this subject, the following symptoms of group thinking can be distinguished³⁸ in the activities of DII during Trust operation:

1. **An illusion of omnipotence and invincibility that creates an optimistic conviction of success and daring to take risks.** This symptom can be seen in the behavior of almost all officers of DII, both from HQ (which formulated extremely bold expectations of operational gains in relation to intelligence centers in the east, ignoring the realities), as well as officers of the external service (who notoriously violated the basic principles of conspiracy of intelligence work³⁹).
2. **Collective defensive rationalization of the adopted solutions** (i.e. the process of cognitive dissonance discussed already by the group involved in the defense of the adopted assumptions).
3. **Stereotypical image of the opponent as too bad to enter into agreements with him or too stupid to thwart any, even risky plans.** This symptom corresponds with the omniscience of omnipotence discussed above. Polish officers, which I tried to show by examples, with astonishing consequence underestimated the opponent, resulting in a disincentive of behaviors such as making illegal interests with GPU agents, ignoring the obvious symptoms suggesting links of acquired sources with Soviet counterintelligence, or even lack of any security of the Polish premises.
4. **Direct emphasis on each member of the group, who presents strong arguments against any of the group stereotypes or illusions.** I think the best illustration of this symptom was the case of Lieutenant W. Michniewicz, who, as a result of writing a report on the Trust putting the organization in an uncertain light (though deprived of a factual base that could realistically threaten to unmask monarchists), was disciplined and removed from the Division II.
5. **Unquestionable faith in the innate morality of one's own group.** This symptom was most visible in the Lt. Col. L. Bociański's report, who – without examining the credibility of E. Opperput's testimony accusing DII officers of treason –

1984, p. 123.

³⁶ Ibidem, p. 121.

³⁷ Ibidem, pp. 123–124.

³⁸ Ibidem.

³⁹ Like ignoring the risk of spy penetration by officers of the Polish military mission.

at the beginning of talks with Finnish officers, declared full confidence in his officers, which certainly affected the subsequent findings of the commission, which found no guilty party, what blocked drastic measures that could have cleaned up the Polish intelligence of the supposed Soviet spy-rings.

6. **Blocking the processes of evaluation and verification of assumptions resulting in self-censorship of deviations from group solutions.** As I have already mentioned, from the article by W. Drymmer (and from the letter of W. Kowalewski quoted by W. Michniewicz) it seems that the case of W. Michniewicz's report was known among the members of DII, however, there are no traces in the documents proving that any of the officers formulated in writing doubts about the Trust. From the preserved documentation, it appears that until 1927, Division II had no suspicions Trust's "monarchists". So, even if the officers repeated themselves in the form of whispered gossip, the history of the report by W. Michniewicz, they presented a line in line with the expectations of the management convinced of having an excellent source on the highest levels of Soviet power.
7. **The illusion of unanimity stemming from self-censorship.** If we assume that Polish officers censored their own conclusions in the materials of the case, each person having access to them, had to believe that **everyone** having to deal with the matter evaluated it positively. Such conclusions were then forwarded to the next desk officers dealing with the case (an example of that are explanations of Capt. A. Niedziński) what completed the illusion of unanimity ratings accepted as a basis for further contacts with the Trust.
8. The final symptom of the syndrome of group thinking is establishing group **guardians of correct thought**, to protect against a tributary of information that could destroy the group's complacency with the adopted decisions. In my opinion, this role was fulfilled mainly by M. Talikowski, who, if you believe Michniewicz, went so far as to damage or hide his report.⁴⁰

Ad. I.2. Structural factors

- Military organization with its rigid hierarchy and subordination levels, based on the undisputed execution of orders, of course attracts people with a predisposition to authoritarian attitudes, who are then amplified and shaped. Authoritarian personality⁴¹ is understood as a group of features, which include mainly: the recognition of conventional values, intolerance of weakness in ourselves and in others, a strong tendency to punish, suspicion, but above all an extraordinary respect for authority and the stiffness of cognitive, or low susceptibility to change one's views.⁴²

⁴⁰ W. Michniewicz, *Wielki bluff sowiecki...*, pp. 132, 137.

⁴¹ E. Aronson, *Człowiek – istota społeczna...*, pp. 248–251. See: T.W. Adorno, *Osobowość autorytarna*, Warszawa 2010.

⁴² E. Aronson, *Człowiek – istota społeczna...*, p. 249.

This type of personality combines in itself two types of conformism: **giving in** (individual behavior is motivated by a desire to obtain a reward or avoid punishment) and **identification** (behavior and beliefs are shaped by the desire of the individual to become more like a person recognized as a model⁴³). In creating a young officer it plays a huge role, because both enforce specific behaviors and beliefs (at least presented to the public), as well as the imitation of older and positioned higher in the hierarchy superiors. DII, as a part of the Polish Army, at least to some extent, reflected the personality trends described above. This affected all aspects of its activities, including intelligence operations.

As an example, one can quote memories of the officers involved in the cooperation with the Trust, who – while dealing with even the most absurd decisions of superiors – succumbed to their orders, even when they had a firm conviction that they were right. In his memoirs, W. Michniewicz openly writes that after the rejection of his report by Capt. M. Talikowski he took no steps, to notify other superiors. Of course, he rationalized his behavior years later, writing that [...] *there was no point in going for a complaint to a higher level – as to whom? For blinded by parliamentary politics Bajer, ignorant intelligence officer?*⁴⁴, but one must explicitly tell say that W. Michniewicz did nothing, probably because he was afraid of further persecution (which occurred despite of it), and realized that his superiors showed solidarity in bullying recalcitrant subordinates.⁴⁵

W.T. Drymmer's memories about his alleged unmasking the Trust reveal the same degree of powerlessness against arbitrariness of superiors:

After returning to Warsaw once again I informed my superiors that we were blind tool in the hands of the Soviets. I was backed up by two officers: (...) whose task was to study the quality and accuracy of our intelligence received by the message. Despite of our reservations – my talented officer Werner was dismissed and another took over his post, also a brave officer, but unfortunately inexperienced, Major Niedziński.⁴⁶

W.T. Drymmer's article, like memories of W. Michniewicz shows conformist subservience to superiors of people who declared to have known **about taking place before their eyes the Soviet secret police's operation threatening Polish interests**. At the same time – an important detail – none of their contemporaries questioned their behavior. Filling commands of superiors was higher in the hierarchy of values than interests of the service and the state itself.

An identical situation is found in another document on cooperation with the Trust, this time prepared by Lt. T. Werner, whom Lieutenant Colonel I. Boerner ordered to contact his aide, J. Szczepkowski with E. Kasatkin-Opperput:

⁴³ Ibidem, p. 57.

⁴⁴ W. Michniewicz, *Wielki bluff sowiecki...*, p. 132.

⁴⁵ F. Kusiak, *Życie codzienne oficerów Drugiej Rzeczypospolitej*, Warszawa 1992, p. 258.

⁴⁶ W.T. Drymmer, *Trust...*, p. 99.

Because this order I found to be inconsistent with the instructions and directives (...) I delayed the execution of it. After a long time I was called to the colonel, who in a very concrete form ordered me within 2 days to get in touch Szczepkowski with the organization "M". Unable to resist as the clear command (...) the next day I went to see Szczepkowski car at the appointed place, where he was waiting for us and got into the car of magician (Opperput). In the car Szczepkowski told him that under the directives he has with him he demanded that the "beard" to come in the coming days to the Attache premises. At first I tried to resist (...) nolens volens I agreed. It took place on Saturday, February 2. The "magician" asked him to meet him in order to go to Attache premises on November 5, 1924, but he did not show up for a tryst. I suspected he would try to avoid a meeting. The same evening the Colonel asked me, if his order had been carried out, I reported to him that the agent did not turn up, so that the Colonel declared that he only saw my ill will and categorically demanded a tryst. The next day I communicated with the "Magician" and we agreed that he would go to Attache premises with me, 8.2, which was also brought to fruition. In Attache premises, he talked to Szczepkowski about 4 hours almost exclusively about the internal political situation in Russia. That same evening (...) I wanted to be present while Lt. Szczepkowski reported to Colonel about the conference. After having listened to the report, Boerner told Szczepkowski to write on the basis of information obtained a report on political situation (...) Since I have found to be clearly not desirable, to contact my people with any of Polish officers, in particular, the adjutant of Colonel in a place so discredited as Attache building (...) and taking into account the services that gives us "M" as a source of intelligence, I find Szczepkowski's meetings with their people, especially during the current political repressions as extremely undesirable – increasing the chances of disclosure, I am asking of instructions in this regard for the future.⁴⁷

This fragment is determined uniquely by the conformity to higher rank officers in a situation of unclear subordination chain. T. Werner, although was aware of the fact that the order of Lieutenant Colonel I. Boerner was given contrary to the most elementary principles of intelligence work what could lead to unmasking the whole organization "M" effectively cooperating (as he thought) with Polish intelligence, after a short hesitations did it and only having done this, demanded from his superior tips in the event of such situations in the future.

Authoritarianism of Polish military intelligence organization could be noticed in thoughtless acceptance of superiors views by intelligence officers. As an example, let's take a piece of explanations of A. Niedziński from 1927:

⁴⁷ CAW, Oddział II, sygn. I.303.4.1781, a letter No 015/24 14.02 1924.

In this place I must emphasize that both the instructions received by me from the Department of Intelligence, as also from the post R7 excluded any distrust as to the very existence of the organization [Trust] as a new man in espionage, I gained the strong conviction that the organization was based on the ideological ground. My faith apparently was based on the basis of the results of the intelligence⁴⁸ work in the form of documents and information and the result of observations resulting from the correspondence control on "M".

The sentences above show that A. Niedziński, coming to Moscow, **had already formed an opinion on Trust, which he drew entirely from his superiors**, because who else from the Department of Intelligence and R7 post could enter it into the secrets of the tasks allocated to him? No wonder, therefore, that in the rest of his explanation, he described the Trust consisted only of professionalism and commitment to its tasks. The officer sent to Moscow without any experience and very limited intelligence level, took for granted what his superiors had told him, and later – acting on the basis of this pattern – became a zealous, though probably unwitting, accomplice of the GPU.

Summing up, we have to come to the obvious conclusion: as in all authoritarian institutions, in DII information and opinions went from the top of the hierarchy down, and any attempt to formulate opinions contrary to the already formed opinions of superiors met with rejection and ridiculing the authors.

- Hierarchically built intelligence organization, in which the supreme driving force of human behavior is the desire for vertical promotion (because in institutions with a strictly respected hierarchy that guarantees high salary and prestige) at the moment when the disinformation operation takes place, especially when it is accompanied by infiltration by the enemy, shows a natural tendency to persistently fail to see the problem. As J. Masterman writes, describing his own experiences of deceiving the Abwehr during World War II:

The mere fact that we were constantly reviewing so many different, detailed information, made it seem obvious to us that sending a message must burn the agent. In reality, however, this case looked different and for many reasons. First of all, the first instance to which the agent sent information was his superior, who in turn passed it to the higher superiors, very often without a detailed examination of them. Even if the errors or misinformation contained in the information consisted of mutual contradictions, it is unlikely that the higher superiors will have such accurate information that these errors and contradictions can be noticed. It may even happen that the right source of information will not be replaced, as the agent's direct agent will want to preserve its prestige, especially if, in addition to real agents, he still has his fictional agents. If even the higher

⁴⁸ CAW, Oddział II, sygn. I.303.4.1781, the annex 130 to *Arkusz obserwacyjny org. „M”*.

authorities make some suspicions, then this direct supervisor of the agent will do everything because of his prestige and personal benefits to defend his informant.⁴⁹

To put it a little easier: in the hierarchical intelligence institution, obtained agent's information gives benefits to the entire chain of superiors supervising the agent and his desk officer, and if the information corresponds to the assumptions of governing politicians, even to the highest posts of the organization. In turn, the detection that the piece of information was incorrect or false (especially when it has already been given to higher superiors) discredits the same chain of intermediaries, putting in a bad light their professionalism and common sense, and this might compromise the main purpose of their activities in the institution hierarchical, i.e. a career. An additional element mentioned by Mr. Masterman is the natural tendency of intelligence institutions, to avoid scandal at all costs, because it would result in the possibility of an audit from the outside, due to the phenomenon of simulating work and extort money from the budget on operating with fictitious sources. There was this phenomenon in all services, although in varying degrees. It is difficult to determine what was the percentage of "dead souls" in DII, but – for comparison – General Szlachcic defined their number in the communist Security Service on 30%, and wrote that the entire industry was created, to extort money, which dragged on colleagues and family members⁵⁰. In Division II the phenomenon occurred with certainty, as evidenced by the indictment of Major. J. Sosnowski, which clearly showed that he used a fictitious agency, to increase the pool of money received from the center.⁵¹

Also, one should not forget about the financial practices of officers involved in the black market contraband, what was at least tolerated by their superiors. All this meant that almost any level of this structure there was a strong will, to prevent the scandal which might lead to in-depth, prosecutorial control of intelligence activities and ultimately to break the careers of many.⁵²

Consequently, there was no real motivation on the part of DII, to reliably verify the information obtained from the Trust. Even in a situation already described obviously forged mobilization document, despite the obvious symptoms of misinformation, was not rejected, instead DII demanded some additional information, even though Polish analysts proved the logical assumptions were nonsense. And when, in April 1927 truth of the Trust was disclosed, DII first for a long time deluded themselves that this is

⁴⁹ J. Masterman, *Brytyjski system podwójnych...*, pp. 56–57.

