PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 25 (13) 2021

Rada naukowa

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

Recenzenci PBW 25

dr hab. Robert Borkowski
dr Piotr Chorbot
Krzysztof Kołtan
dr Robert T. Lach
dr Rafał Leśkiewicz
dr hab. Ryszard Machnikowski
prof. dr hab. Piotr Majer
dr Krzysztof Malesa
dr Witold Ostant
dr Dariusz Pożaroszczyk
dr hab. Grzegorz Tylec
dr Michał Wojnowski
prof. dr hab. Waldemar Zubrzycki

INTERNAL SECURITY REVIEW

WARSAW 25 (13) 2021

Zespół redakcyjny dr Patryk Dobrzycki (redaktor naczelny)
Elżbieta Dąbrowska (sekretarz Redakcji)
Aneta Olkowska, Grażyna Osuchowska,
Izabela Paczesna (redakcja, korekta)
Agnieszka Dębska (skład)

© Copyright by Agencja Bezpieczeństwa Wewnętrznego, 2021

ISSN 2080-1335
e-ISSN 2720-0841

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

Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wersja online czasopisma jest dostępna na stronie www.abw.gov.pl/wyd/

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) jest zamieszczony w Index Copernicus Journal Master List z liczbą 70,13 punktu. Czasopismo jest również dostępne w bazach: Central European Journal of Social Science and Humanities i Polska Bibliografia Naukowa (PBN)

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
ul. Nadwiślańczyków 2, 05-462 Wiązowna

Redakcja
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 693
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Numer zamknięto i oddano do druku w listopadzie 2021 r.

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

SPIS TREŚCI

I. ARTYKUŁY I ROZPRAWY

Piotr Mickiewicz, Daniel Damian Kasprzycki
Od „konfliktu hybrydowego" do działań konwencjonalnych? Koncepcja oddziaływania militarnego Rosji, ze szczególnym uwzględnieniem zmian po 2018 roku 11

Dariusz Gradzi
Najnowsze kierunki zmian regulacyjnych w zakresie walut wirtualnych z perspektywy przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, z uwzględnieniem wpływu pandemii COVID-19 na wzrost obrotu bezgotówkowego 31

Maciej Gurtowski, Jan Waszewski
Niewidzialna infrastruktura Internetu – usługi chmurowe jako krytyczny element środowiska bezpieczeństwa. Przypadek Amazona 59

Remigiusz Lewandowski
Alternatywne narzędzia zdalnej identyfikacji 85

Łukasz Skoneczny, Bogusław Cacko
Sharp power – wprowadzenie do problematyki 102

Rafał Jerzy Kruszyński
Czerwone morze, czyli dominacja komunizmu we współczesnym świecie 120

Rafał Wądołowski
Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne 146

Paweł Gacek
Wszczęcie postępowania karnego o przestępstwo umyślne ścigane z oskarżenia publicznego jako przesłanka zawieszenia funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu w czynnościach służbowych 183

Krzysztof Izak
Dwadzieścia lat od ataku z 11 września 2001 r. Przygotowania do ataku terrorystycznego na USA oraz jego przebieg i skutki 219

II. RECENZJE

Krzysztof Izak
Ewa Martusewicz-Pawlus, Euroislam contra islamizm. Drogi i bezdroża bezpieczeństwa obywateli Unii Europejskiej 253

Robert Borkowski
Adam Kucharski, Prawa epidemii: skąd się epidemie biorą i dlaczego wygasają? 268

III. PRZEGLĄD PRAC KONKURSOWYCH

Jacek Michał Wojciechowski
Typy uprzywilejowane przestępstwa korupcji wyborczej 279

Izabela Dąbrowska
Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika 293

IV. WYBRANE ARTYKUŁY W JĘZYKU ANGIELSKIM

Łukasz Skoneczny, Bogusław Cacko
Sharp power – introduction to the issue 325

Krzysztof Izak
Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA 341

O autorach 370

Informacje dla autorów 374

TABLE OF CONTENTS

I. ARTICLES AND DISSERTATIONS

Piotr Mickiewicz, Daniel Damian Kasprzycki
Evolving from hybrid conflict leading into conventional warfare? The Russian concept of military impact, with particular reference to the changes after 2018 11

Dariusz Gradzi
The latest trends in regulatory changes for virtual currencies with regard to counteracting money laundering and financing of terrorism as well as the increase of cash-less transactions resulting from the COVID-19 pandemic 31

Maciej Gurtowski, Jan Waszewski
The invisible Internet infrastructure – cloud services as a critical element of the security environment. The Amazon case 59

Remigiusz Lewandowski
Alternative tools of remote identification and authentication 85

Łukasz Skoneczny, Bogusław Cacko
Sharp power – introduction to the issue 102

Rafał Jerzy Kruszyński
The sea of red, that is the domination of communism in the world today 120

Rafał Wądołowski
Protection of classified information in the USA. Selected penal and administrative regulations 146

Paweł Gacek
Initiation of criminal proceedings in the case of intent offence subject to a public accusation as a prerequisite of suspending an officer of the Internal Security Agency and the Foreign Intelligence Agency 183

Krzysztof Izak
Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA 219

II. REVIEWS

Krzysztof Izak
Ewa Martusewicz-Pawlus, Euroislam contra islamizm. Drogi i bezdroża bezpieczeństwa obywateli Unii Europejskiej 253

Robert Borkowski
Adam Kucharski, Prawa epidemii: skąd się epidemie biorą i dlaczego wygasają? 268

III. OVERVIEW OF THE WORKS

Jacek Michał Wojciechowski
Mitigated forms of election corruption crimes 279

Izabela Dąbrowska
Operational deception (Maskirovka) as a Russian capability to surprise the enemy 293

IV. SELECTED ARTICLES IN ENGLISH

Łukasz Skoneczny, Bogusław Cacko
Sharp power – introduction to the issue 325

Krzysztof Izak
Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA 341

About the authors 372

Information for the authors 374

I

ARTYKUŁY I ROZPRAWY

ARTICLES AND DISSERTATIONS

PIOTR MICKIEWICZ
ORCID: 0000-0002-3533-337X

DANIEL DAMIAN KASPRZYCKI
ORCID: 0000-0002-7412-3447

DOI: 10.4467/20801335PBW.21.019.14296

Od „konfliktu hybrydowego" do działań konwencjonalnych? Koncepcja oddziaływania militarnego Rosji, ze szczególnym uwzględnieniem zmian po 2018 roku

W publicystyce poświęconej współczesnym konfliktom zbrojnym rosyjskie działania na Ukrainie, zwłaszcza na Półwyspie Krymskim, nazwano wojną hybrydową. W rosyjskiej myśli wojskowej pojęcie „wojna hybrydowa" (wykreowane przez część anglosaskich analityków, przede wszystkim Franka Hoffmana[1]) oznaczało połączenie metod militarnych i niemilitarnych, umożliwiające osiągnięcie celu operacyjnego lub strategicznego. Rosjanie nie odnajdywali w tej koncepcji żadnego novum i nie traktowali jej jako kompletnej wizji wojny nowej generacji czy nowego typu. Pojęcie „wojna hybrydowa" wykorzystano nawet w narracji politycznej, wskazując, że jest to – głównie amerykański – sposób prowadzenia działań, mający na celu obalenie „niewygodnych" reżimów politycznych. W tym tonie wypowiadał się m.in. minister obrony Federacji Rosyjskiej (FR) Siergiej Szojgu: *Nasi zachodni koledzy uwielbiają oskarżać Rosję o prowadzenie jakiejś tam wojny hybrydowej, ale prawdziwe wojny hybrydowe prowadzi Zachód*[2] (tłum. aut.). Uznano także, że w obecnej sytuacji międzynarodowej większe znaczenie dla ochrony interesów narodowych Rosji ma jej zdolność do interwencji poza granicami kraju. To wymagało zdobycia możliwości prowadzenia

[1] W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey 2002; F. Hoffman, *Conflict in the 21st century: The rise of hybrid wars*, Arlington 2007; J.J. McCuen, *Hybrid Wars*, „Military Review" 2008, nr 2, s. 107–113.

[2] *Сергей Шойгу рассказал, как спасали российскую*, 22 IX 2019 r., https://www.mk.ru/politics/2019/09/22/sergey-shoygu-rasskazal-kak-spasali-rossiyskuyu-armiyu.html [dostęp: 22 IX 2019].

kompleksowych działań polityczno-militarnych, które – wzorem amerykańskich koncepcji Prompt Global Strike i Globally Integrated Operations – nazwano „działaniami zintegrowanymi".

Przedmiotem badań podjętych w niniejszym opracowaniu jest ewolucja rosyjskiej koncepcji „wojny nowego typu", będąca wynikiem doświadczeń wyniesionych z działań prowadzonych na Ukrainie oraz – w mniejszym stopniu – z aktywności militarnej w Syrii. Celem tych badań jest wykazanie, że formuła działań polityczno-militarnych, powszechnie określana mianem wojny hybrydowej lub działań hybrydowych, nie oddaje w pełni rosyjskiej koncepcji prowadzenia polityki międzynarodowej z wykorzystaniem potencjału militarnego. Autorzy przyjęli hipotezę roboczą, że obowiązująca w Rosji wizja wojny nowego typu stanowi połączenie różnych przedsięwzięć niemilitarnych i militarnych, bliższych pojęciom „działania asymetryczne" lub „działania nieliniowe". Celem tych działań jest zwiększenie możliwości antydostępowych, zakładające sukcesywne odsuwanie strefy obrony od granic FR i budowanie (odtworzenie) buforu bezpieczeństwa wokół granic państwa (strategia aktywnej obrony), oraz kształtowanie regionalnego ładu międzynarodowego w obszarach ulokowania rosyjskich interesów narodowych zgodnie z oczekiwaniami tego państwa (strategia działań ograniczonych). Osiągnięcie tak zdefiniowanego celu wymaga dysponowania przez FR potencjałem pozwalającym na ograniczenie działań reaktywnych lub odwetowych, podejmowanych zarówno przez państwa poddane takiemu oddziaływaniu, jak i społeczność międzynarodową, do poziomu aprobowanego przez Moskwę. Przyjęta hipoteza robocza została poddana weryfikacji, w ramach której autorzy przeanalizowali problemy szczegółowe dotyczące:

1) roli środków oddziaływania wykorzystywanych w tzw. działaniach zintegrowanych, określanych jako instrumentarium hybrydowe;
2) roli działań pośrednich, zastępczych i specjalnych oraz klasycznych operacji konwencjonalnych w rosyjskiej polityce bezpieczeństwa;
3) znaczenia koncepcji zewnętrznego pierścienia obrony oraz strategii aktywnej obrony w rosyjskiej doktrynie wojennej;
4) roli systemowej reformy rosyjskich sił zbrojnych przeprowadzanej w celu osiągnięcia zdolności do prowadzenia działań zintegrowanych w ramach przedsięwzięć określanych jako budowa zewnętrznego pierścienia obrony oraz zdolności do realizowania strategii działań ograniczonych.

Autorzy zrezygnowali z koncentrowania uwagi na specyfice działań hybrydowych, gdyż uznali, że jest to zagadnienie dobrze opracowane, także przez polskie środowisko naukowe[3]. Ponadto w rosyjskiej polityce bezpieczeństwa zakres przedsięwzięć

[3] Zagadnienie, o którym mowa, było wielokrotnie omawiane także na łamach „Przeglądu Bezpieczeństwa Wewnętrznego".

określanych jako oddziaływanie PEMSI[4] oraz tzw. etapy prowadzenia działań hybrydowych[5] nie zostały zmodyfikowane.