⁵⁰ J.S. Mac, *Przesłuchanie supergliny*, Warszawa 1990, p. 33.

⁵¹ Archiwum Instytutu Pamięci Narodowej w Warszawie (AIPN), sygn. BU 01480/331; K. Graczyk, *Sprawa majora Jerzego Sosnowskiego w świetle niemieckich i polskich akt procesowych*, Katowice 2015, not published master thesis, UŚ, pp. 239–250. See: H. Ćwięk, *Rotmistrz Sosnkowski. As wywiadu Drugiej Rzeczypospolitej*, Kraków 2011; Ł. Ulatowski, *Berlińska placówka wywiadowcza „In.3” (1926–1934). Oddział II i działalność majora Jerzego Sosnowskiego w Niemczech*, Warszawa 2016; P. Kołakowski, A. Krzak, *Sprawa majora Jerzego Sosnowskiego w świetle dokumentów analitycznych Oddziału II SGWP i zeznań Franza Heinricha Pfeifera*, Warszawa 2015.

⁵² Compare CIA activities towards Y. Nosenko.

only a partial failure of the essentially really existing organization “M”, then it began to disavow E. Oppenput’s disclosures, but only in the part relating to Soviet agents in the Polish General Staff⁵³, while trying to figure out whether ambiguous role of DII might be noticed in the West.⁵⁴ In the final step – using the so-called. Bociński’s committee – they covered up the matter, blurring responsibility and the possibility of blocking sanitation measures.

• J. Masterman as a key element in the success of disinformation operations conducted by MI5 against the Abwehr held **dominance of personal interests over common interests among the German intelligence officers**. He wrote as follows:

Almost always, when the Germans committed a fundamental error, it turned out that this was due to personal motives of some employee of the Abwehr. He made money and he gained prestige through his agent, thanks to him he could safely live in a neutral port, so he could not and did not want to objectively and fairly evaluate the agent and his work.⁵⁵

J. Masterman practical observation applies also, unfortunately, in full to the Division II. Headquarters sent officers to Soviet Russia, having been completely detached from the realities in Russia, without any ideas, on how to conduct intelligence activities there. As a result, the officers were trapped: they pursued unrealistic tasks given by the Headquarters, surrounded by 24-hour surveillance and by informants of the GPU located in the diplomatic premises of Poland, probably constantly overheard and usually deprived of even such obvious tools of labor, as the money in the right amounts. Counterintelligence control conducted by the GPU was driven up to the level usually associated with countries at war, and this meant that the effectiveness of Polish officers had to be extremely low.⁵⁶ Thus, Polish scouts were in an extremely difficult situation: on the one hand the real possibilities of intelligence activity were dim, on the other hand, they were bombarded with demands of Warsaw and their failure could have dire consequences for their careers. What was important – the officers going to the intelligence posts, *in fact*, were in a less favorable position than regular officers of the army. Espionage service offered few promotion chances, additionally they were forced to resign from such relative stability of a garrison life.

Thus, it must be said openly that **the interest of the service was in a logical contradiction to the interests of the intelligence posts officers**. Instead of full cooperation with the HQ, there was evident divergence of interests. The HQ demanded fulfillment of unrealistic expectations, while refusing to give enough funds to fulfill these tasks and the officers had to do everything, to remain in the posts, with intelligence success or at least avoiding serious failures. It must be remembered that the intelligence

⁵³ Obvious symptoms of the cognitive dissonance.

⁵⁴ CAW, Oddział II, sygn. I.303.4.2090, a letter No 518/I/C from 26th May 1927.

⁵⁵ J. Masterman, *Brytyjski system podwójnych...*, p. 262.

⁵⁶ *Ibidem*, pp. 236–264.

work abroad meant not only interruption of a career in the military, but also the need to settle property issues in the country. In this situation, the return meant not only a loss of diplomatic diets, but also a number of problems with the re-adaptation. For this reason, as you assume, the GPU provocateurs were sent on fertile ground, because the bad organization of the work of Polish intelligence officers generated a situation where careful analysis *bona fides* of any agent was **not in the interest of the Polish intelligence officer**, who, at the same time activated the dissonance reduction process described above, convincing himself that – even if the agent seems suspicious, he has honest intentions or, in the worst case scenario, one might control him using other sources. Polish intelligence officers, in order to fulfill expectations of the HQ, had to obtain agents, although at the same time full control of the Soviet counterintelligence effectively hindered them to do this, at the same time endangering the risk of detention, beating and sending back to the country. Therefore, there was a psychological readiness to be opportunistic, to accept any agent, who might be the evidence for the HQ, that the officer works and is effective. Such hidden motivation can be widely observed for instance in the characteristic of the agent recruited by R.W. Wolikowski, named Nałęcz-Wojciechowski (*communist mason, occultist type with a very indistinct physiognomy*). Even with the best intentions an agent of such parameters could be believed to have appropriate *bona fides*, and yet he was listed among the members of agents ring exploited by the Polish military attaché.

DII did not establish any mechanism that could objectivize assessment of agents rings cooperating with the post officers, outside rankings provided by analysts in the HQ. This in turn, at some stage of the disinformation operation conducted by the GPU had achieved such a level of saturation with the manipulated information that comparing the newly acquired products of *Krivoje Zerkalo*⁵⁷ to the already existing resources (assuming that the GPU was able to control the internal consistency of misinformation products as effectively as it was done by MI5 during World War II) was not able to detect misinformation, because comparing false information designed so as to fit the previously transferred false intelligence.⁵⁸ The only way to capture the process of misinformation was paying no attention to whether the information fits into their existing knowledge, as it was in a mobilization document described earlier, when Polish HQ pointed out to its contradiction with the existing logistics facilities necessary for the transport of troops. It must therefore be concluded that the Polish analysts were able to draw the correct conclusions, but – according to the rules of deduction – with false premises, they had to obtain false results.

It should be added that the among officers dealing with the Trust during the operation there was constant fight for prestige⁵⁹, the officers were so focused on themselves that they preferred compromising service rather than themselves. This can be noticed in the correspondence of such a good officer as T. Werner, who wrote:

⁵⁷ The interdepartmental Disinformation Office, called humorously “kriwe zierkało”.

⁵⁸ G. Bailey, *The Conspirators*, London 1961, pp. 12–13.

⁵⁹ Compare the demands of Col. Boerner.

I have to report that one of the representatives of the “M” expressed surprise that I did not write to Warsaw on passport for Denisov, to wriggle out of silly situation in which I involuntarily found myself, I said that the statement on the passport was sent to the cipher clerk and it was probably wrongly encrypted.⁶⁰

Summarizing the above, it is as J. Masterman put it: **DII – by the lack of teamwork and close connection between the career of an officer and success gained by his agents without implementing careful validation and continuous verification of *bone fides* of his agents rings, created the organizational framework suitable for success of the Soviet disinformation.**

- Element *sine qua non* of all these factors is relatively low level of professionalism of DII officers, what made possible the occurrence of all of the above mentioned negative phenomena. At the beginning of the 1920s its reasons were obvious: Polish intelligence was created by absolute amateurs from POW youth, whose sabotage and intelligence activities were devoid of any logistics and training⁶¹ and Polish legions officers, whose only experience came down to conducting military reconnaissance and counter intelligence consisting of capturing army defectors and *suspicious men*.⁶² What was the level of the preparation of intelligence personnel is clearly visible from the memories of W.T. Drymmer, which showed that the Polish information service was organized *ad hoc*, and the role of educators of the new intelligence officers was entrusted to former officers of discredited Austro-Hungarian army, which organization, *modus operandi* and operating assets were fully known to the Russians, thanks to the treachery of Colonel Alfred Redl. In addition, Gen. J. Rybak, who led the training, **never alone was not a trained intelligence officer** and the secrets of the work in HK Stelle he learned intuitively. Moreover, his activities against Russia was known to the Russian agent named above – Colonel Redl.⁶³ In addition, if you believe the description of W.T. Drymmer⁶⁴, the same training was carried out in a ridiculous way:

Gen. Rybak in a Polish-Austrian dialect, where he mingled Polish, Czech and German words, gave us professional advice and explained the role of the information officer [...]. My head remained in chaos, I remembered only the words: “szyf, Dancyg, and-but”. All this was rather amusing than interesting.⁶⁵

This situation, of course, should not be surprising: DII was built from the ground up *ad hoc*, without any reliance on major achievements and the experience. The problem, however, was not the fact that the first generation of intelligence officers

⁶⁰ CAW, Oddział II, sygn. I.03.4.1781, a letter No 019/24 from 1st February 1924.

⁶¹ W. Michniewicz, *Wielki bluff sowiecki...*, pp. 12–13.

⁶² J. Rybak, *Pamiętniki generała Rybaka*, Warszawa 1954, p. 102.

⁶³ *Ibidem*, pp. 15–17.

⁶⁴ Gen. Rybak admitted himself not to have any professional training.

⁶⁵ W.T. Drymmer, *W służbie Polsce*, Warszawa–Kraków 2014, p. 84.

were selected from uneducated and unexperienced people, but that later on this generation – supporting each other within the fellow ring, described by W.T. Drymmer as *sitwa* – became the management of DII, imposing their ideas about how one should conduct an intelligence work and decided on the choice of the candidates to the service, their professional training, promotions, etc. That brought about such curiosities of the military bureaucracy, as for example, issuing IDs to the secret agents and giving them the second copy of the contract on cooperation with intelligence service⁶⁶ and a document titled *Rules of conducting intelligence service*⁶⁷, questionnaires used during interrogations⁶⁸ of fugitives and bidders, thanks to whom intelligence queries were brought to official inquiries, as well as the relatively low placement of Polish intelligence residents in diplomatic missions, which made very difficult the cooperation with diplomatic staff. What's worse, the above-mentioned elements also had to be added to the generally low level of military skills of the intelligence staff.⁶⁹

The main problem of DII was not only the professional ignorance of the officers, but also a glaring lack of recognition of the actual situation in Soviet Russia. This resulted in the use of such forms of espionage activity, such as the emphasis on white intelligence⁷⁰ relying on time-consuming reading of the Soviet press and specialist publications, which due to the widespread censorship and common press misinformation – although, sometimes allowed to draw some conclusions – but could not produce results commensurating to the organizational effort needed to acquire and analyze materials⁷¹; the use by the intelligence letters written with secret inks, what – one should think -was the result of a misunderstanding that in Soviet Russia **all the** letters abroad were opened and checked⁷²; or use of so called maneuvering agents who were crossing the border to collect information on the relations in the Soviet Union and so bizarre ideas as recruitment of agents in the railway stations toilets, who were to eavesdrop Soviet railway workers.⁷³

From the point of view of the intelligence system structure, DII was characterized by three major defects, which had repercussions on its functioning:

- 1) described above establishing intelligence agency from scratch, without the basic *know-how*, with un-selected people and, because of their rapid war promotions, occupation of their leadership positions in the information service;

⁶⁶ K. Danielewicz, *Formy i metody pracy operacyjnej wywiadu polskiego w latach 1921–1939 na przykładzie Lwowskiej Ekspozytury nr 5 Oddziału II sztabu Generalnego (Głównego)*, in: *Wywiad wojskowy II Rzeczypospolitej*, P. Kołakowski, A. Peplowski (red.), Kraków 2011, p. 305.

⁶⁷ Ibidem, p. 308.

⁶⁸ Ibidem, p. 292.

⁶⁹ Ibidem, p. 283.

⁷⁰ Ibidem, p. 288.

⁷¹ For instance, CIA was not capable of foreseeing the decline of the USSR.

⁷² Even in years 1945–1990, the postal channel was the best source of intelligence for the communist service in Poland.

⁷³ K. Danielewicz, *Formy i metody pracy operacyjnej...*, p. 288.

- 2) a placing of the intelligence in the army, which contributed to a specific negative selection of the officers wanted by the service, resulting from the fact that the intelligence officers were usually overlooked in promotions and decorations and the head of Division II did not have the freedom of choice of candidates and its staff needs were met in second place⁷⁴;
- 3) a constant underfunding of the DII⁷⁵, which suffered from constant money problems, despite the fact that its size – especially in comparison with the services of the Soviet Russia – was almost of grotesque character.

As a result, as K. Danielewicz writes, the Polish intelligence suffered from a constant shortage of talented, intelligent and dedicated to the service officers⁷⁶ who, while on intelligence posts in Russia faced in addition financial problems, lack of office space and constant surveillance by the Soviet counter-espionage.

During the operation Trust, a lack of even elementary professionalism was constantly observable. Perhaps the clearest evidence of a complete lack of knowledge about the realities of Soviet Russia are memories of W. Michniewicz, who – yet not wanting to ridicule himself – completely discredited himself as an intelligence officer, of which must be concluded that he wrote the truth, even decades after not realizing his mistakes. He, along with the other officers of DII did not see anything wrong in it, to send Trust's reports with the Polish encoded with the Polish cipher, so the Soviet decryption did not have any problems with breaking the Polish codes⁷⁷, and letters of recommendation to the generals of the Academy of the General Staff of the Red Army he held hidden... in a suitcase under his bed. This does not exhaust the list of mistakes made by him. One can look through the contents of his report from 1923 on Trust, to grasp the enormity of ignorance of Polish officers. Quoting a conversation with his informant, Colonel W. Drobyszewski, Michniewicz did not give any substantial information which might unmask the Trust. The entire contents of the report consisted only of opinions of his informant, which *dazzled the* Polish officer:

The conspirators remain in constant communication with foreign countries, and in Moscow and the provinces massively recruit members? They are in government positions and provide intelligence materials? They easily go abroad and come back safely, like going to a picnic in suburban Sokolniki? With today's terror? (...) Only idiots can believe it! This is an overt provocation of the GPU (...). It's a terrible humbug, it is a great stupidity on your part, believe in such nonsense! Every ex-tsarist officer, let alone our generals in positions at the General Staff Academy, must be kept under surveillance (...). The intelligence documents are certainly falsified, bait

⁷⁴ CAW, Oddział II, sygn. I.303.4.1144, Col. Glabisz's financial control report from 16th February 1932.

⁷⁵ CAW, Oddział II, sygn. I.303.4.1781, a letter No 024/24 from 18th March 1924.

⁷⁶ K. Danielewicz, *Formy i metody pracy operacyjnej...*, p. 318.

⁷⁷ *Ibidem*, p. 295.

for suckers! (...) Kasatkin goes to the Polish consulate, how to the public bar? And Yakushev – the conspirator flaunts like a journeyman Chicherin? Only the blind does not see that the whole “organization” is a GPU tool!⁷⁸

Just think for a moment about this sentence, to understand that the Polish intelligence officer issues a clear assessment of the effectiveness of his own professional preparation. The text shows that he did not understand that both Polish officers and the covers used by them were constantly under GPU surveillance; he did not understand that every Russian who came to the Polish embassy or consulate became the object of operational interest of the GPU, he did not seem to understand the scale of constant surveillance and terror that effectively blocked contacts between Soviet citizens and foreign diplomatic missions⁷⁹. This may mean that the Polish intelligence at the beginning of the 1920s had a limited diagnosis of the Soviet realities or that it completely disregarded these realities.

Overview of the archival materials of DII on the cooperation with the Trust is unfortunately also an illustration of the above. They show the actual level of professionalism and disregard for the basic principles of a conspiracy by the Polish officers both at the posts and the HQ.

We know from both memories W. Michniewicz and Sergiej Wojciechowski, that the meetings with the delegations of alleged monarchists coming to Warsaw for discussions with the leadership of DII took place in Warsaw's trendy restaurants. Moreover, S. Wojciechowski says that to the intelligence *rendez-vous* Capt. M. Talikowski came in regular uniform.⁸⁰ The same captain. M. Talikowski, informing Y. Artamonov about the date of transfer of the Trust's agents through the so called window, left an open note about this matter to Artamonov's Russian wife. As I have already mentioned, the activity of Y. Artamonov in Warsaw did not meet with any interest of DII, despite the fact that the young aristocrat had lots of money without having no permanent work. Polish counterintelligence was not even interested in him, when he started recruiting Polish ministerial officials to the Warsaw Trust post named ZJARMO⁸¹. When in 1927 – most likely, to increase information chaos ruling among Polish officers – S. Wojciechowski (yet another agent of the OGPU) and a certain Andro provided information that Mr. Artamonov probably was in 1918 a VChK agent, receiving this information to M. Freyman with disarming candor wrote in the report that he resigned of the protocol, because both Russian gentlemen had reserved discretion.⁸² In the archive there are no signs of any attempts, to verify this information by Polish intelligence.

Another example of the inconceivable naiveté of the DII management are two preserved documents from 1927:

⁷⁸ W. Michniewicz, *Wielki bluff sowiecki...*, pp. 128–130.

⁷⁹ Although T. Werner obviously noticed the problem.

⁸⁰ S. Wojciechowski, *Triest. Wspominanija*, London (Canada) 1974, p. 34.

⁸¹ W. Michniewicz, *Wielki bluff sowiecki...*, p. 114.

⁸² CAW, Oddział II, sygn. I.303.4.2090, report to Major J. Grudziński from 1st July 1927 (annex 183).

Alexandrovich [Y. Artamonov] reported that in the Afghan Legation in Moscow operates one of the sisters Straszkievicz, which by 1921 was met and contacted by Fedorov and Kolesnikov. To find out whether the recent arrests apply to the Straszkieviczs and to explore, whether they are at the service of the GPU, Alexandrovich gave me a letter to Varvara Nikolaevna Straszkievicz asking for discreet delivering it to her and receiving an answer on the spot.

I want this letter to be sent to Moscow and to be established:

- 1) whether VS works at the Afghan embassy,
- 2) whether she would want to give a written or oral answer to this letter too the bearer,
- 3) in the case of her refusal to inform our military attaché about the work of the agents of the GPU in the Afghan embassy.⁸³

Attached is the letter written by Mr Artamonov to Mme Straszkievicz allegedly clerk at Afghan embassy (...). I am expecting an answer, whether Straszkievicz works at the embassy, if not, when she was released and under what circumstances.⁸⁴

The above note and its result in a form of a cipher text to Moscow are extraordinary examples of naivety of Lt.-Col. T. Schaetzel. It is enough, to read the instructions given by him to his subordinates, to understand the situation. The head of the Polish intelligence received from a Russian suspected of having ties to the GPU information, which evidently had only bolster the confidence of Poles to Y. Artamonov (because he still provided them with operational information), and makes his subordinates pass a note to Artamonov's aunt which is supposed to be the agent of the GPU in Moscow. Head of the Division II apparently did not see the absurdity of commands given by himself, according to which the Polish intelligence officer was supposed to deliver a letter too the GPU agent from a relative unseen by her for over 10 years, including a request for information as to whether she actually works for the GPU. Aside from the absurdity of the idea that the active agent of the GPU had to admit to an unknown man claiming to be a Polish diplomat that actually she executes the orders of the Soviet counterintelligence, it should be noted that Lieutenant Colonel T. Schaetzel's command was not only stupid, but in addition absolutely insignificant for the Polish intelligence, which instead of checking whether Y. Artamonov is an agent working for the GPU in Warsaw, had to perform a ridiculous operation, contacting with Artamonov's aunt in Moscow, to determine whether or not she is a spy at the local Afghan embassy. In addition, no one noticed that the information about Y. Artamonov's aunt Straszkievicz was supposed to give some credibility to the version promoted by the GPU from the beginning about the Trust, according to which the GPU operation in Reval was

⁸³ CAW, Oddział II, sygn. I.303.4.2090, a document titled PRO DOMO.

⁸⁴ CAW, Oddział II, sygn. I.303.4.2090, a letter for the military attaché in Moscow (no other references) from June 1927.

a coincidence cleverly deployed by W. Steckiewicz, not a planned performance for expatriates and western intelligence, what dismissed suspicions towards first actors of the affair, i.e. Y. Artamonov and V. Shchelgachev.

Sending to Finland Col. Bocianski for questioning Opperput, although he knew neither the language nor the Soviet realities, as well as dispatching with him Capt M. Talikowski, who was responsible for the whole affair and was interested in sweeping all this under the carpet, do not exhaust the list of mistakes made by the Division II. As it is apparent from archival materials, Capt. M. Talikowski, sending his own agents to Soviet Russia, asked Trust agents for help in their journey and providing them documents and arranging in Russia funds needed to start a business.⁸⁵ This means that he broke the most basic rule of intelligence work prohibiting informing agents about other agents operating on the same territory. From the same source we know that DII under the direction of Capt. M. Talikowski – was engaged in some type of economic cooperation with the Trust, leading negotiations with one of the Polish ministries called in documents *Ministerstwo Gosudarstwiennych Imuszczeztw*.⁸⁶ That was yet another basic error of involving Polish officers in unclear business ties with their agents (as it turned out in the future – double agents), which always creates a risk for the officers.

Not only headquarters behaved in so outrageously unprofessional manner. The DII Office in Vilnius hosted with honors a delegate allegedly from so called Eurasia, A. Denisov, who, thanks to parties with the Office chief W. Sekonda⁸⁷ was able to not only conduct a reconnaissance of Polish institutions, but also to establish relations with the DII Office beyond the control of the DII center in Warsaw.⁸⁸

In Moscow, disregarding the previously described total immersion of Polish officers in the GPU agents net, resulting in total control over their activities, there were also bizarre cases, such as the destruction of letters sent by the Trust via Polish diplomatic mail due to the use by Polish clerks bad chemical reagents in an attempt, to open them secretly, what revealed to the GPU that Poles controlled Trust's correspondence.⁸⁹ The ridicule of that action consisted from the fact that during the visit of Lt. Tadeusz Werner in Warsaw, Cpt. T. Rybotycki ordered him to open the Trust's correspondence, to demonstrate to other officers how it should be actually done.⁹⁰ Whereby, T. Werner, who normally used a bone as a tool for smoothing the wrinkled by the chemicals paper, could no do that, because of... lacking bone⁹¹. It says a lot about the technical level of the Polish intelligence and the recklessness of its management.

⁸⁵ CAW, Oddział II, sygn. I.303.4.1781, a text in Russian without any references.

⁸⁶ Ibidem.

⁸⁷ W. Michniewicz, *Wielki bluff sowiecki...*, p. 165.

⁸⁸ CAW, Oddział II, sygn. I.303.4.1781, a text in Russian without any references.

⁸⁹ CAW, Oddział II, sygn. I.303.4.1781, a letter from the intelligence post „R.7/I” to Referat Centralnej Agentury, l. dz. 013/24 from 6th February 1924.

⁹⁰ Ibidem.

⁹¹ Ibidem.

Another example of an almost comic character was provided by the Polish scout, (probably Edward Czyżewski) his agent in Russia with a wrongly written phone contact number. Whereby the collaborator of the Polish intelligence rang with the agreed password to a private apartment in Moscow. Then, the agent waited in vain for the appearance of a Polish officer in the place and time given to him as a backup, in the absence established telephone communications. No one appeared, so distraught Russian agent, unable to call a meeting with the Poles other, simply went to the Polish embassy.⁹²

Of course, the above examples can be regarded as anecdotal, but they show serious system errors committed during creating and managing the Polish intelligence. The officers, at least at the beginning of the 1920s, had essentially no theoretical knowledge and little practice. The experience was gained either during the war (and therefore fundamentally different from a normal operations conducted in a peaceful period), or during the live operations carried out in Russia

The problem was that the Polish intelligence in the East from the very beginning was controlled by the Soviet counterintelligence, flooding it with agents-provocateurs. Thus, the Polish officers, learning the job during their missions and transforming their experience in the spy's *know-how*, from the beginning were systematically deceived. In such conditions it was impossible, to create an efficient structure of intelligence – in fact there was no real experience, which could become the groundwork for the development of effective operational instructions. You can figuratively say that DII in their operations in the East since the very beginning based his knowledge and professional experience on the illusions provided by the Soviet double-agents system.⁹³

Moreover, neither in the operation, nor in 1927, when it became clear that – as S. Mayer wrote – *there was nothing secret in the Polish secret service*⁹⁴, DII took no remedial action aimed at changing personnel and adopting a set of new operational solutions.