Przyjęte podejście wpłynęło na dobór metod badawczych, wśród których najważniejsze były: analiza dokumentów i dorobku badawczego rosyjskich strategów wojskowych oraz analiza czynnikowa z elementami analizy historycznej. Celem badań było wskazanie czynników determinujących sposób realizowania polityki bezpieczeństwa przez FR, a w konsekwencji pokazanie przeobrażeń doktryny wojskowej i koncepcji wykorzystania potencjału sił zbrojnych. Jest to podejście odmienne od dotychczas przeprowadzonych analiz o tej tematyce, które koncentrowały się na zagadnieniu hybrydowości form oddziaływania międzynarodowego, a ostatnio – na budowie potencjału antydostępowego.

Dyskurs naukowy dotyczący roli poszczególnych środków oddziaływania wykorzystywanych w ramach działań zintegrowanych został zdominowany przez tezy autorstwa Hoffmana, a w Polsce głównie przez środowiska skupione wokół Centrum Doktryn i Szkoleń Ministerstwa Obrony Narodowej oraz ośrodków analitycznych zajmujących się problematyką militarną lub Wspólnotą Niepodległych Państw. Dorobek w tym obszarze badań obejmuje przede wszystkim udokumentowanie działań uznawanych za hybrydowe, wskazanie cech, które je wyróżniają, zwłaszcza w odniesieniu do działań asymetrycznych i przeciwnika asymetrycznego. Wnioski zaprezentowane w niniejszym artykule zostały oparte na analizie rosyjskich działań na Półwyspie Krymskim i w Donbasie, w minimalnym stopniu przeanalizowano także działania prowadzone w Syrii.

W przypadku drugiego problemu szczegółowego wiodącym podejściem badawczym jest tradycyjne postrzeganie koncepcji A2/AD[6] (zgodnie ze szkołą amerykańską) i ocena rosyjskiego potencjału bojowego pod kątem możliwości prowadzenia skutecznych działań antydostępowych. W europejskiej literaturze przedmiotu, w tym polskiej, badacze w ograniczonym stopniu odnoszą się do problematyki podnoszonej przez rosyjskich strategów wojskowych w związku z wizją wojny nowego typu. Jest to zazwyczaj prezentacja autorskich koncepcji poszczególnych środowisk i badaczy, bez uwzględnienia ich wpływu na całokształt polityki bezpieczeństwa. Niniejsze opracowanie jest próbą ukazania uwarunkowań i zakresu modyfikacji tej koncepcji w kontekście

---

[4] PEMSI (ang. *politics*, *economy*, *military*, *social affairs*, *information technology*) – skrót oznaczający działania w obszarach: politycznym, ekonomicznym, militarnym, społecznym i informacyjnym (przyp. red.). Pojęcie i strategię PEMSI upowszechniają w Polsce oficerowie z Centrum Doktryn i Analiz MON. Zob. „Przegląd Sił Zbrojnych" 2017, nr 4; C. Pawlak, *Konflikt na wschodzie Ukrainy sztandarowym przykładem działań hybrydowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, nr 1, s. 268–287; J. Keplin, C. Pawlak, *Hybrydowość wyzwaniem dla bezpieczeństwa przyszłości*, „Biuletyn CDiS SZ" 2016, nr 2, s. 5–7; C. Pawlak, J. Keplin, *Aneksja Krymu w kontekście działań hybrydowych*, „Kwartalnik Bellona" 2016, nr 3, s. 23–32.

[5] В. Герасимов, *Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий*, „Военно-промышленный курьер", 26 II 2013 r., http://www.vpk-news.ru/articles/14632 [dostęp: 10 II 2018].

[6] Skrót od *Anti-Access/Area Denial* oznaczający systemy antydostępowe (przyp. red.).

polityki bezpieczeństwa FR oraz formuły przygotowania rosyjskich sił zbrojnych do prowadzenia działań bojowych, jaką wdraża Sztab Generalny Sił Zbrojnych FR kierowany przez gen. Walerija Gierasimowa.

Ewolucja koncepcji wykorzystania sił zbrojnych w polityce bezpieczeństwa Federacji Rosyjskiej po 2018 roku

Rosyjska polityka bezpieczeństwa jest oparta na kilku niezmiennych założeniach. Jej podstawą doktrynalną jest, wywodząca się z teorii realizmu politycznego, koncepcja bezpieczeństwa, przyjmująca, że podmiotem jest państwo jako gracz międzynarodowy[7]. Tak zwana potęga państwa[8], która we wspomnianej teorii odgrywa istotną rolę, jest natomiast postrzegana przez pryzmat koncepcji geopolitycznej Wieniamina Siemionowa Tien-Szańskiego. Za cel polityki bezpieczeństwa uznawał on zdolność do zapewniania władzy centralnej kontroli nad obszarem państwa, ochronę „centrów" decydujących o potędze państwa oraz zdominowanie obszarów ulokowania interesów narodowych, zwłaszcza tych zlokalizowanych wokół zewnętrznych granic państwa[9]. Powyższe założenia powodują, że w polityce Rosji koncepcja tzw. działań zintegrowanych jest sprowadzona do wykorzystania elementów swoistego „zbioru" instrumentów, pozwalających na realizację – w sposób maksymalnie ograniczający możliwość reakcji na rosyjskie działania – celów politycznych na określonym obszarze. Z tego względu preferowanym instrumentarium są działania niemilitarne i nieagresywne działania komponentu militarnego, jednak w sytuacji braku możliwości ich prowadzenia podstawowym środkiem pozostaje instrumentarium militarne. Dlatego też potencjał militarny FR musi być rozbudowywany i powinien dysponować zdolnością do szybkiej reakcji na zaistnienie zdarzeń ograniczających tak rozumiane bezpieczeństwo państwa (niemożność osiągnięcia interesów narodowych i zagrożenie integralności państwa).

Analiza doboru instrumentarium wykorzystanego na Krymie i we wschodniej Ukrainie pozwala stwierdzić, że są to przykłady klasycznego zastosowania koncepcji działań zintegrowanych. Priorytetowe potraktowanie działań niemilitarnych na obszarze Półwyspu Krymskiego wynikało z przeprowadzonych analiz i założenia, że uwarunkowania społeczne pozwolą na osiągnięcie celów środkami niemilitarnymi. Uznano również, że konwencjonalne wykorzystanie instrumentarium militarnego może wywołać negatywną reakcję społeczności międzynarodowej. Nie był to główny czynnik

[7] Zob. szerzej: J. Czaputowicz, *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa 2008, s. 58.

[8] Zob. szerzej: A. Wojciuk, *Dylemat potęgi. Praktyczna teoria stosunków międzynarodowych*, Warszawa 2010, s. 27–35.

[9] P. Mickiewicz, *W poszukiwaniu teoretycznych podstaw rosyjskiego myślenia strategicznego ery W. Putina*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, nr 2, s. 39–56.

decydujący o charakterze rosyjskich działań, ale został wzięty pod uwagę. We wschodniej części Ukrainy postawa lokalnej społeczności była inna, dlatego wykorzystano zarówno potencjał protestu, jak i potencjał militarny.

Tab. 1. Korelacja militarnych i niemilitarnych środków oddziaływania według gen. Walerija Gierasimowa (koncepcja z 2013 r.).

Etap operacji	Działania niemilitarne	Etap operacji	Działania militarne
1–2	tworzenie wewnątrzpaństwowej opozycji w państwie, które jest celem agresji	1–6	prowadzenie działań destabilizujących sytuację polityczną
1–3	budowanie koalicji i potencjału protestu w państwie, które jest celem agresji	1–4	aktywna polityka odstraszania (redukowanie możliwości udzielenia wsparcia państwu, które jest celem agresji)
2–3	wywieranie presji politycznej		
2–4	wywieranie presji polityczno-ekonomicznej	3–4	strategiczne rozmieszczenie sił zbrojnych
3–4	kreowanie wystąpień opozycji		
4	blokada ekonomiczna	4–5	przeprowadzenie operacji zaprowadzającej lub zapewniającej pokój (stabilizacyjnej, humanitarnej, pokojowej)
5	wymuszenie procesu mobilizacji gospodarki; próba zmiany przywództwa politycznego		
5–6	działania na rzecz deeskalacji konfliktu wewnętrznego w państwie, które jest celem agresji	6	działania na rzecz budowania pokoju

Źródło: Opracowanie własne na podstawie: В. Герасимов, *Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий*, „Военно-промышленный курьер", 26 II 2013 r., http://www.vpk-news.ru/articles/14632 [dostęp: 10 II 2018].

Istnieją przesłanki świadczące o tym, że rosyjscy wojskowi nie uznają działań hybrydowych za uniwersalną koncepcję wojny nowego typu. Wskazują na to wyniki analizy dotyczącej procesu modernizacji (jego zakresu i skali) rosyjskich sił zbrojnych oraz odmienne podejście do działań prowadzonych na Półwyspie Krymskim i w obwodach wschodniej Ukrainy. Jeszcze silniej potwierdzają tę tezę dwa inne zjawiska – specyficzne rozumienie interesu narodowego przez rosyjski establishment polityczny oraz sposób definiowania pojęcia „bezpieczeństwo państwa". W odniesieniu do odmienności działań prowadzonych na różnych obszarach Ukrainy należy podkreślić, że skuteczność operacji krymskiej w dużej mierze wynikała z odpowiedniego wykorzystania specyfiki społecznej, zwłaszcza uwarunkowań narodowościowych. Nieco inna struktura społeczna, jak również odmienne poglądy na kwestię przynależności państwowej prezentowane przez ludność obwodów ługańskiego i donieckiego uniemożliwiły powielenie tam scenariusza krymskiego i wymusiły użycie potencjału

militarnego[10]. Ta sytuacja dowiodła, że „metoda krymska" (w postaci skoordynowanych działań PEMSI) nie może być traktowana jako jedyny sposób czy uniwersalna koncepcja prowadzenia operacji polityczno-militarnej. Dużo ważniejsze jest jednak postrzeganie potęgi państwa, któremu przyznaje się rangę mocarstwa globalnego, i zapewnienie mu bezpieczeństwa. Zgodnie z teorią Tien-Szańskiego dotyczącą funkcjonowania mocarstwa lądowego rosyjski potencjał militarny ma odgrywać rolę instrumentu służącego zarówno do odstraszania potencjalnych wrogów, jak i do realizacji interesów narodowych[11]. Federacja Rosyjska musi więc dysponować potencjałem bojowym adekwatnym do tego, jaki mają jej główni rywale polityczni, i być zdolna do prowadzenia operacji militarnych pozwalających na realizację i ochronę interesów strategicznych państwa. Należy się zgodzić z tezą, że porażka w wyścigu zbrojeń w latach 80. XX w. (zwłaszcza jej konsekwencje polityczne i ekonomiczne) spowodowała, że w późniejszych rosyjskich koncepcjach militarnych uwzględniono możliwość korzystania z różnych form działań pośrednich, zastępczych i specjalnych zamiast klasycznych operacji konwencjonalnych. Szczególną rolę przypisano działaniom sił specjalnych o charakterze dywersyjnym i sabotażowym, zdolnościom do działania w specyficznym środowisku naturalnym oraz mobilności poszczególnych oddziałów. Jest to widoczne przede wszystkim w realizowanym od 2014 r. procesie rozbudowy potencjału militarnego w rosyjskiej Arktyce. Początkowo ograniczono go do tworzenia systemu baz dla komponentów wojsk lądowych, sił morskich i powietrznych. Stacjonujące w nich oddziały miały być zdolne do obrony Jakucji i ulokowanych tam instalacji wydobywczych oraz do kontroli żeglugi na wybranych akwenach Oceanu Arktycznego. Dzięki kolejnym inwestycjom w rozwój systemu baz wojskowych oraz potencjału militarnego (13 lotnisk i 10 stacji radarowych pozwalających na monitorowanie ruchu morskiego i przestrzeni powietrznej Oceanu Arktycznego), jak również dzięki rozbudowie potencjału bojowego sił morskich i sił specjalnych możliwe stało się podejmowanie działań określanych jako zabezpieczenie strategiczne rosyjskich obszarów arktycznych[12].