The lack of professionalism of the Polish staff described above was the result of erroneous system solutions. Polish military intelligence, although extremely small, was the beginning of the 1920s, poorly funded, ill-trained, headed by politicized management, and ruled by relations characteristic for community and not institution-type groups, that is – somewhat vulgarizing the issue – by an informal network of good-old-boys system (called by W.T. Drymmer *sitwa*) That obviously affected the quality of the staff selection. The DII's operational activities clearly show the impact of these factors. W. Michniewicz's report was compromised not only by the indication of its inadequacy, but at the same time it was presented as a possible intrigue of officers who were supporters of Józef Piłsudski.⁹⁵ In turn, the selection of officers sent to the eastern facility was excellent illustration of the thesis of the absence of any objective procedures

⁹² CAW, Oddział II, sygn. I.303.4.1781, a report in Russian language, without any references.

⁹³ W.T. Drymmer, *W służbie Polsce...*, pp. 124–125.

⁹⁴ A. Krzak, „Czerwoni Ażefowie”. *Afera „MOCR-TRUST” 1922–1927*, Warszawa 2010, p. 157.

⁹⁵ W. Michniewicz, *Wielki bluff sowiecki...*, p. 132.

used for the selection of candidates for such positions. DII appointed as liaisons with the Trust in Moscow very young people, who were sent there without any professional experience, some of which (like Capt A. Niedziński) were characterized by intellect and personality traits disqualifying them as intelligence officers. The only criterion of the selection was the favor of decision-makers, who appointed candidates for the posts. W. Michniewicz was chosen to a post in Moscow, because he knew (and probably was a friend) Capt W.T. Drymmer, who also sent there his another colleague from the Polish legions (E. Czyżewski) as W. Michniewicz's deputy.⁹⁶ In turn, his successors as liaisons with MOCR-Trust owed their posts to the personal decisions of Capt M. Talikowski, however, according to the documents, (...) *they were subject to his requests to take the posts*⁹⁷. It follows that at least in relation to this operation carried out by the DII, no objective procedures were applied in Polish intelligence that could select a suitable candidate for any substantive position, apart from personal acquaintances. In the same way, the military attaché deputy in Reval was Capt W.T. Drymmer, although he had just left the army declaring hatred towards relations prevailing there and had no idea about the intelligence work.

As it has already been mentioned – to carry out the interrogation of E. Opperput in 1927, L. Bociński was appointed, although he did not know a word in Russian.⁹⁸ It seems that personnel decisions were not only based on full voluntarism of decision-makers, but in addition, apart from the most obvious requirements of the role. No one could expect that Lt. Col. L. Bociński would be able to conduct the interrogation of the Russian agent without at least some language skills⁹⁹ and having no idea about the situation in the USSR. It demonstrates the real decision-making mechanisms in Division II of the Polish Armed Forces and lack of good management and motivation of personnel promotions and openness of career paths for talented and hard-working officers.

From the analysis of the archive material on the Trust operation, a picture emerges of the Polish intelligence governed by informal relationships that could even outweigh the elementary common sense, as it was during appointing A. Niedziński to the post of the Head of Department "East", despite the fact that he was well known to the Russians for years having led him by the nose and having him under pressure due to the arrest of his mistress in Moscow. Voluntarism, described by W.T. Drymmera *sitwa*, unclear promotion criteria, which after all in a situation of low pay officers was the only way to stabilize their financial situation and ignoring the objective requirements assigned to management roles not only disrupted the functioning of the Polish intelligence, but also significantly facilitated the Soviet penetration, generating interpersonal tension among officers chosen for rapid career paths (eg. Drymmer W.) and the rest, which in the course of their service was overlooked

⁹⁶ W.T. Drymmer, *W służbie Polsce...*, p. 107.

⁹⁷ CAW, Oddział II, sygn. I. 303.4.1781, T. Werner's letter to W.T. Drymmer, l.dz. 08/24 from 24th January 1924.

⁹⁸ Of course, it should be noted that the hering was conducted by Łaniewski.

⁹⁹ Although he could communicate with the Finnish officers, who spoke German.

in promotions not only in posts, but also in ranks.¹⁰⁰ It had to affect the officers' attitudes towards the service and the superiors and to have a negative impact on recruitment, because young officers realized that the regular army units offered a better chance of being noticed by and promoted than the ruled with unclear principles information service.

So called Bociański's committee is a good example of lacking good management and civil courage. In 1927, the committee did not – although in the face of such a large degree of possible Soviet infiltration it was absolutely necessary – carry out personnel purges in DII. Despite the statements of people in charge of the Division II suggesting that they were aware of the seriousness of the situation after the Trust affair, they did not exchange the personnel involved in the operation, to stop described by A. Niedzińskiego “engagement” of the Polish intelligence into Soviet counter-intelligence. The structure of the DII, its staff, activity forms and methods of operational work, cover institutions and prevailing mentality had been thoroughly researched by the GPU in years before 1927. Doing nothing, to change this situation, only facilitated the further penetration, offering to Polish officers self-limitation of their activity.

Possible motivations of the officers responsible for those decisions were the result of their emotions and beliefs, probably understandable and noble¹⁰¹, but at the same time they were extremely harmful and – given the seriousness of the threat – really petty. Indeed, if Bociański's committee had decided to carry out the purge and accepted its possible consequences in the form of a probable compromise of Division II, it could at least partially save the Polish intelligence on the USSR¹⁰² but it would ultimately destroy their own careers.

End

Summing up, one has once again to emphasize that the above described causes were complex and worked synergistically to enhance each other. Group-thinking, stemming from personal interests participating lie along with its consequences in terms commissioning processes of cognitive dissonance-reduction were both the result and the cause of the system errors occurring in the Polish intelligence. It must be stressed at this point that the internal causes, briefly outlined above, only facilitated external factors. Because DII was the object of constant interest of Soviet Russia, a situation when the military intelligence became a victim of the psycho-social processes that effectively hampered its functioning, facilitating the aggressive action of the Soviets was an unacceptable mistake. Internal factors were like the weakness of the body, which then usually falls victim to the disease, although in normal conditions it can defend itself.

¹⁰⁰ A. Wszendyrówny, *System doboru kadr do Oddziału II Sztabu Głównego Wojska Polskiego w latach 1929–1939*, „Rocznik Archiwalno-Historyczny Centralnego Archiwum Wojskowego” 2009, No 2, p. 129.

¹⁰¹ Naturally, it should be emphasized that decision was influenced by many other factors.

¹⁰² Though it should be noted that receiving any intelligence documents from the USSR quickly became impossible due to extremely difficult conditions of spy-work.

Since 1925 Polish strategic thought was founded on the assumption that a war on two fronts was inevitable, and the only remedy was to have the efficient intelligence and the army based upon maneuvering possibilities combined with high firepower.¹⁰³ But most of the decisions made by the Polish government and the army acted contrary to those, how legitimate, assumptions: the army was technologically retarded, and therefore less mobile, the Soviet invasion on 17 September 1939 was a total surprise, because the government had been convinced that the Soviet Union at worst be neutral, and DII – which was to be the key to efficient army and policy – mired in the problems described above, which effectively blocked its intelligence abilities in the USSR. As Stanislaw Mackiewicz put it, years after the first world war was a time of preparation for the next, inevitable war. Unfortunately, as so often in the history of Poland, this we were unable to use well.

Abstract

The article elaborates upon causes staying behind the involvement of the Division II of the Polish Army in the cooperation with the so called MOCR-Trust, i.e. a provocative organization established and managed by the Soviet counterintelligence. The author puts forward the hypothesis that there was no one reason for the above-mentioned intelligence failure, but a conglomerate of synergistically acting causes. The author divides these causes into two groups: external ones to the Division II, to which he includes political conditions and activities of Soviet spy-rings in the Polish Army and internal ones, which he groups into psycho-social causes resulting from cognitive processes and human interactions and structural causes, related to the functioning of the Division II as an hierarchical organization. Describing and explaining the second group of causes, the author reaches for explanations to the achievements of social and organization psychology, combined with a thorough historical research.

Keywords: Division II SG of the Polish Army, disinformation operation, Trust, OGPU, social and cognitive psychology, organization psychology, history of special services, disinformation theory.

¹⁰³ P. Stawecki, *Polityka wojskowa Polski 1921–1926*, Warszawa 1981, pp. 82–93.

VI
REVIEWS

Krzysztof Izak

Charles Townshend, *Terrorism*¹

In 2017 the University of Lodz Publishing House started to publish „*Krótkie Wprowadzenie*” (*A Short Introduction*) series of “books that change the way of thinking”, as the editor notifies on the cover. These are small textbooks (21x13 dm) of hundred and tens to ca. two hundred pages of text. They concern different fields of expertise and their authors are Oxford scientists who bring readers into a world of knowledge and different scientific disciplines in a way that is easily accessible. In the United Kingdom *A Very Short Introduction* (VSI) series being issued from 1995 by the Oxford University Press has more than 500 titles now, which have been very successful worldwide. Until now, they have been translated into 25 languages. Now it is time for a Polish translation, although in the second half of the 1990s and in 2000 Prószyński i S-ka Publishing House decided to edit the VSI. Several books of the series, as far as I remember, got printed, dedicated to religious studies and other chosen fields of humane sciences.

Care for the merits of the present Polish edition of the series provide scientist from the University of Lodz. I recommend particularly volume five written by a British historian, Charles Townshend, *Terrorism*. Professor Townshend is a British historian with particular expertise on the historic and political consequences of British imperialism in Ireland and the Middle East, so on the territories where British presence was accompanied by huge activity of organizations using terrorism as a method of political activity. These organizations stayed active even after the British had left the region. Professor Ryszard M. Machnikowski, a well known political scientist at the University of Lodz with expertise on terrorism, current military conflicts and international security, has translated the book into Polish. This 201-page long book was accompanied by the professor’s introduction *Current faces of terrorism*. Before I go to the description of the content of this valuable book, it is worth quoting translator’s comment: *Townshend punctures in the pages of his book several unnecessary – but still present in people’s minds, not only laymen – myths on terrorism. It should sadly be admitted that they are quite often spread by numerous commentators sitting long hours in TV studios. His work allows to look closer to the phenomenon, get to know it inside out despite the fact that the first edition appeared in bookstores already in 2002 and reader of the Polish version got second completed and corrected edition issued in 2011, so more than five years ago* (pp. 9–10).

The book consists of seven chapters on various topics linked to terrorism and each of them starts with a motto or a maxim by famous people known from history or still living.

¹ Łódź 2017, University of Lodz Publishing House, p. 202.

In chapter 1, *Problem with terrorism*, the author raises such issues as: disputes about terrorism definition, terrorism and war, process of terror origins and development of the phenomenon, strategies of terror, terror and politics, terror and women. He notices that terror is a separate form of political activity to undermine the state ability to ensure security to its citizens, and this causes the need to justify such activities. There is more than 200 definitions of terrorism. In the 1980s two researchers, Alex Schmid and Albert Jongman, compared more than 100 existing back then definitions of terrorism with respect to the presence of key words.² The most common words were: force and violence (more than 83%), political nature (65%), fear (51%). What is interesting, in ca. 5% of definitions there were such words as unpredictability or incalculability which are common in definitions formulated in the last two decades. Confusion about the terrorism term is present in media and in scientific literature. It applies to both definitions and language. What is terrorism for some, for others it means struggle for national independence. Israeli and Palestinian conflict is a good example here. Arab world, or even more – Muslim world, perceives Palestinian organizations not like terrorists but as fighters for freedom.

Terrorism is a political not psychological phenomenon. Words like terrorism, terrorists unequivocally have negative connotations, while those who use it question legitimacy of such understanding. They call themselves warriors, fighters, partisans and guerillas. The last word also causes chaos because guerilla fights run on military logic. Guerillas engage military forces of a country, no matter the scale of their activities is. Their goal are mainly military forces of the adversary. So, it is war which defines guerilla activities. At this moment, it is worth citing Henry Kissinger, the former US Secretary of State 1973–1977, who said *guerillas win when they do not lose, regular army loses when it does not win*. The sentence reflects best the difference between guerillas and regular army of its own country or some other country, which guerillas have conflict with.

The nature of terrorism is negation of fight understood in military terms. Its goal are non-fighting people, vulnerable, civilians. In case of terrorism we deal with fight carried out by the weak who use violence, because of their weakness they cannot take up an open fight. The fight can escalate and then such kind of fight we call asymmetric war, waged by parties with uneven forces. This asymmetric factor is something that makes terrorism different from symmetric wars, i.e. clashes of more or less even forces. Term of asymmetric wars, which was to assist in defining terrorism and clear any doubts, caused even more confusion. It is often abused because not every asymmetric conflict is the same as terrorism. Townshend totally omitted in his works the concept of asymmetric war. There was also no comparison between terrorism and south American guerilla, which was the name for guerilla troops fighting with authoritarian regimes, not for terrorist organizations.

² A.P. Schmid, A. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concept, Data Bases, Theories and Literature*, New Brunswick 1988, pp. 5–6.

Introducing readers into a strategy of terrorism, the author describes the phenomenon from a historical perspective, although it avoids any chronology and clouds the whole picture. One cannot also agree with the author, who, referring to the logic of terrorism, says that *for the first time it was presented so clearly in the „Philosophy of a bomb” by Jonathan Most* (the correct name should be Johann not Jonathan), *an anarchist treatise of 1880* (p. 33). It was Mikhail Bakunin, regarded as the author of anarchism idea, followed by a German apologist named Most, who had created the idea of violence. He was the author of such slogans as *the pleasure of destruction is a creative feeling* and *the basis for anarchists’ activities is the realization of revolutionary ideology in a non-revolutionary situation*. His compatriot and colleague Sergey Netchayev was the author of the famous Catechism of revolutionary, ideological treatise constituting a basis for revolutionary activity, which is described at present as anarchist terrorism. Peter Kropotkin, the third of Russian anarchism ideologists, claimed, inter alia, that *moderation is not good for violence*.

One cannot forget other German terrorism precursors and theoreticians of the 19th century. One of them, Wilhelm Weitling, described terrorism as a combination of revolutionary awareness and criminal abilities, briefly said terrorist equals revolutionary plus criminal.³ On the other hand, Karl Heine, in his terrorism doctrine justified the need of mass killings for a good cause.⁴

In the second chapter – *Crusaders and conspirators* – Townshend touches some very interesting issues, one may think very far away from each other. He tries to distinguish „good terrorists” from bad ones. The term *good terrorist* refers to revolutionary terrorists from the 19th century fighting against oppressive states. In case of fighters for freedom the author tries to give some features distinguishing them from terrorists. The most important thing is that they carry out terrorist attacks extremely rarely to gain political aims. From the historical point of view none of the organizations appealing only to terror did not succeed in liberation. Terrorism as such is a negative phenomenon and its use causes very often unexpectedly catastrophic consequences for terrorists. A good example are activities of the so called good terrorists in the 1970s, who belonged to Movimiento de Liberación Nacional-Tupamaros, MLN-T, which caused the end of liberal Uruguay. In spite of some unpredictable events in many cases the thesis that violence liberates from the inferiority complex, despair and impotence, makes fearless and restores self-esteem, by Frantz Fanon (1925–1961), a participant of the Algerian War, during which both sides used terror against the opponent and against the so called traitors, who had been avoiding the fight, who were against any violence or who had been supporting the opponent, seems to be accurate.

³ There is another definition formulated by an Indian Muslim theologian, philosopher and poet Muhammad Iqbal (1877–1938) which is associated with this definition, for whom bolshevism plus God is almost Islam.

⁴ Those who are interested in anarchist terrorism are recommended to see: A. Pawłowski, *Terroryzm w Europie XIX i XX wieku*, Zielona Góra 1980; W. Potkański, *Terroryzm na usługach ugrupowań lewicowych i anarchistycznych w Królestwie Polskim do 1914 roku*, Warszawa 2014.

Moving on to the description of international terrorism, the author gives no definition of the phenomenon, nevertheless, he writes that it has appeared with Carlos' career (p. 49). But capture under the photograph on p. 46 informs: *idea of international terrorism was born together with Chicago Haymarket attack of 4 May 1886, when the police started to scatter anarchists' gathering (many of whom had been former immigrants from Germany) and was attacked with a bomb.* Definitely participation of German immigrants in the event cannot lead to its description as international terrorism, to which Ilich Ramirez Sanchez, alias Carlos, known as Carlos the Jackal, brought a new dimension. Many authors acknowledge hijacking of the El Al Israeli aircraft from Rome to Tel Aviv by members of the Popular Front for the Liberation of Palestine on 23 July 1968 as the beginning of international terrorism. The aircraft was hijacked to Aliers. It is worth citing definition of international terrorism formulated in 1986 by the UN Commission of International Law. International terrorism is (...) *taking up, supporting and enhancing by the state authorities to terrorist acts in other countries, or tolerating by the authorities any activities to carry out terrorist attacks in other country.* During the Cold War era terrorist organizations were supported by different countries, including the USSR and the US. It seems though, that currently division between domestic terrorism and international terrorism makes no sense because of network of relationships, excluding maybe the US where different groups with no important international ties are active.

Trying to answer the question *Whether terrorism can be even worse in the future?* the author is of the opinion that such risk is probable to grow with technology capabilities of terrorists. In the past they have already used chemical weapon and are able to get components to it in the future. Nevertheless, super terrorism in the form of weapon of mass destruction, especially nuclear one, which strikes fear among the public is more like journalist fantasy, not a real threat. Nevertheless, its usage by some countries seems possible.

In chapter three – *Rules of terror* – the author introduces a very interesting topic of spreading fear in France during the French Revolution. In 1793 Jacobins instituted the reign of terror to defend revolution against aristocracy and royalists, although the most victims were ordinary people. The uprising in Vandee was suppressed bloodily and became for Jacobins a symbol of counter revolution and extermination of civilians is a good example of it. Not so long further the French Revolution devoured its own children. The members of the National Convention Maximilien Robespierre, Louis Saint-Just and Georges Danton were guillotined. Cruelty and violence on a mass scale during the French Revolution created a model of terror for those who wanted to keep the old order (so called white terror) and for those who wanted to overthrow it. This way red terror (for example of Bolsheviks) and black terror (nationalist, for ex. Hitlerian). So, the terms terror and terrorism should be divided. Terror means using violence by stronger state organs against weaker citizens and terrorism means the other way round – using violence by weaker citizens against stronger state organs.

Townshend identifies *terrorism of a free coverage* which shall include activities of Latin American death squadrons, supporting counterterrorist activities of the state. There goes next ultra terrorism, which happens (...) *in a situation when formerly significant group feels like abandoned and betrayed by a country. This sense of betrayal appears when local people face negotiations between insurgents and a state, what happened in French Algeria in the fall campaign carried out by the FNL (Front de Liberation Nationale), and, to a much lesser extent, in the North Ireland during „the peace process”* (p. 72). By the end of the struggles with the Algerian FLN quite active was *l'Organisation Armee Secrete, OAS. It was created in March 1961 and it was against Algeria's independence. Local people became its target. Using scorched-earth tactics it wanted to cause a mutiny of French settlers there, which it failed, in the end. It moved terrorist activities to France organizing few unsuccessful attacks on President Charles de Gaulle. In case of Northern Ireland loyal organizations as Ulster Volunteer Force, UVF have not attacked representatives of the British government or British targets but concentrated on Irish-republican (catholic) targets. Their activity was called volunteer terrorism. If Townshend had written his book after 2011, he would have called many groups which were established during the Arab spring this way.*

Chapter 4 – *Revolutionary terrorism* – has been divided into four subchapters. The first two are: *Two centuries of terrorism: century I* and *Two centuries of terrorism: century II*. They present a phenomenon of terrorism from a historical perspective, starting from Russian anarchists called terrorists-revolutionaries. They embraced, for example, members of National Will organization, called nationals (rus. Narodniki) who wanted to provoke an outbreak of revolution to preserve existing order and build a stateless society country on it. Anarchists called their activities „propaganda via actions”. There is also a Polish mark here. *Polish socialist, Józef Piłsudski used to call such activities „armed acts”, syndicalists used a name of „direct action” or reprise individuelle* (fr.) – individual retaliation.⁵ As targets for attacks revolutionary terrorists chose heads of state and top officials. In the period of 1881–1914 there were seven effective terrorist attacks carried out on rulers (including the tsar of Russia, presidents of the US and France, king of Italy and Austro-Hungarian heir to the throne). While describing revolutionary terrorism one can add two Polish accents – one is a killer of tsar Alexander II, who was a Polish student from Podlasie region, Ignacy Hryniewiecki. He died from wounds caused by explosion of a bomb tossed on March 13, 1881 directly at the emperor's feet. Hryniewiecki's decapitated head was put into a jar filled with spirit and exhibited in the hall of the Petersburg police station as a warning. The second Polish accent is connected to Bronisław Piłsudski, Józef's elder brother, who took part in an unsuccessful conspiracy to murder tsar Alexander III in 1887. For that action he was sent to Sakhalin, where he was doing

⁵ Since 1904 Piłsudski was heading the Combat Organization, a fraction of the Polish Socialist Party, which had been carrying out attacks on Russian targets in the Kingdom of Poland area. More details in *Polscy terroryści* by Wojciech Lada, Kraków 2014.

research into Ainu people, indigenous people of the southern part of the island and next ethnographic research into other peoples of Japan⁶.

In the author's opinion revolutionary terrorism is responsible for rebirth of political violence after World War II when anti colonial liberation movement was under way. Terrorism was a significant element of it. The example organizations are Vietmin and Vietcong responsible for death of more than 20 000 people. A vital role in a revolutionary terrorism played *Latin American factor* (title of the next chapter). A consistent place took Ernesto Che Guevara, Abraham Guillen, who wrote *The strategy of urban guerillas* (1966), Regis Debray, author of *The Revolution in Revolution* (1967) and Carlos Marighella, author of *the Mini manual of urban guerilla* (1969). In case of the Latin America the source of revolutionary terrorism were mass social movements carrying out guerilla operations. These operations were moved to cities creating the urban guerilla. The best known guerilla organization was active in the most democratic country in Latin America – Uruguay. It was, mentioned already, the Tupamaros movement. Finally, its activity led to a less liberal and just country, what made its members to go underground and finance its activities from bank robberies.

Tupamaros guerillas were looked up to for West Germany youth. Reasons for this particular interest should be looked for in conditions, Uruguay fighters struggled in. Successes of the guerillas in the second half of the 1960s were also not meaningless. That was the time when non-parliamentary youth opposition in the Federal Republic of Germany was very active. Tupamaro victories appeared to be only interim and in the final result they turned against not only the organization itself but also against the Uruguayan democracy. Nevertheless, the Latin American guerilla was an inspiration for many extreme left terrorist organizations in Europe. There is more on these organizations in the last sub-chapter – *Terrorism of fractions*. One can find short descriptions of Italian Brigade Rosse, BR, there and German organization Baader-Meinhof, i.e. Rote Armee Fraction, RAF. Finally, leftist terrorists in Europe were defeated by state institutions.

Another motivation for some terrorist groups is a national and separatist ideology. This is what chapter 5 – *Nationalism and terror* – is about. Nationalist movements were much more immune to counterterrorist operations and their own destruction. The author gives examples of the Sri Lankan Liberation Tigers of Tamil Elam, LTTE and Armenian nationalist organizations, being heirs to the Dashnak movement of the 19th century.⁷ Separated subchapters are devoted to the Irish Republican Army,

⁶ In October 2013 a monument by B. Piłsudski in Shiraoui on the isle of Hokkaido was opened. In Yokohama lives grandson Kuzuyasu Kimura.

⁷ The name comes from the name of a Dashnaksutyun town. An armed group of members of the Armenian Revolutionary Federation occupied the Ottoman Bank on August 26, 1896. The purpose of the raid was to dictate the ARF's demands of reform in the Armenian populated areas of the Ottoman Empire and to attract European attention to their cause and, last but not least, to restore peace in the country and "cutting criminal human indifference". Otherwise, they threatened to blow up the building of the bank together with its personnel and its financial assets. Other Dashnak operations were two unsuccessful attempts on the life of the Sultan Abdulhamid II.

IRA, basque Euskadi ta Askatasuna, ETA and Zionism as the ideology and policy of terror, which drew the Jews to their own sovereign Israel country. Both IRA and ETA, using the experiences of anti-colonial and Latin movements, appreciated the role of media. They realized that without TV and radio broadcast and press coverage they were not able to achieve projected goals. If they were active nowadays, they would use undoubtedly social media for their goals. Cyberspace would be the main area of contacts with public.

In the 1970s and 1980s in many regions of Europe there have separatist terrorist organizations been established. Their goal was to get autonomy for a particular region or splitting it off from the country. All those groups referred to leftist ideologies and stressed their reluctance to the West, particularly to the US. Terrorist activities of the then many terrorist groups was a result of sui generis political vogue for imitation of violence by already existing separatist organizations, which activities were limited to one or several series of attacks. They embraced groups active in Alto Adige Region in Italy, in Brittany, in Corsica, in the Canary Islands, in the Molucca Islands or in the Swiss Jurassic Highland.