---

[10] M. Kofman, M. Rojansky, *A Closer look at Russia's 'Hybrid War'*, „Kennan Cable" 2015, nr 7, s. 4–5, https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf [dostęp: 12 I 2021].

[11] P. Mickiewicz, *W poszukiwaniu teoretycznych podstaw*…

[12] Poza klasycznymi związkami taktycznymi na obszarze Dowództwa Strategicznego Północ funkcjonują: oddział rozpoznania specjalnego, oddziały sił specjalnych przeznaczone do zwalczania i prowadzenia działań sabotażowo-dywersyjnych i walki radioelektronicznej (WRE), które mogą skutecznie zakłócać systemy obserwacji technicznej, nadzoru ruchu i łączności. Zob. szerzej: P. Mickiewicz, *Rosyjska polityka arktyczna – próba zdominowania regionu czy instrument polityki bezpieczeństwa?*, w: *Geopolityka Rosji i obszaru postsowieckiego*, L. Sykulski (red.), Warszawa 2020, s. 178–204; D.D. Kasprzycki, *Militarny aspekt rosyjskiej obecności w Arktyce w kontekście regionalnego bezpieczeństwa do 2018 r.*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, nr 2, s. 190–216. Szczegółowe zestawienie sił wchodzących w skład Dowództwa Strategicznego Północ znajduje się na blogu Milkavkaz, na stronie Северный Флот, 7 VII 2017 r., http://milkavkaz.com/index.php/voorujonnie-cili-racii/vmf/cf [dostęp: 10 III 2018].

Analiza środowiska bezpieczeństwa, ocena potencjału innych graczy międzynarodowych oraz doświadczenia płynące z tzw. kolorowych rewolucji na obszarze Wspólnoty Niepodległych Państw doprowadziły do sformułowania głównego założenia rosyjskiej polityki bezpieczeństwa, zgodnie z którym podstawową metodą wpływania na państwo rosyjskie i jego interesy będą różnorodne instrumenty asymetryczne (nieliniowe). To z kolei implikuje konieczność korzystania z metod adekwatnych do tego rodzaju działań. Po przeanalizowaniu poglądów współczesnych rosyjskich teoretyków wojskowości można założyć, że w przypadku konfrontacji z przeciwnikiem o porównywalnym lub większym potencjale, jak również w sytuacji, w której może dojść do niekontrolowanej eskalacji konfliktu, Rosja będzie stosować różne działania pośrednie[13]. Powinny one przyjąć postać działań mieszczących się w ramach szeroko interpretowanego prawa dotyczącego konfliktów zbrojnych czy też pokojowego wykorzystania potencjału bojowego oraz działań ograniczających możliwość wskazania ich kreatora (cyberataki, różne formy oddziaływania radioelektronicznego, niszczenie obiektów w przestrzeni międzynarodowej). Natomiast w przypadku konfrontacji z przeciwnikiem o mniejszym potencjale prawdopodobne jest przeprowadzenie klasycznej operacji militarnej, która będzie sankcjonowana za pomocą stosownej interpretacji prawa międzynarodowego (prawo do samostanowienia, operacja humanitarna, ochrona ludności i jej praw itp.). Zrealizowanie takiej operacji może być również uzasadniane zaistnieniem, wykreowanej przez państwo rosyjskie, destabilizacji w państwie, które jest obiektem agresji.

Celem współczesnych operacji militarnych powinno być nie tyle opanowanie terenu, ile uniemożliwienie przeciwnikowi prowadzenia działań obronnych. Można to osiągnąć przez udaremnienie działania jego siłom zbrojnym, zniechęcenie społeczeństwa do prowadzenia wojny obronnej oraz ograniczenie do minimum możliwości ekonomicznych państwa, które jest celem agresji[14]. Skutkiem prowadzonych równolegle działań politycznych ma być natomiast dyplomatyczne wyizolowanie tego państwa ze społeczności międzynarodowej.

Zgodnie z przyjętymi założeniami rosyjski potencjał bojowy powinien zapewniać możliwość przeprowadzania precyzyjnych uderzeń na obiekty infrastruktury krytycznej i decydującej o sposobie funkcjonowania społeczeństwa i gospodarki państwa będącego obiektem agresji oraz zrealizowania klasycznej (kinetycznej) operacji militarnej[15]. Uznano, że celami dla broni precyzyjnej są obiekty, przede wszystkim systemy

---

[13] Zob. szerzej: *Rosyjska myśl strategiczna i potencjał militarny w XXI wieku*, P. Mickiewicz (red.), Warszawa 2018.

[14] П.А. Дульнев, В.Г. Ковалев, Л.Н. Ильин, *Асимметричное противодействие в сетецентрической войне*, „Военная мысль" 2011, nr 10, s. 3–8, http://militaryarticle.ru/voennaya-mysl/2011-vm/10357-asimmetrichnoe-protivodejstvie-v-setecentricheskoj [dostęp: 11 X 2019]; С.Г. Чекинов, С.А. Богданов, *Асимметричные действия по обеспечению военной безопасности России*, „Военная мысль" 2010, nr 3, s. 13–22, http://militaryarticle.ru/voennaya-mysl/2010-vm/10291-asimmetrichnye-dejstvija-po-obespecheniju-voennoj [dostęp: 10 X 2019].

[15] Równocześnie ma być on zdolny do prowadzenia działań A2/AD.

wykorzystywane przez administrację centralną państwa i jego siły zbrojne, kompleksy gospodarcze, zwłaszcza systemy sektora energetycznego, paliwowego, chemicznego i transportowego oraz kreujące tzw. łańcuchy zdarzeń kryzysowych. Sposobem prowadzenia działań zapożyczonym z amerykańskich rozwiązań jest korzystanie z prywatnych firm wojskowych (ang. *private military company*, PMC) i ochroniarskich (ang. *private military and security company*, PMSC)[16].

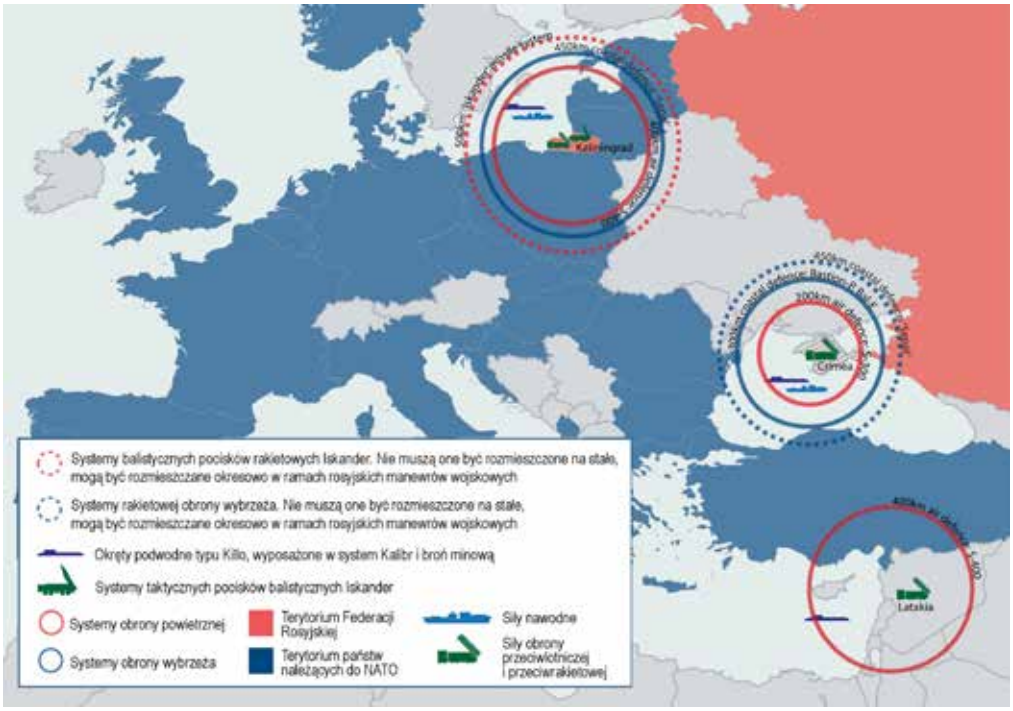
W sferze działań obronnych dominuje natomiast koncepcja dotycząca budowy zdolności antydostępowych w dwóch równoległych wersjach. Pierwszą niezmiennie pozostaje tworzenie stref buforowych wokół zewnętrznych granic FR. Drugą, wdrażaną obecnie, jest stosowanie rozwiązań A2/AD w wariancie tzw. obronnych działań zaczepnych. Podstawowym założeniem rosyjskiej koncepcji jest przesuwanie własnej strefy obrony, czemu towarzyszy poszerzanie strefy wpływów, osiągane przez zwiększanie potencjalnego obszaru rażenia (dyslokacje uzbrojenia lub jego wymiana na takie, które ma lepsze właściwości taktyczne lub większy zasięg). Drugą cechą rosyjskiego systemu antydostępowego jest konsolidacja potencjału militarnego różnych rodzajów sił zbrojnych i wojsk stacjonujących na danym obszarze, zwłaszcza systemów: obserwacji i wskazania celów, obrony przeciwlotniczej, walki radioelektronicznej, obrony wybrzeża oraz zestawów rakiet taktycznych. Analizując tę formułę budowy rosyjskiego potencjału antydostępowego, należy wskazać jego dwie kolejne cechy. Pierwszą jest duża samodzielność operacyjna na poszczególnych regionalnych teatrach działań wojennych, uzyskiwana dzięki tworzeniu swoistych centrów militarnych, które w rosyjskiej myśli wojskowej określa się mianem twierdz[17]. Drugą natomiast jest specyficznie tworzony potencjał militarny w tych regionach. Formalnie ma on charakter obronny, ale daje również możliwość prowadzenia działań ofensywnych lub wyprzedzających. Trzonem sił realizujących zadania antydostępowe są bowiem jednostki sił specjalnych, które są wspierane potencjałem broni precyzyjnego rażenia. Na ogół w tych regionach jest rozmieszczony wielowarstwowy potencjał rakietowy i służący do walki radioelektronicznej, wzmocniony siłami konwencjonalnymi oraz dobrze dobranym zabezpieczeniem logistycznym. Ten potencjał tworzą zazwyczaj:

- brzegowe systemy rakietowe zdolne do prowadzenia uderzeń na poziomie taktycznym, operacyjnym i strategicznym (zasięg od 150 do 600 km);
- systemy walki elektronicznej przygotowane do prowadzenia działań na poziomie operacyjno-taktycznym oraz do zakłócania systemów łączności i satelitarnych systemów nawigacyjnych;

[16] Zob. S. Sukhankin, *"A black cat in the dark room". Russian Quasi-Private Military and Security Companies (PMSCs) – 'Non-existent,' but Deadly and Useful*, National Defence and the Canadian Armed Forces, http://www.journal.forces.gc.ca/vol19/no4/page43-eng.asp [dostęp: 12 XII 2020].

[17] Dla rosyjskiej doktryny obronnej najważniejszymi twierdzami są: Obwód Kaliningradzki, Półwysep Krymski, Jakucja i Kamczatka.

- siły okrętowe i powietrzne, których potencjał bojowy zależy od uwarunkowań geograficznych i fizycznych kontrolowanego obszaru (uzbrojenie rakietowe, potencjał desantowy itp.);
- systemy obserwacji powietrznej i obrony przeciwlotniczej, które mają zdolność do ograniczania możliwości rozpoznania powietrznego;
- systemy obserwacji nawodnej o zasięgu do 300 km oraz systemy obserwacji podwodnej;
- siły obrony lądowej, których potencjał bojowy zależy od specyfiki regionu i potencjalnych zdolności bojowych przeciwnika.



Rysunek. Rosyjskie strefy A2/AD w Europie Środkowo-Wschodniej i na Bliskim Wschodzie.

Źródło: *The Military Balance 2015*, International Institute for Strategic Studies, luty 2015.

Przedstawione na powyższym rysunku strefy antydostępowe na zachodnim kierunku obrony pełnią określoną funkcję w systemie aktywnej obrony. Wyposażenie bojowe rozlokowane w twierdzach w Kaliningradzie, na Krymie, w Noworosyjsku oraz w Latakii umożliwia prowadzenie nie tylko działań A2/AD, lecz także realizację przedsięwzięć o charakterze ofensywnym, wykraczających poza formułę aktywnej obrony. We wspomnianych bazach są skoncentrowane środki oddziaływania przeciwlotniczego, przeciwrakietowego, zwalczania sił morskich i prowadzenia walki radioelektronicznej, ale równocześnie są one przygotowane do realizowania działań stricte ofensywnych (możliwość przerzutu i bazowania sił) oraz polityczno-militarnych. Ma to pozwolić

na kreowanie sytuacji w regionie oraz stwarzanie napięcia politycznego w formule incydentów polityczno-militarnych. Należy więc przyjąć, że rozwijanie koncepcji budowy stref antydostępowych w postaci tzw. twierdz było pochodną zmian w sposobie myślenia rosyjskiego kierownictwa polityczno-wojskowego. Zostało to jednoznacznie wyeksponowane w doktrynie wojennej FR z 2014 r.[18], która de facto była próbą przełożenia teorii dotyczących koncepcji wojny nowego typu na praktyczne działania rosyjskich sił zbrojnych. Analizując jej treść w odniesieniu do działań sił zbrojnych, można zauważyć, że zapowiedziano w niej przygotowanie tych sił do prowadzenia działań opartych na tzw. koncepcji aktywnej (agresywnej) obrony, czyli równoległego prowadzenia działań ofensywnych i defensywnych. Wskazano także na konieczność zmiany podejścia do zagadnienia wyposażenia sił zbrojnych oraz, co ważniejsze, niezbędność ścisłego skorelowania zapisów zawartych w tej doktrynie z innymi dokumentami strategicznymi państwa[19]. W porównaniu z poprzednią doktryną istotną zmianą było podkreślenie roli innych niż nuklearne środków odstraszania jako instrumentu polityki bezpieczeństwa[20]. Jednoznaczne stwierdzenie, że samo dysponowanie określonym potencjałem nuklearnym nie gwarantuje bezpieczeństwa państwa, jest istotnym novum. Należy więc przyjąć, że za takowy instrument uznano także nowoczesne siły konwencjonalne, przygotowane do szybkiego reagowania zarówno na obszarze FR, jak i poza jej granicami. Analiza wspomnianej doktryny prowadzi do wniosku, że mogą one być użyte również w celu likwidacji zagrożeń wskazanych w tym dokumencie, w tym tłumienia separatyzmów i rebelii oraz reagowania na zagrożenie rosyjskich interesów w dowolnym regionie świata[21]. Przyjęcie takiego rozwiązania wymagało uzupełnienia składu poszczególnych związków operacyjnych o komponent sił szybkiego reagowania oraz utrzymania wysokiego stopnia gotowości bojowej. Osiągnięciu tych zdolności ma służyć przeprowadzanie licznych manewrów zakrojonych na szeroką skalę oraz niezapowiedzianych ćwiczeń, które jednocześnie mają być sposobem na zademonstrowanie siły. Ich celem jest również sprawdzenie gotowości bojowej poszczególnych jednostek.

---

[18] *Указ Президента Российской Федерации N Пр-2976 от 25 декабря 2014 г.*, *„Военная доктрина Российской Федерации"*, http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf [dostęp: 12 III 2021].

[19] Tamże, rozdział I, pkt 4. W doktrynie wojennej, o której mowa, zostały uwzględnione podstawowe założenia: koncepcja długoterminowego rozwoju społeczno-gospodarczego FR do 2020 r., strategia bezpieczeństwa narodowego FR do 2020 r., jak również odpowiednie regulacje dotyczące: polityki zagranicznej FR, doktryny morskiej FR do 2020 r., strategii rozwoju strefy arktycznej FR i zapewnienia bezpieczeństwa narodowego do 2020 r. oraz innych dokumentów planowania strategicznego.

[20] Tamże, rozdział I, pkt 8, ppkt m. System odstraszania (powstrzymywania) niejądrowego – zespół przedsięwzięć polityki zagranicznej, przedsięwzięć wojskowych i wojskowo-technicznych, które są ukierunkowane na zapobieżenie środkami niejądrowymi agresji przeciwko FR.

[21] Zagrożenia bezpieczeństwa FR są scharakteryzowane w rozdziale II omawianej doktryny, w punktach: 9, 10 i 11. W punkcie 12 zaprezentowano główne zewnętrzne niebezpieczeństwa wojenne, a w punkcie 13 – główne wewnętrzne niebezpieczeństwa wojenne. Opis podstawowych zagrożeń wojennych znajduje się w punkcie 14.

Te elementy pozwoliły na modyfikację strategii aktywnej obrony, która została zaprezentowana w marcu 2019 r.[22]

Obecnie obowiązująca strategia zakłada wykorzystanie „zestawu środków do proaktywnego neutralizowania zagrożeń bezpieczeństwa państwa"[23]. Podkreśla się w niej, że jest ona reakcją na wzrastające zagrożenie ze strony państw wspólnoty transatlantyckiej (co jest stałym elementem narracji uzasadniającej wymóg zwiększenia potencjału militarnego FR) i wskazuje się hybrydowość kreowanych zagrożeń (zmienność zagrożeń kreowanych przez Zachód). Rosyjscy stratedzy wojskowi uznali, że specyfika tych zagrożeń wymusza wprowadzenie zmian w koncepcji dotyczącej reagowania na nie. Niezbędne jest zarzucenie – stosowanej wcześniej – polityki reagowania polityczno-militarnego na zdarzenia niepożądane z punktu widzenia interesu rosyjskiego, które zaistniały na obszarze ulokowania interesów FR lub istotnym dla jej bezpieczeństwa. Została ona zastąpiona ideą polityki służącej zapobieganiu możliwości wystąpienia takich zagrożeń. Wizja tzw. aktywnego reagowania na procesy mogące wywoływać zagrożenia przewiduje korzystanie z całej gamy środków oddziaływania militarnego i niemilitarnego, dobieranych stosownie do charakteru tych procesów[24].

Strategia aktywnej obrony FR, przedstawiana jako stricte defensywna odpowiedź na politykę NATO i USA, zakłada możliwość wyprzedzającego (prewencyjnego) użycia sił zbrojnych w następstwie oceny sytuacji strategicznej. Istotą planowania strategicznego staje się utrzymanie lub przejęcie inicjatywy strategicznej w sytuacji narastania kryzysu. W tym przypadku rosyjscy stratedzy mają na myśli skorelowane przedsięwzięcia polityczno-ekonomiczno-militarne, których celem jest strategiczne powstrzymywanie i wyprzedzające neutralizowanie zagrożeń bezpieczeństwa narodowego państwa. Jednak najważniejszym zadaniem jest przesuwanie zewnętrznego pierścienia obrony (poszerzanie go) w kierunku potencjalnego przeciwka. Jest to realizowane przez wzmacnianie potencjału bojowego, zwłaszcza w postaci broni precyzyjnego rażenia o zwiększonym zasięgu, oraz tworzenie obszaru buforowego za pomocą politycznego lub ekonomicznego zwasalizowania państw graniczących z FR.

Swoistym, gdyż jest to koncepcja lansowana przez część tzw. postępowych kręgów eksperckich, odwołujących się do wizji wojny nowej generacji[25], uzupełnieniem strategii aktywnej obrony jest strategia działań ograniczonych. Zdaniem przedstawicieli tego środowiska powinna ona zakładać prowadzenie działań zewnętrznych w celu

---

[22] Strategię zaprezentował osobiście Szef Sztabu SZ FR gen. Gierasimow w trakcie dorocznego wystąpienia w rosyjskiej Akademii Nauk Wojskowych 2 marca 2019 r. Zob. В. Герасимов, *Векторы развития военной стратегии*, „Красная звезда", 4 III 2019 r., http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1 [dostęp: 1 V 2020].

[23] Tamże.

[24] Tamże.

[25] Liderem tej grupy był gen. Władimir Slipczenko, twórca teorii wojny bezkontaktowej oraz wojny szóstej generacji, ale należy wskazać także generałów Walerija Gierasimowa i Siergieja A. Bogdanowa oraz płk Siergieja G. Czekinowa. Byli oni twórcami koncepcji operacji informacyjno-uderzeniowej.

zarówno ochrony, jak i promowania rosyjskich interesów za granicą[26]. Po przeanalizowaniu wypowiedzi gen. Gierasimowa oraz ekspertyz rosyjskich strategów, zwłaszcza tych odnoszących się do doświadczeń wynikających z przebiegu konfliktu w Syrii[27], można stwierdzić, że obecnie ta koncepcja jest integralnym elementem rosyjskiej polityki bezpieczeństwa. Wydaje się, że w sytuacji narastania kryzysu w obszarze ulokowania rosyjskich interesów głównym scenariuszem działania będzie groźba podjęcia bezpośredniej interwencji wojskowej. Nie zawsze będzie ona tożsama z samą interwencją, gdyż ma to być przede wszystkim sposób na zademonstrowanie siły i woli podjęcia działań. Należy się więc zgodzić z tezami Marena Garberga Bredesena i Karsten Friis, że groźba interwencji odgrywa w rosyjskiej strategii oddziaływania międzynarodowego rolę pomocniczą dla działań prowadzonych z wykorzystaniem środków niemilitarnych[28].

Tab. 2. Doświadczenia płynące z działań militarnych w Syrii.