Comparing activities of terrorist groups motivated by different ideologies it turns out that terrorism used by organizations of nationalist nature can in some cases succeed. For it makes the sides of the conflict to conclude political agreement. The activity of Israeli Irgun Cwai Leumi, Ecel in the 1940s made British to retreat from Palestine. It was the same with Cypriots from Ethniki Organosis Kiprijon Agoniston, EOKA, the French were made by the FLN to leave Algeria, the UK and IRA signed in 1998 the Good Friday Peace Agreement which resulted in expressing by IRA regret for civilian victims of its activities and the process of its arsenal reduction started. The period of peace came, however, it did not last long. After the Agreement was written, there has a new IRA fraction been established, the Real IRA, RIRA. In March 2009 RIRA conducted an attack on a British military base in Massereene, Antrim County (24 km north of Belfast). Two soldiers were killed back then and several were wounded. Later on, there were next attempts of attacks. It turned out that terrorist campaign which had been started long before, was very difficult to stop.

Fighting for religion and faith is the obligation of the community, there is no other obligation, apart from the faith itself, more important than the fight against the enemy that destroys our way of life and our religion. These words come from *Kitab al-Iman* by Taki ad Din ibn Tajmijja (1263–1328) and are the motto of the sixth chapter of the book – *Religious terror*. Townsend claims that the last decade of the 20th century caused a change in perceiving religion motivated terrorism. Activity of Islamic fundamental organizations using violence has been noticed then. For them terrorism is a way of struggle to implement requested social changes and introducing Allah rule over the world, i.e. global hegemony of Islam. Muslim radicals use violence against infidels and those of their faith who do not share the one and only right beliefs. Those are treated as traitors.

Violence has accompanied religion since ancient times, although back then foreign peoples' raids or hostile civilizations' raids were not motivated by religion. Temples

were destroyed, statues of gods were destroyed or taken away as spoils of war. Pagan religions were able to incorporate into their pantheons gods of the conquered peoples. It is only monotheist religions that abandoned this tradition, fighting fiercely paganism and idolatry. Changes in the attitude of people of different religions to violence over the years were presented in a book by K. Armstrong *Fields of blood*, reading of which I strongly recommend.⁸ On page 126 Townshend cites Bruce Hoffman's opinion, who (...) *pointed out that none of the eleven well known terrorist groups active in 1968 cannot be qualified as „religious”*. According to him (...) *first modern groups of such character appeared in around 1980*. One cannot, however, agree with this opinion because in 1968 in the US there was established Jewish Defense League (JDL) by rabbi Meir David Kahane, organization combining Jewish orthodoxy and racist beliefs on Jewish superiority over other nations. Rabbi Kahane perceived himself as a religious guide of the Jewish nation showing the best path to salvation. Strict subordination to divine rights was exactly the best way to salvation. From the moment of its establishment until 1976, JDL had carried out attacks in the US (including on Polish consulate in New York), in which seven people were dead and 22 were wounded. Jewish „purity of race” was one of the main points in the rabbi's program and his supporters. Their group was called „Kach”, which means „only this way” in Hebrew. This description refers to realization of the rabbi's idea of how to deal with Palestinians to clean the Land of Israel (Erec Izrael) of non-Jewish inhabitants.⁹ It should be added that after the Six-Day War in 1967, when Israel seized east Jerusalem, in Israel started to assert different extreme religious organizations coming from Haredi Judaism movement.

In the 1960s in India there was established the most radical and fundamental organization of the Hindu religion believers, Shiv Sena, which appreciated using violence. At that time, the religious and nationalist concept of Hindutva developed and it was very popular in the 1980s. Since the 1920s there has been popular a very active Sikh organization Shiromani Akali Dal, SAD, in India, which regarded Islam and Hindu religions believers as enemies. That is the reason why it is very hard to agree with the opinion that in 1968 there was no terrorist organizations of religious nature at all. At that time in underground there was active al Ikhwan al-Muslimin (the Muslim Brotherhood) in Egypt, whose members found shelter in Saudi Arabia. It is most probable that the Polish issue contains wrongly formulated sentence that *The longest chapter – Inside Terrorism – in the work of Bruce Hoffman's Rand Corporation, the head of the study group on terrorism is dedicated to religion* (p. 126). Rand Corporation is an American neoconservative think tank, to which Hoffman is linked, *Inside Terrorism* is the title of his book, *Religion and Terrorism* is its longest, 50-page long chapter.¹⁰

⁸ K. Armstrong, *Rola krwi. Religia i przemoc*, Warszawa 2017.

⁹ A. Krawczyk, *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej polowie XX wieku*, Toruń 2007, pp. 154-203.

¹⁰ B. Hoffman, *Inside Terrorism*, Columbia University Press 2006. *Correct sentence could sound:*

A very similar title – *Religion and violence* – has one of the subchapters of chapter six. Townshend seems to argue with Hoffman and other authors, for whom religious terrorism is totally transcendental not of political nature. Indeed, it is very hard to agree with the thesis because terrorist organizations motivated by religion have in reality political aims. Referring to the ancient history (Zealots) or to the Middle Ages (Assassins) has also got not much sense because religious organizations of that time had also political aims (fighting in Roman rules in Palestine in case of Zealots, the Seljuq Sultanate and Crusaders in case of Assassins).

In the next subchapters the author briefly describes implications of religion in politics, touches on Messianism, Millenarism, suicidal terrorism and fundamentalism. It is a pity that in the part devoted to the last phenomenon concentrating exclusively on Islamic fundamentalism giving only a few words to fundamentalism in Judaism and mentioning briefly the Aun Shinrikyo movement.

Fundamentalism, as already been said, is present in all monotheistic religions as well as in Hinduism and Buddhism. The term was formed in the US in the 19th and early 20th centuries. It meant radical protestant movements going beyond the general stream of Protestantism with its ideology. Dwight L. Moody (1837–1899) was regarded as the forefather of American fundamentalism and the founder of the Moody Bible Institute of Chicago (1886), which aim was to get cadres ready to fight for the faith. The most important goal Moody had set was to save people's souls. This is why he was ready to cooperate with each and every Christian. He was also taking care of social reforms. Graduates of his institute were to be missionaries of the poor. He claimed that atheistic ideologies would lead to the world's destruction. In his opinion situation worldwide was worsening day by day, that is why people should turn to God. In 1910 Presbyterians¹¹ from Princeton formulated the concept of infallibility of the Holy Bible¹² and announced a list of five basic dogmas: 1) infallibility of the Holy Bible, 2) Jesus's birth of the Virgin, 3) absolute reality of his miracles, 4) atoning by the Christ for people's sins on the cross, 5) physical resurrection of the Christ. In the years of 1910–1915 brothers Lyman and Militin Stewart, oil millionaires from California, financed a series of 12 booklets under the common title *The Fundamentals. The Testimony of the Truth* consisting of 90 articles. Their authors, leading conservative Protestant theologians, explained the rules of the faith in an easily accessible way. The 12 booklets were published in 3 million pieces each and were sent free of charge to vicars, preachers, heads of Sunday schools, professors and students of theology in the US.

The longest chapter „Religion and Terrorism” in a known paper „Inside Terrorism” by Bruce Hoffman, the head of the study group on terrorism in Rand Corporation is dedicated to religion.

¹¹ Presbyterians next to Quakers, Methodists, Baptists and others are included into a group of dissenters beliefs, which means branch of Protestantism which does not belong to Anglican Church.

¹² The *sola Scriptura* rule (“only the Book”) says that the Holy Bible is the first and final Book, solely sure and infallible. To this rule the so called Biblical Quranism is linked which rejects any dogmas and views not justified by the Bible authority.

The project was symbolic because it was recognized as the official beginning of a fundamental movement worldwide.¹³

In the last chapter of the book the author presents possible reactions of a country to a terrorist threat, citing a Walter Laqueur's question¹⁴ he had asked: *whether a democratic society is able to nip terrorist violence without sacrificing values key for its system?* (p. 147). He answers that the victim of terrorists becomes not only democracy itself, which structures had not been changed, but its liberal values. Factors influencing the weakness of democracy in view of terrorist threats are freedom of movement, freedom of association, multitude of targets for a potential terrorist attack limits coming from accepted legal systems protecting human rights, high value of human life and free media. At this point it is worth citing the words of terrorists from 2015: *Your human rights are our weapon, and we love death as you love life*. Western societies agreed to limit their civil freedoms in the name of sense of security. Nevertheless, together with development of powers of state institutions' responsible for security, the situation has not improved. Since September 11, 2004 the world has not become more secure, on the contrary – it has become more endangered by terrorism.

Townshend claims that the most appropriate reaction on “pure terrorism”, i.e. a method used in a conflict and not one of the war tactics, is to ignore it, because risk of death following terrorist attack is much smaller than in a car accident. The best public answer to terrorism should not be showing fear. Unfortunately, reactions of states are quite often inadequate to the threat. The best example of the global war with terrorism announced by the US in 2001 was its attack together with three of its allies on Iraq on March 20, 2003, which caused in consequence death of thousands of people and creation of a new demon in a form of the Islamic State. Also disproportionate to a threat was the US attack on Afghanistan, which has triggered anti-Western psychosis in Muslim world instead of Al Qaida destruction. The current presence of NATO forces in Afghanistan has not brought stabilization in the country and Talibs still control its vast territory. This is a reason why response to terrorist threats should be proportionate to their scale. Probably the worst reaction to terrorism is imitation of terrorists. Such methods are used for many years by special services of Israel, which try to eliminate the most dangerous terrorists in covert operations and army destroys housing compounds belonging to families of assassins. According to Benjamin Netanyahu, the Prime Minister of Israel, retaliation not only prevents terrorism but also it is able to defeat it. It also happens that it is the state authorities who manipulate the fear caused by real or imaginary terrorist threat, example of which was the American politics between the 9/11 attacks and military incursion into Iraq on 2003. Acting back then *Patriot Act* had a broad public support according to a thesis by Ronald Creslinsten: *The majority of people will sacrifice its freedom in exchange for security if it is scared enough*

¹³ K. Armstrong, *W imię Boga. Fundamentalizm w judaizmie, chrześcijaństwie i islamie*. Warszawa 2005, p. 249.

¹⁴ American historian and publicist, author of books related *inter alia* to terrorism issue and author of *Ostatnie dni Europy. Epitafium dla Starego Kontynentu*, Wrocław 2008.

(p. 177). Townshend points out differences between *antiterrorism* and *counterterrorism*. Antiterrorism is associated with application of defensive measures to recognize terrorist threats and to prevent them, so it regards all preventive undertakings. Counterterrorism embraces the whole sphere of offensive terrorism countering, and hence to engage military forces and security forces to liquidate terrorist organizations and eliminate their individual members. In reality both terms are currently interchangeable and some authors use the term anti/counter/terrorism. Every country threatened by terrorism has its own strategy of combating it. Special forces are inter alia serve this purpose. The European Union strategy is based on preventing (for example deradicalization, cutting off financial means and logistic support), securing (people, property and infrastructure), prosecuting (investigations and law suits) and reaction (neutralizing and minimizing results of terrorist attacks), regarding human rights.

Antiterrorist operations carried out by states should be better calculated and more precise than terrorist actions. Principle rules of fighting with terrorism should be an anticipation strategy, in other words preventive activity to strike at terrorist cells before they carry out an attack, and strategy of proportionate retaliation after terrorist attack, which was not able to prevent, was carried out. To implement effectively the anticipation strategy appropriate measures operational sources are crucial. Both strategies are perfectly implemented by Israeli special services.

The author touched also some sensitive international matters, which did not allow to define the term *act of terrorism* for a long time. In the end the differences have been overcome but avoiding the term *terrorism* to omit controversial problem of political motivation. Neutral terminology used in a convention largely failed in its purpose, since it is very hard to establish what an act of terrorism is, without taking into account ideology, ethnic lines or religion of their perpetrators or supporters. Furthermore, state sponsoring of terrorists can be added as well, what is a subject to firm critique of the US, which counted Iraq, Iran and North Korea to a group of “rogue countries” after the 9/11. It was also Sudan, Syria and Libya which were listed as countries supporting financially terrorism. During the Cold War the USSR was accused of sponsoring, supporting and even training of terrorists.

Additional advantage of the book by Charles Townshend are photographs and lists of literature linked to individual key words, separately to each chapter and also annex bibliography of chosen topics related to terrorism. There is a combined index of names, organizations, geographic names and the most important key words in the end. It is worth stressing communicative style and narration of the work which make reading it interesting and comprehensible. This book I would particularly recommend to officers at the beginning of their career in countering terrorism departments. Short introduction into a matters they are going to cope with, will certainly be a valuable input into their knowledge. In other words, it is worth devoting one weekend to reading the book, and there is some time left for one’s own reflection on it.