Element zdobytego doświadczenia	Komentarz
Zdobycie i przetestowanie zdolności do uzyskania przewagi w procesie zarządzania konfliktem i dowodzenia działaniami	Celem uzyskania przewagi jest podejmowanie właściwszych (w stosunku do przeciwnika) i szybszych decyzji, co ma wymusić na dowództwie strony przeciwnej poruszanie się w rosyjskich ramach decyzyjnych. Uzyskanie przewagi w procesie zarządzania konfliktem i dowodzenia działaniami ma być głównym celem w początkowej fazie konfliktu. Przyjęto, że sprawność dowodzenia i kontroli (C2) jest najważniejszym predyktorem sukcesu w operacjach przeprowadzanych zarówno obecnie, jak i tych w przyszłości

[26] В. Герасимов, *Векторы развития военной стратегии*…

[27] Przede wszystkim chodzi o wnioski dotyczące modernizacji systemów C4ISR (z ang. *Command*, *Control*, *Communications*, *Computers*, *Intelligence*, *Surveillance and Reconnaissance*, pol. dowodzenie, kontrola, komunikacja, komputery, wywiad, nadzór i rozpoznanie – przyp. red.), systemów robotycznych i UAV (z ang. *unmanned aerial vehicle*, pol. bezzałogowy statek powietrzny – przyp. red.) oraz modyfikację sposobu prowadzenia operacji humanitarnych i działań z zakresu *conflict management* za granicą. Ciekawą analizą na ten temat jest raport opracowany przez Institute for the Study of War, opublikowany w styczniu 2021 r. Zob. M. Clark, *The Russian Military's Lessons Learned In Syria*, Washington 2021, http://www.understandingwar.org/sites/default/files/The%20Russian%20Military%E2%80%99s%20Lessons%20Learned%20in%20Syria_0.pdf [dostęp: 10 III 2021].

[28] Zob. szerzej: M.G. Bredesen, K. Friss, *Missiles, Vessels and Active Defence. What Potential Threat Do the Russian Armed Forces Represent?*, „The RUSI Journal" 2020, nr 5–6, s. 68–78, https://www.tandfonline.com/doi/full/10.1080/03071847.2020.1829991 [dostęp: 10 III 2021]; D. Massicot, *Anticipating a New Russian Military Doctrine in 2020: What It Might Contain and Why It Matters*, War on the Rocks, 9 IX 2019 r., https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/ [dostęp: 10 III 2021].

Element zdobytego doświadczenia	Komentarz
Koordynacja i sposób zawiązywania formalnych koalicji w przyszłych wojnach	Przyjętym wariantem jest zastąpienie koncepcji „wojny zastępczej" (ang. *proxy war*) przez projekcję siły i działania koalicji chętnych. Obecnie jest to realizowane w postaci wspólnych ćwiczeń dotyczących sposobu prowadzenia operacji koalicyjnych w ramach manewrów wojskowych oraz poszerzania międzynarodowych powiązań wojskowych
Uzyskanie doświadczenia bojowego przez jak najliczniejsze komponenty sił konwencjonalnych	Działanie określane jako „optymalizacja dyslokacji wojsk" miało na celu skierowanie w rejon działań bojowych jak największej liczby oddziałów. W tym celu stosowano rotacyjne rozmieszczanie oddziałów oraz rotację oficerów. To pozwoliło na uzyskanie przez znaczną część korpusu oficerskiego szczebla operacyjnego i taktycznego doświadczenia w sposobie planowania i prowadzenia działań w operacjach innych niż wojenne
Wykorzystanie doświadczeń w procesie szkolenia bojowego	Wnioski istotne dla procesu planowania i prowadzenia działań bojowych były na bieżąco weryfikowane w trakcie ćwiczeń, a następnie wkomponowywane w plany operacyjne. Należy się spodziewać, że część z nich zawiera obowiązujący *Plan obrony Federacji Rosyjskiej na lata 2021–2025* (obowiązuje od 1 I 2021 r.)
Zdolność do planowania i przeprowadzania operacji połączonych	W trakcie ćwiczeń zwracano szczególną uwagę na możliwości prowadzenia operacji na obszarze o skomplikowanej sytuacji polityczno-militarnej

Źródło: Opracowanie własne na podstawie: M.G. Bredesen, K. Friss, *Missiles*, *Vessels and Active Defence. What Potential Threat Do the Russian Armed Forces Represent?*, „The RUSI Journal" 2020, nr 5–6, s. 68–78, https://www.tandfonline.com/doi/full/10.1080/03071847.2020.1829991 [dostęp: 10 III 2021]; M. Clark, *The Russian Military's Lessons Learned In Syria*, Washington 2021, http://www.understandingwar.org/sites/default/files/The%20Russian%20Military%E2%80%99s%20Lessons%20Learned%20in%20Syria_0.pdf [dostęp: 10 III 2021]; D. Massicot, *Anticipating a New Russian Military Doctrine in 2020: What It Might Contain And Why It Matters*, War on the Rocks, 9 IX 2019 r., https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/ [dostęp: 10 III 2021]; В. Герасимов, *Векторы развития военной стратегии*, „Красная звезда", 4 III 2019 r., http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1 [dostęp: 1 V 2020].

Decydujący wpływ na skuteczną realizację koncepcji strategii aktywnej obrony mają zarówno umiejętne prowadzenie polityki międzynarodowej oraz rozbudowa potencjału bojowego, zwłaszcza zaawansowanych systemów uzbrojenia, jak i poziom wyszkolenia bojowego sił zbrojnych. Te wszystkie elementy zostały uwzględnione w strategii bezpieczeństwa i realizowanych programach[29]. W odniesieniu do sfery militarnej należy wskazać zapisy dotyczące wdrażanych programów modernizacyjnych, rozwojowych oraz reformy struktury organizacyjnej sił zbrojnych. Skutkiem podjętych działań miało być uzyskanie przez wszystkie siły zbrojne zdolności do prowadzenia

[29] Zob. szerzej: *Rosyjska myśl strategiczna i potencjał militarny*…

operacji zintegrowanych z wykorzystaniem różnych rodzajów sił zbrojnych i wojsk. Głównym czynnikiem determinującym te procesy jest założenie, że we współczesnych konfliktach o zwycięstwie decydują: poziom gotowości bojowej armii, zdolność do uzyskania przewagi informacyjnej i technologicznej oraz posiadanie możliwości precyzyjnego rażenia w trybie *stand-off* nie tylko sił nieprzyjaciela, lecz przede wszystkim elementów jego infrastruktury krytycznej. Oceniając ich zakres, trzeba wziąć pod uwagę rolę, jaką przypisano zmianom w systemie dowodzenia i kontroli nad siłami zbrojnymi. Wdrożono rozwiązania ujednolicające struktury dowodzenia na poziomie strategicznym i operacyjnym. Przekształcenia objęły również Sztab Generalny Sił Zbrojnych FR – zmieniono jego usytuowanie i zakres kompetencji[30]. Za istotne rozwiązanie należy uznać stworzenie (umownego) poziomu strategiczno-operacyjnego, który stanowi pięć dowództw pełniących w trakcie pokoju funkcję okręgów wojskowych. Podporządkowano im prawie wszystkie siły rozmieszczone na ich obszarze (związki operacyjne: wojsk lądowych, wojsk kosmicznych, marynarki wojennej oraz związki operacyjne i samodzielne oddziały specjalistycznych rodzajów wojsk, jak np. rozpoznania, dowodzenia i łączności, walki radioelektronicznej, wojsk specjalnych)[31]. Na poziomie taktycznym powrócono natomiast do formowania dywizji pancernych i zmechanizowanych, które miały stanowić uzupełnienie istniejących brygad. Ta decyzja jest elementem procesu wdrażania wniosków z doświadczeń wyniesionych z działań bojowych w Donbasie, zwłaszcza z działań batalionowych grup bojowych i brygad oraz ich ograniczonych możliwości przełamywania silnie umocnionych pozycji obronnych przeciwnika. Należy również zgodzić się z opinią amerykańskich analityków, że wspomniane rozwiązanie wynika także z oceny struktury organizacyjnej armii państw NATO[32]. Tego typu związek taktyczny dysponuje bowiem pewną przewagą technologiczną nad porównywalnymi związkami taktycznymi państw Sojuszu.

---

[30] Jako centralny organ dowodzenia odpowiada on także za koordynację działań z innymi podmiotami zewnętrznymi. W toku reorganizacji usprawniono przepływ informacji i proces podejmowania decyzji oraz doprecyzowano podział kompetencji, dzięki czemu zwiększyło się tempo podejmowania istotnych decyzji i ich realizacji w postaci konkretnych rozkazów. W strukturze Sztabu Generalnego SZ FR znalazł się m.in. Komitet Wojskowo-Naukowy, odpowiadający za koordynowanie zarówno systemu kształcenia i szkoleń, jak i prac naukowo-badawczych dotyczących bezpieczeństwa i obronności państwa.

[31] Wyjątkiem są dowództwa związków operacyjnych i taktycznych podległych bezpośrednio dowództwom, takim jak: Dowództwo Sił Specjalnych Operacji, Dowództwo Sił Powietrzno-Kosmicznych, Dowództwo Strategicznych Wojsk Rakietowych oraz Dowództwo Wojsk Powietrznodesantowych. W tych przypadkach podlegają one dowódcom operacyjno-strategicznym tylko w sprawach związanych z ich przebywaniem na danym obszarze. Zob. *Rosyjska myśl strategiczna i potencjał militarny*…

[32] C. Harris, F.W. Kagan, *Russia's Military Posture: Ground Forces Order of Battle*, Institute for the Study of War, Washington 2018, s. 8–18; *Западный военный округ*, https://web.archive.org/web/20170419224721/http://www.milkavkaz.net/2015/12/zapadnyj-voennyj-okrug.html [dostęp: 21 VII 2020]; *Powrót wielkich jednostek. Rosja formuje sztaby armii i korpusów [ANALIZA]*, Defence 24, 29 I 2017 r., https://www.defence24.pl/powrot-wielkich-jednostek-rosja-formuje-sztaby-armii-i-korpusow-analiza [dostęp: 21 VII 2020].

Zwłaszcza że – pomimo rozmaitych ograniczeń, głównie finansowych i logistycznych – w dużym stopniu przeprowadzono modernizację techniczną armii, priorytetowo traktując modernizację w Zachodnim Okręgu Wojskowym oraz Południowym Okręgu Wojskowym[33]. Mimo że nie udało się osiągnąć zakładanych wskaźników nasycenia (70 proc.) nowoczesnym sprzętem poszczególnych rodzajów sił zbrojnych i wojsk, to w trakcie realizacji programu ГПВ-2020 (ros. *Государственной программы вооружения на 2011–2020 годы*, pol. *Państwowy program uzbrojenia na lata 2011–2020*) poziom tego nasycenia wyniósł: 83 proc. w Strategicznych Siłach Nuklearnych, 75 proc. w Siłach Powietrzno-Kosmicznych, 63 proc. w Siłach Powietrznych i Marynarce Wojennej i 50 proc. w Wojskach Lądowych[34].

Po przeanalizowaniu powyższych danych można stwierdzić, że pomimo rozmaitych ograniczeń program został wdrożony. Istotniejsze jest jednak to, że w jego nowym wariancie – programie ГПВ-2027 (na lata 2021–2027) – uwzględniono istniejące zaległości, dostosowując go do rzeczywistego stanu modernizacji rodzajów sił zbrojnych i wojsk. W przeszłości takie podejście nie było oczywiste. Oceniając zakres reformy rosyjskich sił zbrojnych, należy również zwrócić uwagę na – pomijany w analizach – proces przeobrażeń systemu szkolnictwa wojskowego. Przede wszystkim utrzymano jego pionową strukturę (uczelnie wyższe – wojskowe szkoły średnie i wyspecjalizowane wojskowe szkoły średnie), ale znacznie zmniejszono liczbę szkół[35]. Zasadniczą zmianą była jednak gruntowna wymiana kadry dydaktycznej, jej uzupełnienie osobami z praktycznym doświadczeniem bojowym oraz ścisłe powiązanie zakresu prac badawczych z celami programów modernizacji sił zbrojnych oraz założeniami przyjętymi przez Sztab Generalny SZ FR. Uczelnie wojskowe sukcesywnie stają się ośrodkami dydaktycznymi ukierunkowanymi na wykształcenie oficera przygotowanego do działań zgodnych z przyjętymi scenariuszami wykorzystania sił zbrojnych oraz ośrodkami

---

[33] Jak podaje gen. Jarosław Stróżyk, na sfinansowanie programu ГПВ-2020 zostały przewidziane środki w wysokości 20,7 bln rubli (ok. 681 mld dolarów), z czego dla resortu obrony przeznaczono 19,4 bln rubli (ok. 638 mld dolarów). Dodatkowe 3 bln rubli (98,7 mld dolarów) przeznaczono na odbudowę parku maszynowego kompleksu wojskowo-przemysłowego. Należy się zgodzić z uwagą tego eksperta, że tzw. złota era modernizacyjna, trwająca ok. 30 lat, skończyła się w 2015 r., z chwilą zmniejszenia budżetu Ministerstwa Obrony Federacji Rosyjskiej, która to tendencja utrzymała się także w następnych latach. Zob. J. Stróżyk, *Ocena realizacji Programu Zbrojeń FR 2011–2020. Perspektywy modernizacji technicznej do 2025 roku*, s. 2–3, Fundacja Bezpieczeństwa i Rozwoju Stratpoints, https://www.stratpoints.eu/publikacje/ocena-realizacji-programu-zbrojen-fr-2011-2020-perspektywy-modernizacji-technicznej-do-2025-roku/ [dostęp: 10 VII 2020].

[34] Tamże. Dla przykładu, w 2019 r. na uzbrojenie wojsk lądowych i marynarki wojennej przewidziano ponad 1,5 biliona rubli (ponad 2 mld dolarów), a ponad 70% tych środków przeznaczono na zakup nowoczesnej seryjnej broni i sprzętu. Żołnierze otrzymali ponad 2300 jednostek nowego i zmodernizowanego sprzętu. W porównaniu z 2018 r. tempo podaży nowoczesnej broni wzrosło o 6,7%. Na rozwój infrastruktury w 2019 r. przeznaczono łącznie 168 mld rubli (2,372 mld dolarów).

[35] Obecnie (marzec 2021 r.) funkcjonuje: 28 wojskowych uczelni wyższych, 12 wojskowych szkół średnich (tzw. Federalne Suworowskie Szkoły Korpusu Kadetów) oraz 3 wojskowe wyspecjalizowane szkoły średnie. Zob. Ministry of Defence of the Russian Federation, Secondary Specialized Education, http://eng.mil.ru/en/education/specialized_secondary.htm [dostęp: 2 VIII 2020].

realizującymi badania dotyczące taktyki prowadzenia działań bojowych. Aktywność naukowo-badawcza jest koncentrowana na projektach związanych z nowymi formami prowadzenia działań bojowych, wyposażeniem bojowym żołnierza oraz z wymogami taktyczno-technicznymi dla nowego uzbrojenia[36].

Podsumowanie

Po przeanalizowaniu procesu ewoluowania rosyjskiej doktryny wojennej między rokiem 2013 a 2020 należy wskazać na zmianę statusu poszczególnych metod konfrontacji. W 2013 r. za wiodące uznano środki polityczne, ekonomiczne oraz informacyjne, które miały być uzupełniane przez środki militarne i te o charakterze niemilitarnym. W koncepcji obowiązującej od 2018 r. podstawą działań jest natomiast skoordynowane użycie środków wojskowych i pozamilitarnych, przy czym decydującą rolę odgrywają siły zbrojne. Uznanie, że podstawową formą współczesnego i przyszłego konfliktu polityczno-militarnego będzie konflikt nieliniowy o dynamicznym przebiegu, spowodowało, że ważną rolę przypisano możliwościom stosowania instrumentarium kinetycznego, niekinetycznego oraz operacjom specjalnym o kompleksowym charakterze. Zgodnie z tym założeniem konieczne stało się dostosowanie sposobu funkcjonowania systemu dowodzenia armią i przygotowanie dowódców do prowadzenia operacji połączonych, realizowanych przez kombinowane zgrupowania wojsk, jak również poszerzenie możliwości prowadzenia całościowego, zintegrowanego rażenia sił nieprzyjaciela. Doświadczenia płynące z działań w Donbasie i Syrii pokazały także, że posiadanie tego rodzaju uzbrojenia nie gwarantuje sukcesu prowadzonym operacjom i musi być połączone z umiejętnym dowodzeniem siłami oraz z ich wysoką gotowością bojową. Wnioski wyciągnięte z tych doświadczeń oraz przeanalizowanie trendów rozwojowych sił zbrojnych głównych rywali doprowadziły do gruntownej zmiany wizji reformy rosyjskiej armii, która nastąpiła w 2019 r. Jej najistotniejszym postulatem jest odejście od prymatu zsynchronizowanych działań niemilitarnych w ramach niekinetycznej operacji destabilizacyjnej. Główny sposób prowadzenia tego typu operacji został oparty na koncepcji skoordynowanego użycia środków wojskowych i pozamilitarnych, przy czym siły zbrojne odgrywają w nim rolę decydującą.

Bibliografia

Bredesen M.G., Friss K., *Missiles, Vessels and Active Defence. What Potential Threat Do the Russian Armed Forces Represent?*, „The RUSI Journal" 2020, nr 5–6, s. 68–78, https://www.tandfonline.com/doi/full/10.1080/03071847.2020.1829991 [dostęp: 10 III 2021].

[36] Oszacowanie jakości tego kształcenia jest trudne, gdyż brakuje dokładnych danych, a okres wdrażania nowych rozwiązań jest zbyt krótki.

Clark M., *The Russian Military's Lessons Learned In Syria*, Washington 2021, http://www.understandingwar.org/report/russian-military%E2%80%99s-lessons-learned-syria [dostęp: 10 III 2021].

Czaputowicz J., *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa 2008, Wydawnictwo Naukowe PWN.

Harris C., Kagan F. W., *Russia's Military Posture: Ground Forces Order of Battle*, Washington 2018, Institute for the Study of War.

Hoffman F., *Conflict in the 21st century: The rise of hybrid wars*, Arlington 2007, Potomac Institute for Policy Studies.

Kasprzycki D.D., *Militarny aspekt rosyjskiej obecności w Arktyce w kontekście regionalnego bezpieczeństwa do 2018 r.*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, nr 2, s. 190–216.

Keplin J., Pawlak C., *Hybrydowość wyzwaniem dla bezpieczeństwa przyszłości*, „Biuletyn CDiS SZ" 2016, nr 2, s. 5–7.

Kofman M., Rojansky M., *A Closer look at Russia's 'Hybrid War'*, „Kennan Cable" 2015, nr 7, https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf [[dostęp: 12 I 2021].

McCuen J.J., *Hybrid Wars*, „Military Review" 2008, nr 2, s. 107–113.

Mickiewicz P., *Rosyjska polityka arktyczna – próba zdominowania regionu czy instrument polityki bezpieczeństwa?*, w: *Geopolityka Rosji i obszaru postsowieckiego*, L. Sykulski (red.), Warszawa 2020, Zona Zero, s. 178–204.

Mickiewicz P., *W poszukiwaniu teoretycznych podstaw rosyjskiego myślenia strategicznego ery W. Putina*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, nr 2, s. 39–56.

Nemeth W.J., *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey 2002, Naval Postgraduate School.

Pawlak C., *Konflikt na wschodzie Ukrainy sztandarowym przykładem działań hybrydowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, nr 1, s. 268–287.

Pawlak C., Keplin J., *Aneksja Krymu w kontekście działań hybrydowych*, „Kwartalnik Bellona" 2016, nr 3, s. 23–32.

Rosyjska myśl strategiczna i potencjał militarny w XXI wieku, P. Mickiewicz (red.), Warszawa 2018, Wydawnictwo Naukowe PWN.

Wojciuk A., *Dylemat potęgi. Praktyczna teoria stosunków międzynarodowych*, Warszawa 2010, Wydawnictwa Uniwersytetu Warszawskiego.

Źródła internetowe

Massicot D., *Anticipating a New Russian Military Doctrine in 2020: What It Might Contain and Why It Matters*, War on the Rocks, 9 IX 2019 r., https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/ [dostęp: 10 III 2021].

Stróżyk J., *Ocena realizacji Programu Zbrojeń FR 2011-2020. Perspektywy modernizacji technicznej do 2025 roku*, https://www.stratpoints.eu/publikacje/ocena-realizacji-programu-zbrojen-fr-2011-2020-perspektywy-modernizacji-technicznej-do-2025-roku/ [dostęp: 10 VII 2020].

Sukhankin S., *"A black cat in the dark room". Russian Quasi-Private Military and Security Companies (PMSCs) – 'Non-existent,' but Deadly and Useful*, National Defence and the Canadian Armed Force, http://www.journal.forces.gc.ca/vol19/no4/page43-eng.asp [dostęp: 12 XII 2020].

Rosyjskie źródła internetowe

Чекинов С.Г., Богданов С.А., *Асимметричные действия по обеспечению военной безопасности России*, „Военная мысль" 2010, nr 3, s. 13–22, http://militaryarticle.ru/voennaya-mysl/2010-vm/10291-asimmetrichnye-dejstvija-po-obespecheniju-voennoj [dostęp: 10 X 2019].

Дульнев П.А., Ковалев В.Г., Ильин Л.Н., *Асимметричное противодействие в сетецентрической войне*, „Военная мысль" 2011, nr 10, s. 3–8, http://militaryarticle.ru/voennaya-mysl/2011-vm/10357-asimmetrichnoe-protivodejstvie-v-setecentricheskoj [dostęp: 11 X 2019].

Герасимов В., *Векторы развития военной стратегии*, „Красная звезда", 4 III 2019 r., http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1 [dostęp: 1 V 2020].

Сергей Шойгу рассказал, как спасали российскую, 22 IX 2019 r., https://www.mk.ru/politics/2019/09/22/sergey-shoygu-rasskazal-kak-spasali-rossiyskuyu-armiyu.html [dostęp: 22 IX 2019].

Указ Президента Российской Федерации N Пр-2976 от 25 декабря 2014 г. „Военная доктрина Российской Федерации", http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf [dostęp: 12 III 2021].