Marek Świerczek

**Konrad Paduszek, *Look into Lenin's brain.
Intelligence of the Second Republic of Poland
and post-revolutionary Russia*¹**

In the night of September 17, 1939 vice minister of the USSR foreign affairs, Vladimir Potomkin passed to the Ambassador of the Second Republic of Poland in Moscow, Waław Grzybowski a note signed by Vyacheslav Molotov, which contained, inter alia, such sentence:

Polish-German war has revealed internal bankruptcy of the Polish state. During ten days of war operations Poland has lost all its industry regions and cultural centers. Warsaw has stopped being the capital of Poland. Polish government has fallen apart and has shown no signs of life. It means that Polish state and its government have, in fact, ceased to exist. In view of this treaties concluded between the USSR and Poland have lost their power.²

Almost at the same time the Red Army troops crossed eastern borders of the Second Republic of Poland and started treacherous aggression, called – along with the Soviet practice of inside-out world – “liberation march”. After 20 years of independence, Poland ceased to exist. Wehrmacht met the Red Army to celebrate war brotherhood over a dead body of the Polish Republic.

However, in a description of this sinister event historians make mistake thinking that the Soviet aggression started from the moment of passing the diplomatic note at 3 a.m. to the not understanding a thing Ambassador Grzybowski. This time mistake is – what a trifle – almost 18 years long. Since vicious sticking a Soviet bayonet through the Polish back was a only a consequence of the process which had started banally – from a visit of a Polish renegade, Wiktor Steckiewicz in Rewel during the first snow period of 1921. It was then the Polish intelligence was caught into unbelievably diverging disinformation play by the Soviet counterintelligence which had been stupefying the HQ of Polish Army until April 1927. It had been giving documents produced in a bulk by forgers working in the interdepartmental Disinformation Office, called humorously *kriwe zwierkało*. That was a time of a complete disintegration of Polish intelligence structure. Polish officers had been meeting Soviet provocateurs instead of agents, instead of secret documents they had been providing materials full of lies or half-truth. What is worse, being constantly under surveillance of the adversary, they were an easy recruitment target. They had been falling into the hands of Soviets, trying to supplement their poor officers' salaries and because of their childish naivety of former cavalymen, sent by the HQ to the USSR almost without any training for

¹ Łomianki 2016, LTW, p. 608.

² *Zmowa. IV rozbiór Polski*, A.L. Szcześniak (ed.), Warszawa 1990, p. 135.

a quick penetration of the highest administration institutions and the Red Army. So that those 20-something spies sent hastily into the bear's mouth were not too self-confident, decision-makers from the Army skimped on a budget and caused the lack of money in the Polish intelligence and officers had to pay even for using cars of the Polish diplomatic post with their own money.

When the Soviets got bored with this masquerade and revealed via the next provocateur that agent nets of the Polish intelligence in the east were *de facto* on the Soviet OGPU payroll, leadership of the Division II, after a time of pretending that nothing wrong had happened, reacted with hysterical exaggeration..., by giving up informants recruitment in the USSR at all. This was the way, as the highest officials of Polish intelligence argued, next traps of Soviet Azefs were to be avoided, and there was a need to focus only on what was real instead of possible documents and forgeries of agents' documents and reports. Only that Russians effectively limited Polish officers moving around the USSR and this way effectively paralyzed Polish intelligence. In a result the Polish Republic was blinded.

In spite of the huge effort of the whole Polish country, which had been giving (depending on methodology) from ca. 23,5% to 42% of the budget to an enormous army consisting of 30 infantry divisions and 10 cavalry divisions, Poland was vulnerable in the East and unable to predict when and how the possible attack would be carried out. Despite the fact that already since 1925 the Office of Strict Council of War had correctly assumed that Polish defense should be based on efficient intelligence, the Polish Republic – at least in the east – had in practice no intelligence at all.

With only a lack of elementary abilities to recognize adversaries' intentions (and their allies) can be explained the involvement of The Polish Republic in a war with Germans in the situation when the Ribbentrop-Molotov agreement had been signed. Polish intelligence was not able to recognize absolutely clear symptoms of the catastrophe coming from the East.

It was already in 1938 when the French ambassador in Moscow, Robert Coulondre got information that the vice minister of foreign affairs of the USSR, Vladimir Potomkin, promoted the idea of the fourth partition of the Republic of Poland as inevitable. Polish intelligence did not raise the topic, nor settlements between chief commands of France and England for April 1939 that the allies would wait for the final result of Polish-German war, quitting the assistance during a border struggle. And then, when German war machine started to crush Poland, Polish intelligence was not able to notice full tactical alert of the Red Army and concentration of the Soviet troops across the whole border line with the Republic of Poland. Even getting rid of wire fences by the Soviets did not raise any concern of neither in Division II of the HQ of Polish Army, nor in the Border Protection Corps (KOP). It all made Polish Army on the eastern provinces of Poland surprised and were sent – almost without any resistance – to prison camps, and finally to execution spots in Katyń.

A doctoral thesis by Konrad Paduszek entitled *Look into Lenin's brain* assists in understanding how did it happen that the above events occurred. Its author shall

meticulously summarize the activities of Polish intelligence in the east during the most important period 1921–1927 from a perspective of the following events. Although the topic has been explored by recognized Polish historians, nevertheless, there was a lack of such detailed paper based on source documents that would give such a precise picture of Division II activities in the east and make it easier to understand how was it possible to paralyze it.

The author describes step by step intelligence nets in the USSR (both in the country as well as outside), refers to officer personnel active on a Soviet line, describes sources of information used by the Polish intelligence in the east, cooperation of the Division II with other intelligence services working against the USSR and finally the results of recognition in the USSR. Each chapter is a sum of current knowledge on the topic and a repetition of the past studies, supplemented by a result of additional and meticulous archive query.

K. Paduszek quotes very liberally archive materials and gives a picture of Polish intelligence in the east, despite the fact that the topic is very extensive. His narrative is very meticulous and based on verified facts. The description is supplemented by tables with results of multiannual detailed queries. Wealth of the presented knowledge demonstrates how hardworking person the author is. He has analyzed thousands of documents and has created a vast evidence-based compendium with clear organizing assumptions. The publication by K. Paduszek allows further analyses and new hypotheses. That is why it is not only a synthesis, but a prolegomena to further studies. We should add that because of its meticulousness and completeness this is a publication that should find its place on a bookshelf of every explorer of intelligence during 20-year of inter-war period. At the same time, in spite of the volume of the book, which equals a volume of a phone book, one can read it with interest in a traditional way but one can also read only chosen chapters and use them in a work.

Although the author, while preparing his work, never exhibited any hard-hitting passion and it was not his goal to change the way Division II officers are remembered, his information are unambiguous in his meaning. They indicate that the Second Republic of Poland did not understand what it had to deal with in the east. Despite the Soviets were demonized in newspapers, in reality many did not realize how powerful their services were and how innovative the waged war was. Decision-makers, who had been sending Polish officers to Moscow or Minsk, had lived in a world of delusions and had not accepted that poorly paid and without any know-how, as far as absolutely unique solutions used by the Soviet services is concerned, Division II had to lose that struggle. Polish officers were able to give instructions to their agents, in which they advised them, in case of being in the USSR, not to hesitate and openly come at ex-comrades from the tsar army because they must kept officer honor and *esprit de corps*. Polish intelligence officers vouched with honor for their Soviet agents, who – in their opinions – had honor and hated Soviets that much that they could not lie. One of the chiefs of Division II ordered his officers in a written form to verify whether a person suspected of being an OGPU informant by... asking openly

that question. Mister colonel seemed to imagine that a person being asked face to face would not have any other option than to say, truth or at least he would get flushed or would start cleaning his glasses nervously, leaving the officer with a sense of insight. Polish officer personnel, being mentally in the 19th century, did not realize that in the “Soviet paradise”, full of mass graves, concentration camps and secret police execution compounds, all human reactions had stopped and people whose families could be murdered at any time, would do anything what the OGPU operator demanded.

Thanks to the work of Konrad Paduszek one can understand how the September defeat was possible and how was possible the subsequent enslaving of the country by Soviet governors with Polish-sounded names. As professor Sławomir Cenckiewicz wrote in a short description of the work: *Józef Pilsudski was supposed to say once that Poland's play with Bolsheviks was about to look into Lenin's brain. Unfortunately, the plan of the Marshall of Poland (...) has not been realized.*

And this is the value of K. Paduszek's work, instead of encomium we got a careful description of pros and cons of the pre-war Polish intelligence. And thanks to it we can draw conclusions. Not only in respect to the past.

O autorach

Jolanta Darczewska – doktor nauk humanistycznych, pracownik Ośrodka Studiów Wschodnich im. Marka Karpia, ekspert w dziedzinie bezpieczeństwa, zarządzania bezpieczeństwem i walki informacyjnej.

Danuta Gibas-Krzak – doktor habilitowana nauk politycznych, bałkanistka. Prowadzi badania dotyczące stosunków międzynarodowych w Europie Wschodniej, polemologii, konfliktów narodowościowo-etnicznych i terroryzmu, pracownik naukowy Akademii im. Jana Długosza w Częstochowie, współpracownik ośrodków badawczych i naukowych w Serbii, Bośni i Hercegowinie oraz Chorwacji.

Sławomir Gładysz – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Marcin Gołaszewski – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Justyna Jastrzębska – studentka V roku psychologii na Wydziale Filozofii Chrześcijańskiej Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, młodszy specjalista z zakresu badań poligraficznych, od 2017 r. członkini Polskiego Towarzystwa Badań Poligraficznych.

Andrzej Krzak – doktor habilitowany, pracownik naukowy Akademii im. Jana Długosza w Częstochowie, historyk wojskowości, ekspert w dziedzinie teorii i sztuki wojennej, sił zbrojnych Europy Wschodniej i Południowo-Wschodniej (Bałkany) oraz służb specjalnych.

Anna Łasińska – doktor, funkcjonariuszka Agencji Bezpieczeństwa Wewnętrznego.

Paulina Markowicz – studentka V roku psychologii na Wydziale Filozofii Chrześcijańskiej Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, młodszy specjalista z zakresu badań poligraficznych, członkini Polskiego Towarzystwa Badań Poligraficznych.

Marek Świerczek – doktor, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

About authors

Jolanta Darczewska – PhD, employee of the Center for Eastern Studies (OSW), expert in the field of security, security management and information warfare.

Danuta Gibas-Krzak – PhD political science, expert on Balkan issues. Doing research into international relations in Eastern Europe, war studies (polemology), ethnic conflicts and terrorism, researcher at Jan Długosz Academy in Częstochowa, associate researcher at research and scientific centers in Serbia, Bosnia and Herzegovina and Croatia.

Sławomir Gładysz – officer of the Internal Security Agency.

Marcin Gołaszewski – officer of the Internal Security Agency.

Krzysztof Izak – former officer of the Internal Security Agency (retired).

Justyna Jastrzębska – fifth year student of psychology at the Faculty of Christian Philosophy, Cardinal Stefan Wyszyński University in Warsaw, junior expert in polygraph examinations, since 2017 member of the Polish Association of Polygraph Examinations.

Andrzej Krzak – PhD, researcher at Jan Długosz Academy in Częstochowa, military historian, expert in theory and art of war, armed forces of Eastern Europe and South-Eastern Europe (Balkans) as well as special services.

Anna Łasińska – PhD, officer of the Internal Security Agency.

Paulina Markowicz – a fifth year student of psychology at the faculty of Christian Philosophy, Cardinal Stefan Wyszyński University in Warsaw, junior expert in polygraph examinations, member of the Polish Association of Polygraph Examinations.

Marek Świerczek – PhD, officer of the Internal Security Agency.

Siódma edycja ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa

Edycja 2016/2017 – wyniki konkursu

Na ogłoszony przez Szefa Agencji Bezpieczeństwa Wewnętrznego konkurs wpłynęły 2 prace doktorskie oraz 41 prac absolwentów studiów I i II stopnia obronionych w roku akademickim 2016/2017.

Komitet konkursowy, po dokonaniu oceny nadesłanych prac, zdecydował przyznać następujące nagrody:

W kategorii prac doktorskich:

miejsc I, II i III – nie przyznano

wyróżnienie – p. dr Arkadiusz Nyzio (Uniwersytet Jagielloński w Krakowie, Wydział Studiów Międzynarodowych i Politycznych), *Transformacja polityki bezpieczeństwa wewnętrznego Polski w latach 1989–1993. Analiza funkcjonalna*.

W kategorii prac magisterskich i licencjackich:

miejsce I – p. Kamil Leśniewski (Uniwersytet Jagielloński w Krakowie, Wydział Prawa i Administracji), *High-tech assassination. Zabójstwa jako przejaw pozainformacyjnych operacji wywiadowczych*,

miejsce II – p. Paweł Wawrzyniak (Wyższa Szkoła Administracji i Biznesu w Gdyni, Wydział Prawa i Administracji), *Cyberprzestępczość i cyberterroryzm jako kluczowe zagrożenia dla bankowości cyfrowej*,

miejsce III – p. Maciej Białek (Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Wydział Prawa i Administracji), *Wojna hybrydowa a bezpieczeństwo Rzeczypospolitej Polskiej*,

wyróżnienia:

- p. Aleksandra Gołaś (Uniwersytet Warszawski, Wydział Nauk Politycznych i Studiów Międzynarodowych), *Specyfika i uwarunkowania procesu radykalizacji muzułmanów w zakładach karnych. Studium przypadków Wielkiej Brytanii*,

- p. Rafał Podolak (Katolicki Uniwersytet Lubelski Jana Pawła II, Wydział Prawa, Prawa Kanonicznego i Administracji), *Dopuszczalny zakres kontroli operacyjnej w systemie praw człowieka*,
- p. Krzysztof Wąsala (Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii), *Karnoprocesowe aspekty ustawy o działaniach antyterrorystycznych*,
- p. Daniel Czebielko (Akademia Sztuki Wojennej, Wydział Bezpieczeństwa Narodowego), *Bezpieczeństwo energetyczne na przykładzie powiatu będzińskiego*.

**Ogólnopolski konkurs Szefa ABW na najlepszą pracę doktorską,
magisterską lub licencjacką dotyczącą bezpieczeństwa państwa
w kontekście zagrożeń
wywiadowczych, terrorystycznych, ekonomicznych.
Edycja VIII – 2018.
Ogłoszenie i warunki konkursu**

Organizatorem konkursu jest Szef Agencji Bezpieczeństwa Wewnętrznego. Celem konkursu jest promowanie i upowszechnianie problematyki bezpieczeństwa wewnętrznego państwa wśród studentów i kadry akademickiej, zwiększenie świadomości społecznej w tym zakresie oraz profilaktyka i edukacja na rzecz bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Tematy konkursu:

1. Rola i zadania służb specjalnych w demokratycznym państwie prawa i w państwach autorytarnych.
2. Konstytucyjne prawa obywateli a uprawnienia służb specjalnych.
3. Służby specjalne – historia, teraźniejszość.
4. Bezpieczeństwo Polski i Europy w XXI wieku – zagrożenia i wyzwania.

Nagrody w konkursie:

miejsce I – nagroda finansowa w wysokości 6000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

miejsce II – nagroda finansowa w wysokości 5000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

miejsce III – nagroda finansowa w wysokości 4000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

wyróżnienie – nagroda rzeczowa oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”.

Warunki:

Do konkursu uczestnicy zgłaszają własną pracę doktorską (I kategoria) napisaną w języku polskim i obronioną w latach 2015–2018 oraz pracę magisterską lub licencjacką (II kategoria) napisaną w języku polskim i obronioną na **ocenę bardzo dobrą** w roku akademickim 2017/2018 lub w roku ubiegłym (2016/2017).

Organizator informuje, że prace będą oceniane w dwóch odrębnych kategoriach:
kategoria I – prace doktorskie,
kategoria II – prace magisterskie i licencjackie.

Prace wraz z wymaganymi dokumentami powinny zostać przesłane zarówno w wersji papierowej, jak i elektronicznej.

Dokumenty, które należy załączyć:

1. Wypełniony i podpisany formularz zgłoszenia do konkursu (plik do pobrania).
2. Opinia promotora lub (i) recenzenta.
3. Pisemna zgoda autora opinii (recenzji) na jej wykorzystanie do celów konkursu.

Adres, na który należy przysłać prace wraz z załącznikami:

Gabinet Szefa ABW
ul. Rakowiecka 2a
00-993 Warszawa

z dopiskiem na kopercie „KONKURS”

Adres e-mail, na który należy przesłać wersję elektroniczną pracy oraz skany załączników: **redakcja.pbw@abw.gov.pl**

Terminy:

Prace należy przesłać do **30 września 2018 r.** (decyduje data stempla pocztowego).

Prace będzie oceniać Komitet Konkursowy powołany przez Szefa ABW, który wyłoni laureatów konkursu w terminie do **31 stycznia 2019 r.**

Wyniki konkursu zostaną opublikowane na stronie internetowej www.abw.gov.pl w ciągu 14 dni od momentu wyboru laureatów przez Komitet Konkursowy. Laureaci zostaną zawiadomieni o wynikach konkursu telefonicznie oraz drogą elektroniczną.

W formularzu zgłoszeniowym uczestnik akceptuje warunki konkursu oraz wyraża zgodę na:

- 1) upowszechnienie treści zawartych w jego pracy do promowania tematyki bezpieczeństwa państwa oraz do celów służbowych ABW,
- 2) gromadzenie i przetwarzanie podanych danych osobowych i ma prawo dostępu do treści swoich danych i ich poprawiania zgodnie z przepisami ustawy z 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 r. nr 101 poz. 926 ze zm.).

Informacje dla autorów „Przeгляdu Bezpieczeństwa Wewnętrznego”

Redakcja zwraca się do autorów nadsyłających teksty do druku o stosowanie następujących zasad:

1. Wszystkie teksty należy przysyłać w postaci zapisu elektronicznego (Word, Open Office) na adres Redakcji: redakcja.pbw@abw.gov.pl.
2. Do artykułu należy dołączyć: bibliografię załącznikową (według schematu opisanego w pkt 10), streszczenie o objętości tekstu do pół strony wydruku komputerowego, notkę o autorze (zawód lub tytuł naukowy, miejsce pracy) oraz pięć słów kluczowych (w celu maksymalnie zwięzłego określenia tematyki artykułu – mają one ułatwić klasyfikację treści oraz wyszukiwanie artykułu w elektronicznych bazach danych; słowa kluczowe nie powinny być powtórzeniem tytułu). Streszczenie i słowa kluczowe powinny być przekazane również w języku angielskim.
3. Autorzy powinni wypełnić *Formularz zgody autora na publikację artykułu w czasopiśmie „PBW”* dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego i przesłać go na adres Redakcji podany w pkt 1.
4. Wszelkie ilustracje, zdjęcia oraz schematy, które autor chciałby umieścić w artykule, powinny być dostarczone w oddzielnych oryginalnych plikach; ich wymiary powinny być nie mniejsze, niż te, które mają być otrzymane po wydruku oraz możliwie jak najlepszej jakości (min. 300 dpi w skali 1:1). W przypadku dostarczenia ilustracji złej jakości Redakcja zastrzega sobie prawo do ich nieumieszczenia.
5. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itd.).
6. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.
7. Odsyłacze do przypisów powinny być umieszczone w tekście przed znakami interpunkcyjnymi – kropką kończącą zdanie (wyjątek: skrót r. – rok lub podobny), przecinkiem itd.
8. Cytaty ze źródeł i literatury przedmiotu, nazwy ustaw i innych aktów prawnych, tytuły prac naukowych, utworów literackich, muzycznych, dramatycznych, obrazów, konkursów należy wyróżniać kursywą.
9. Nazwy wystaw, konferencji i sesji naukowych należy pisać antykwą (tekstem prostym) w cudzysłowie.
10. W przypisach powinien być zachowany następujący schemat opisu:
 - a) przypis zaczynamy wielką literą (wyjątek stanowi przypis internetowy) i kończymy kropką,

- b) przypis archiwalny: nazwa archiwum, po przecinku – nazwa zespołu, po przecinku – sygnatura, po przecinku – nazwa dokumentu (kursywą) lub jego opis (np.: list, sprawozdanie) i data, po przecinku – numer karty (strony),

PRZYKŁADY:

AIPN, OBUiAD w Krakowie, IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57; APK, UWŚl., sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r. z 5 I 1929 r., k. 57;

- c) druki zwarte: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – ewentualnie tom, po przecinku – miejsce i rok wydania, po przecinku – wydawnictwo, po przecinku – numery stron; po tytule publikacji zamieszczonej w pracy zbiorowej stawiamy przecinek i piszemy: w: i tytuł pracy (kursywą),

PRZYKŁAD:

W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 36;

- d) artykuły w czasopismach: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – tytuł czasopisma w cudzysłowie, dalej (bez przecinka) rok wydania, po przecinku – zeszyt, numer, część (w opisie należy stosować cyfry arabskie), po przecinku – numery stron,

PRZYKŁAD:

W. Nowak, *Służba więzienna*, „Prokuratura i Prawo” 2009, nr 4, cz. 2, s. 13;

- e) wydawnictwa internetowe: adres internetowy rozpoczynający się małą literą (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:

<http://www.pbw.gov/abw/cat.html> [dostęp: 1 XII 2011];

- f) artykuły lub dokumenty zamieszczone na stronach internetowych: tytuł artykułu (dokumentu) kursywą, po przecinku – adres internetowy, po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:

EU NAVFOR Somalia – mission, <http://www.eunavfor.eu/about-us/mission/> [dostęp: 20 VII 2014];

- g) podając numer strony, należy stosować skrót: s. (np. s. 30); zakres stron należy zaznaczyć półpauzą bez świąteł, np.: s. 24–27,
- h) należy stosować oznaczenia: tamże, tenże, taż (jeżeli tego typu zwroty rozpoczynają przypis, należy stosować wielką literę), inicjał imienia, nazwisko autora, po przecinku – skrót tytułu (kursywą), po przecinku – numery stron; nie stosujemy skrótów: op. cit., loc. cit.,

PRZYKŁAD:

W. Nowak, *Shūzba...*, s. 12.

Tamże, s. 14;

- i) po skrótach: zob. i por. nie stawiamy dwukropka,
 - j) po skrócie: cyt. za: stawiamy dwukropek,
 - k) po słowie: patrz stawiamy dwukropek.
11. Przy zestawianiu bibliografii załącznikowej kolejne pozycje szeregujemy w porządku alfabetycznym (również akty prawne). Opis każdej pozycji rozpoczynamy od nazwiska autora, po nim umieszczamy inicjał imienia, kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. W przypadku druków zwartych na końcu opisu bibliograficznego należy podać łączną liczbę stron, w przypadku artykułu w czasopiśmie lub w pracy zbiorowej – zakres stron.

PRZYKŁADY:

Kowalski W., *Shūzba więzienna*, „Prokuratura i Prawo” 2009, nr 4, cz. 2, s. 12–20.

Nowak W., *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 32–47.

Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014, Zysk i S-ka, 542 s.

12. W tekście głównym należy stosować ogólnie przyjęte skróty (np., itp., m.in., rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
13. W tekście głównym, podając datę, nazwę miesiąca należy zapisywać słownie, np.: 3 lipca 1969 r. Wyjątek stanowi zapis podany w przypisie, gdy miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
14. Różne sposoby zapisu daty stosowane w tekście głównym powinny być ujednolicone do następującej formy: dzień zapisany cyframi arabskimi, miesiąc zapisany słownie, rok zapisany cyframi arabskimi (np. jak wyżej – 3 lipca 1969 r.); nie należy zamieniać na liczbę rzymską nazw miesięcy pisanych słownie w tekstach źródłowych.
15. Przy podawaniu daty dostępu do źródeł internetowych miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.

16. W tekście głównym należy podawać pełne imię i nazwisko osoby, która jest wymieniana po raz pierwszy.
17. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
18. Obce nazwy organizacji oraz skróty od nich utworzone powinny być pisane antykwą.
19. Nie należy stosować tzw. twardych spacji.
20. Ortografię i interpunkcję tekstu należy uwspółcześniać.
21. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być zaznaczone wytłuszczoną czcionką.
22. Nawiasy ukośne /.../ powinny być zamieniane na nawiasy półokrągłe (...).
23. Skróty słownikowe należy pozostawić bez rozwinięcia.
24. Uzupełnienie odautorskie, od Redakcji itp. należy podawać w nawiasach półokrągłych antykwą.
25. Opuszczenia tekstu pochodzące od wydawcy powinny być zaznaczone trzema kropkami w nawiasie okrągłym.
26. Opuszczenia tekstu w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie okrągłym.
27. Redakcja zastrzega sobie prawo do zwracania autorom tekstów opracowanych bez uwzględnienia powyższych zasad.
28. Redakcja zastrzega sobie prawo do dokonywania zmian i skrótów w porozumieniu z autorem.
29. Redakcja zwraca uwagę, że *ghostwriting** i *guest authorship*** są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą ujawniane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.).
30. Redakcja zwraca uwagę, że autorzy tekstów powinni w sposób przejrzysty, rzetelny i uczciwy prezentować rezultaty swojej pracy, a wszelkie przejawy nierzetelności naukowej, zwłaszcza łamanie i naruszanie zasad etyki obowiązujących w nauce, będą przez Redakcję dokumentowane.

* Z *ghostwriting* mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, ale jego udział jako autora nie zostaje ujawniony lub choćby uwzględniony w podziękowaniach dołączonych do tekstu.

** Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.