Abstrakt

W artykule opisano ewolucję rosyjskiej koncepcji działań militarnych jako formy realizacji polityki bezpieczeństwa. Przedstawiono istotne zmiany w koncepcji dotyczącej prowadzenia działań hybrydowych w stosunku do sposobu, w jaki je realizowano podczas aneksji Półwyspu Krymskiego oraz rosyjskiej interwencji w Syrii. Wykazano, że obowiązująca od 2018 r. koncepcja przebudowy sił zbrojnych ma na celu ich przygotowanie do realizacji zarówno tzw. operacji zintegrowanych, poszerzania zewnętrznej strefy obrony, jak i operacji o charakterze antydostępowym. Służyć temu ma wyposażenie sił zbrojnych w odpowiednie środki, umożliwiające wykonywanie tak sformułowanych zadań, oraz wdrożenie strategii aktywnej obrony, zakładającej podejmowanie przez Rosję działań wyprzedzających na podstawie precyzyjnych algorytmów planowania. Uzupełnieniem rosyjskiej strategii aktywnej obrony jest strategia działań ograniczonych. Zdaniem rosyjskich ekspertów powinna ona zakładać prowadzenie działań zewnętrznych w celu ochrony oraz promowania rosyjskich interesów za granicą. Z przeprowadzonych analiz wynika, że Rosjanie uznali, że podstawową formą konfliktu polityczno-militarnego zarówno obecnie, jak i w przyszłości będzie konflikt nieliniowy o dynamicznym przebiegu. W związku z tym ważną rolę przypisano możliwościom stosowania instrumentarium kinetycznego i niekinetycznego oraz operacjom specjalnym o kompleksowym charakterze. W celu realizacji tych planów gruntownie zreformowano siły zbrojne. Zmieniono strukturę organizacyjną, system szkolenia i zmodernizowano uzbrojenie. Najważniejszy etap reform został ukończony, pomimo sankcji, w grudniu 2020 r. Na zmiany wprowadzane w rosyjskiej doktrynie wojskowej miały wpływ doświadczenia płynące z działań w Syrii i Donbasie. Przede wszystkim nastąpiło odejście od prymatu zsynchronizowanych działań niemilitarnych w ramach niekinetycznej operacji destabilizacyjnej. Obecnie główny sposób prowadzenia operacji polega na skoordynowanym użyciu środków wojskowych i pozamilitarnych, przy czym siły zbrojne odgrywają w takich operacjach decydującą rolę.

Słowa kluczowe: A2/AD, Rosja, działania konwencjonalne, działania nieliniowe, działania zintegrowane, reforma, siły zbrojne, strategia, doktryna.

Evolving from hybrid conflict leading into conventional warfare? The Russian concept of military impact, with particular reference to the changes after 2018

Abstract

The article presents the evolution of the Russian idea of military operations as a form of implementing security policy. Significant changes in the concept of conducting hybrid operations were pointed out in relation to the way they were carried out in the process of the annexation of the Crimean Peninsula and during the Russian intervention in Syria. It was shown that the concept of the reconstruction of the armed forces since 2018 has been aimed at both preparing them for the implementation of the so-called integrated operations, expanding the external defence zone, and performing anti-access operations. This is to be achieved by adequately saturating the armed forces with the necessary means to conduct such a task and by practically implementing the active defence strategy, which assumes that Russia will take pre-emptive actions based on precise planning algorithms. The Russian strategy of active defence is complemented by a strategy of limited operations. According to Russian experts, this strategy should involve external actions to protect and promote Russian interests abroad. The analyses demonstrate that the Russians have decided that the basic form of contemporary and future political-military conflict will be a non-linear conflict with a dynamic course. That is why a key role has been assigned to both kinetic and non-kinetic instrumentation capabilities and special operations with a comprehensive scope. To implement these plans, a thorough reform of the armed forces was carried out in terms of restructuring the organization, reforming the training system and modernizing the armaments. The main phase of the reforms had been successfully implemented by December 2020, despite the sanctions. The experience of Syria and the Donbass influenced the transformation of the Russian military doctrine. Its most important assumption was to move away from the primacy of synchronized non-military actions within a non-kinetic destabilizing operation. The concept of coordinated use of military and non-military means with a decisive role of the armed forces has become the basic form of conducting operations of this type.

Keywords: A2/AD, Russia, conventional operations, nonlinear operations, integrated operations, reform, armed forces, strategy, doctrine.

DARIUSZ GRADZI
ORCID: 0000-0002-4612-0564

DOI: 10.4467/20801335PBW.21.020.14297

Najnowsze kierunki zmian regulacyjnych w zakresie walut wirtualnych z perspektywy przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, z uwzględnieniem wpływu pandemii COVID-19 na wzrost obrotu bezgotówkowego

W artykule zostanie zaprezentowany europejski i polski stan regulacji prawnych dotyczących kryptoaktywów (do których są zaliczane waluty wirtualne), obrotu nimi oraz zwalczania zjawisk prania pieniędzy i finansowania terroryzmu (procederów, w których bardzo często są używane kryptoaktywa).

W pierwszej kolejności zostanie omówiony wpływ pandemii COVID-19 na obrót bezgotówkowy. Następnie zostaną zaprezentowane definicje prawne kryptoaktywów, walut wirtualnych oraz próby uregulowania ich podaży. Regulacje dotyczące ochrony interesów użytkowników kryptowalut do tej pory pozostawały poza sferą zainteresowania przepisów prawa (dotychczas wydane przepisy koncentrowały się wyłącznie na przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu).

Przeprowadzenie tych analiz będzie miało na celu uzyskanie odpowiedzi na pytania, czy opisywane regulacje prawne dotyczące walut wirtualnych będą miały wpływ na dynamikę ich rozwoju oraz czy te regulacje wpłyną na koszty związane z podażą tych walut.

Można powiedzieć, że w ostatnich latach nic bardziej nie przyczyniło się do rozwoju i cyfrowej ekspansji technologicznej, w tym w obrocie bezgotówkowym, niż sytuacja wywołana ogólnoświatową pandemią COVID-19. Nie odnotowuje się jednak wpływu COVID-19 na powstawanie nowych regulacji związanych z przeciwdziałaniem praniu pieniędzy i finansowaniem terroryzmu, a zmiany prawne, z którymi mamy do czynienia, były już planowane przed pandemią. Wydana przez World Health

Organization[1] rekomendacja *COVID-19: physical distancing*[2], dotycząca wdrożenia tzw. dystansu społecznego (*physical distancing*[3]) powodowała natychmiastowe wprowadzanie rozwiązań, które przed pandemią przez wiele lat pozostałyby w sferze zamierzeń i pilotażu lub utknęłyby w tzw. piaskownicy regulacyjnej[4] (*regulatory sandbox*). Przedsiębiorstwa funkcjonujące w tradycyjnych modelach i nieprzystosowane do pracy zdalnej w zaledwie kilka tygodni były zdolne wdrożyć rozwiązania takie, jak m.in. ZOOM, chmura obliczeniowa w modelu SaaS (*Software as a Service*)[5], Google Hangouts czy Microsoft Teams, które wspierały ich pracowników w zdalnym wykonywaniu zadań.

Wzrost liczby płatności elektronicznych i płatności walutami wirtualnymi może powodować większe zainteresowanie grup przestępczych tymi obszarami, np. nielegalnym wydobywaniem walut wirtualnych[6], kradzieżą mocy obliczeniowej do tzw. *miningu*[7], stosowaniem oszustw socjotechnicznych (np. przez otwieranie fałszywych giełd kryptowalut, tworzenie fałszywych ofert emisji kryptowalut i podszywanie się sprawcy pod znane i renomowane podmioty)[8], atakami na infrastrukturę do zarządzania tokenami[9]. Na polskim

---

1 Wszelkie informacje dotyczące Covid-19 WHO publikuje na stronie: https://www.who.int [dostęp: 10 V 2021].

2 https://www.who.int/westernpacific/emergencies/covid-19/information/physical-distancing [dostęp: 10 V 2021].

3 Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

4 Zwrot oznacza testowanie innowacyjnych rozwiązań biznesowych pod nadzorem organów regulacyjnych. Celem jest przygotowanie tych rozwiązań do wejścia na prawdziwy rynek. Testy są wykonywane na klientach, co pozwala dopracować model biznesowy w środowisku zbliżonym do realnego. Zob. https://fintek.pl/co-to-jest-piaskownica-regulacyjna/ [dostęp: 10 V 2021].

5 Oprogramowanie używane jako usługa, umożliwiające odbiorcy usług korzystanie z aplikacji uruchomionych na infrastrukturze chmury dostarczonej przez dostawcę. Usługi są dostępne na różnych urządzeniach klienta za pośrednictwem aplikacji lub przeglądarek internetowych. Zob. https://pl.wikipedia.org/wiki/Oprogramowanie_jako_usługa [dostęp: 10 V 2021].

6 Należy zauważyć, że np. bitcoin nie może być przedmiotem przestępstwa z art. 310 kk (fałszowanie pieniędzy i innych środków płatniczych). Zob. Ł. Pasternak. *Kryptowaluta i pieniądz wirtualny jako przedmiot przestępstwa z art. 310 § 1 k.k*, „Prokuratura i Prawo" 2017, nr 4; J. Liberadzki. *Karnoprawne aspekty walut kryptograficznych (bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2019, z. 3, https://www.czpk.pl/index.php/zeszyty-archiwum/zeszyt-2019-3 [dostęp: 11 V 2021].

7 Proces wydobywania walut wirtualnych (bitcoin), które następnie są wprowadzane do obiegu, https://comparic.pl/wykopywanie-bitcoin/ [dostęp: 11 V 2021].

8 https://www.kaspersky.pl/o-nas/informacje-prasowe/2988/w-zeszlym-roku-socjotechnika-ukierunkowana-na-kryptowaluty-pomogla-cyberprzestepcom-zarobic-prawie-10-milionow-dolarow [dostęp: 28 VII 2021].

9 P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 42, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjN2tuP6MPwAhXgCRAIHWipCRUQFjABegQIBBAD&url=https%3A%2F%2Fpk.gov.pl%2Fwp-content%2Fupload-

rynku kapitałowym odnotowuje się zagrożenia związane z rynkiem kryptoaktywów, który nie podlega kontroli. Przykładem minimalizowania tego ryzyka jest inicjatywa realizowana przez Giełdę Papierów Wartościowych w Warszawie o nazwie „GPW Private Market", która dotyczy inwestowania w instrumenty finansowe oparte na technologii blockchain[10] i tokenach cyfrowych[11] przy udziale renomowanego partnera – GPW S.A. Statystyki pokazują, że w przypadku oszustw dokonywanych na niekorzyść inwestorów i użytkowników mamy do czynienia z olbrzymimi kwotami. W pierwszej połowie 2019 r. straty z tego tytułu wyniosły 4,26 mld dolarów[12]. Waluty wirtualne są m.in. używane przez południowoamerykańskie kartele narkotykowe do prania pieniędzy w Chinach oraz jako środek płatniczy za substancje odurzające i psychotropowe[13] w tzw. darkmarketach[14] i Darknecie[15].

W Polsce do przestępstw związanych z walutami wirtualnymi dochodzi najczęściej na giełdach kryptowalut. Polegają one na tradycyjnym inwestowaniu środków pozyskanych w nielegalny sposób (np. przez nieuprawniony dostęp do bankowości elektronicznej) w kryptowaluty, a następnie po ich wymianie na środki pieniężne – wpłacanie na rachunki tzw. słupów[16].

COVID-19 a polski system płatniczy[17] i waluty wirtualne

System płatniczy jest rozumiany jako pewna grupa podmiotów, instrumentów, procedur oraz systemów wykorzystywanych do zapewnienia obiegu pieniądza na danym obszarze geograficznym[18]. W ramach systemu płatniczego należy wyróżnić cztery kategorie uczestników[19]: kategoria pierwsza obejmuje podmioty będące stronami

s%2F2021%2F01%2F3opitek-poprawiony.doc&usg=AOvVaw3gTPSTRL7wRc_wWKuKPp7K [dostęp: 11 V 2021].

[10] https://blockgeeks.com/guides/what-is-blockchain-technology/ [dostęp: 10 V 2021]; https://pl.wikipedia.org/wiki/Blockchain [dostęp: 10 V 2021].

[11] https://blockgeeks.com/guides/what-is-blockchain-technology/ [dostęp: 10 V 2021]; https://www.gpw.pl/privatemarket [dostęp: 11 V 2021].

[12] P. Opitek, *Przeciwdziałanie praniu pieniędzy*…, s. 43.

[13] Tamże, s. 60.

[14] Miejsce nielegalnego handlu zabronionymi towarami, usługami w sieci Internet. Zob. https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down [dostęp: 11 V 2021].

[15] Sieć nakładkowa w Internecie, do której dostęp jest możliwy za pośrednictwem specjalnego oprogramowania. Zob. https://en.wikipedia.org/wiki/Darknet [dostęp: 11 V 2021].

[16] P. Opitek, *Przeciwdziałanie praniu pieniędzy*…

[17] *Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2020 r.*, Narodowy Bank Polski, październik 2020 r., https://www.nbp.pl/systemplatniczy/ocena/ocena2020_1.pdf [dostęp: 10 V 2021].

[18] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, s. 79.

[19] Tamże, s. 80.

dokonywanych transakcji płatniczych; kategoria druga to podmioty obsługujące procesowanie transakcji pomiędzy uczestnikami poziomu pierwszego (m.in. dostawcy usług płatniczych, tj. banki i instytucje płatnicze); kategoria trzecia to podmioty uczestniczące w rozliczaniu transakcji pomiędzy uczestnikami kategorii drugiej (np. Krajowa Izba Rozliczeniowa); kategoria czwarta obejmuje podmioty przechowujące środki pieniężne dostawców usług płatniczych lub papiery wartościowe (np. Narodowy Bank Polski oraz Krajowy Depozyt Papierów Wartościowych S.A.).

W pierwszym okresie pandemii można było zaobserwować zwiększenie wypłat gotówki. Wartość pieniądza gotówkowego w obiegu poza kasami banków wyniosła w tamtym czasie 283,2 mld zł, co stanowiło wzrost o 59,1 mld zł (wzrost o 26,4 proc.) w stosunku do 2019 r.[20] Dzienna wartość pobrań banknotów i monet z NBP w marcu 2020 r. w stosunku do marca 2019 r. wzrosła o 121,7 proc.[21]

W zakresie obrotu bezgotówkowego pandemia COVID-19 przyspieszyła wprowadzenie większego limitu transakcji zbliżeniowych (z 50 do 100 zł) bez konieczności wprowadzania kodu PIN (*Personal Identification Number*)[22], co było planowane jeszcze przed wystąpieniem pandemii. Kolejne restrykcje związane ze stanem pandemii, które ograniczały funkcjonowanie stacjonarnych podmiotów handlowo-usługowych, spowodowały wzrost zainteresowania transakcjami w Internecie oraz płatnościami za pośrednictwem Internetu.

Pandemia wpłynęła również na rozwój infrastruktury wykorzystywanej do obrotu bezgotówkowego. Liczba terminali POS (*point of sale*)[23] na koniec czerwca 2020 r. wzrosła o 7,5 proc. w stosunku do grudnia 2019 r. W tym samym okresie liczba punktów handlowych wyposażonych w terminal POS zwiększyła się o 707 tys. (wzrost o 10 proc.), liczba sklepów internetowych umożliwiających płatność kartą wzrosła o 8,8 proc. i wyniosła 55,8 tys., a liczba transakcji dokonywanych kartą w tych sklepach wzrosła o 6,7 proc. i wyniosła 66,7 mln. Jeszcze wyraźniej widać tę tendencję, gdy porówna się dane z końca czerwca 2020 r. z pierwszym półroczem 2018 r. – w tym czasie liczba transakcji w sklepach internetowych wzrosła o 97,9 proc. Liczba transakcji realizowanych kartą bez jej fizycznej obecności (*card non present*, CNP[24]) zwiększyła się w pierwszym półroczu 2020 r. o 35,7 proc. odpowiednio do analogicznego okresu

[20] *Ocena funkcjonowania polskiego systemu płatniczego*…, s. 6.

[21] Tamże, s. 19.

[22] Kod alfanumeryczny lub hasło służące do uwierzytelniania, używane najczęściej podczas wypłaty gotówki z bankomatu lub dokonania płatności w placówce handlowej (usługowej) za pomocą magnetycznej lub mikroprocesorowej karty płatniczej. Zob. https://pl.wikipedia.org/wiki/Osobisty_numer_identyfikacyjny [dostęp: 10 V 2021].

[23] Urządzenie instalowane w punktach handlowo-usługowych służące do dokonywania transakcji płatniczych przy udziale np. banku i agenta rozliczeniowego (*acquirer*), potocznie określane jako „terminal płatniczy". Zob. https://pl.wikipedia.org/wiki/Terminal_POS [dostęp: 10 V 2021].

[24] Przykładem są transakcje dokonywane kartą telefoniczną (*Mobile Order*), mailowo (*Mail Order*) lub internetowo (*Internet Order*). Zob. https://pl.wikipedia.org/wiki/Card_not_present [dostęp: 10 V 2021].

w 2019 r. i o 75,6 proc. – do tego samego okresu w 2018 r. Pomimo tych wzrostów odnotowano w tym czasie spadek liczby transakcji kartowych bezgotówkowych oraz ich wartości, która wyniosła 2,796 mld zł (spadek o 8 proc.)[25]. Można to tłumaczyć niechęcią społeczeństwa do wydawania pieniędzy w czasach pandemii.

Powyższe wzrosty mają bezpośrednie przełożenie na statystyki dotyczące oszustw dokonywanych instrumentami płatniczymi. W pierwszym półroczu 2020 r. liczba transakcji oszukańczych (nieuprawnionych)[26] zgłoszonych przez banki wyniosła 126,7 tys., z kolei dane zgłoszone przez agentów rozliczeniowych mówią o 17,6 tys. oszustw. Liczba transakcji oszukańczych dokonanych kartami w pierwszym półroczu 2020 r. (zgłoszonych przez banki) wzrosła o 11,4 proc. w porównaniu z drugim półroczem 2019 r. (113,7 tys. transakcji oszukańczych). Większość oszukańczych operacji kartowych odnotowanych w 2020 r. została zrealizowana kartami wydanymi w Polsce, ale przeprowadzono je poza terytorium kraju. Pomimo wzrostu liczby transakcji oszukańczych wartość kwotowa transakcji w tym okresie spadła o 5,6 proc. (z 27,2 mln zł do 25,6 mln zł)[27].

Według raportu Europejskiego Banku Centralnego (European Central Bank, ECB) w Polsce wciąż stwierdza się najniższy poziom oszustw, tzw. fraudów, w stosunku do ogólnej liczby i wartości transakcji kartowych[28].

Wpływ pandemii COVID-19 na rozwój obrotu bezgotówkowego potwierdzają także badania dotyczące zmian zwyczajów płatniczych konsumentów[29]. Świadczą o tym dane statystyczne: 38 proc. badanych respondentów potwierdziło, że w czasie pandemii częściej płaciło bezgotówkowo, 29 proc. częściej niż przed pandemią dokonywało transakcji w sklepach internetowych, a 65 proc. respondentów deklarowało utrzymanie tego trendu także po zakończeniu pandemii. Konkludując, 48 proc. respondentów potwierdziło, że pandemia miała bezpośredni wpływ na sposób dokonywania przez nich płatności w sklepach stacjonarnych. Badania przeprowadzono w drugiej połowie 2020 r.

---

[25] *Ocena funkcjonowania polskiego systemu płatniczego*…, s. 7.

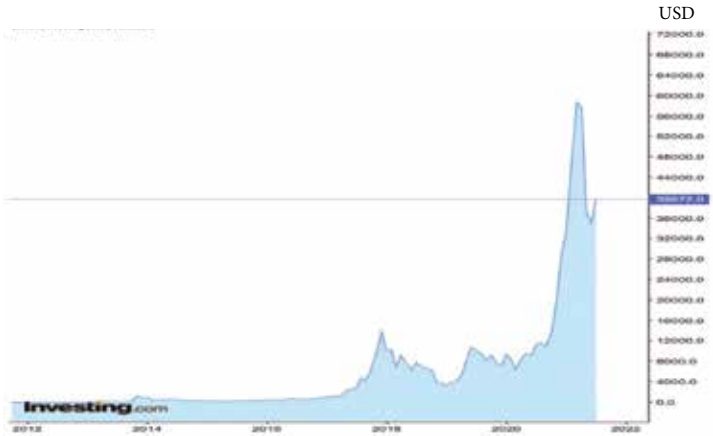
[26] https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty/informacje_kwartalne.html [dostęp: 10 V 2021]; *Informacja o kartach płatniczych IV kwartał 2020 r.*, Narodowy Bank Polski, kwiecień 2021 r., https://www.nbp.pl/systemplatniczy/karty/q_04_2020.pdf [dostęp: 10 V 2021].

[27] *Ocena funkcjonowania polskiego systemu płatniczego*…, s. 137.

[28] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html#toc12 [dostęp: 10 V 2021].

[29] Firma badawcza Polasik Research, www.polasik-research.pl. Zob. M. Polasik, *Jak bardzo Polska jest bezgotówkowa? Zwyczaje płatnicze a rozwój sieci akceptacji kart. Wybrane wyniki badań realizowanych na rzecz Programu Polska Bezgotówkowa* (prezentacja), https://www.cashlesscongress.pl/wp-content/uploads/2020/09/Dzie%C5%84-1-Micha%C5%82-Polasik-POLASIK-Research-Jak-bardzo-Polska-jest-bezgot%C3%B3wkowa.pdf [dostęp: 10 V 2021]; *Ocena funkcjonowania polskiego systemu płatniczego*…, s. 33.

Rynek walut wirtualnych to blisko 4 tys. cyfrowych monet i tokenów[30]. W przypadku walut wirtualnych rok 2020, mimo załamania w marcu[31], był dla bitcoina rekordowy, a jego cena wzrosła o 400 proc.[32] W grudniu 2020 r. odnotowano jedną z najwyższych zmian kursów walut wirtualnych, wartość niektórych z nich wzrosła o ponad 10 proc. Według badań 74 proc. respondentów potwierdziło, że planuje zainwestować więcej swoich środków finansowych w bitcoiny, a 47 proc. ankietowanych, którzy obecnie nie inwestują w tę kryptowalutę, mają zamiar to uczynić w 2021 r.[33] Podobnie sytuacja wygląda z innymi walutami wirtualnymi, jak bitcoin cash, ethereum, litecoin, ripple. Widoczne obecnie tendencje mogą doprowadzić do sytuacji, że coraz więcej niedoświadczonych inwestorów będzie angażowało swoje środki finansowe w tego typu inwestycje, zwłaszcza że mogą oni tego dokonać w bardzo prostu sposób, korzystając m.in. z aplikacji na smartfony (np. Revolut[34]).



Wykres. 1. Zmiany kursu bitcoina w stosunku do dolara w latach 2012–2021.

Źródło: https://pl.investing.com [dostęp: 10 V 2021].

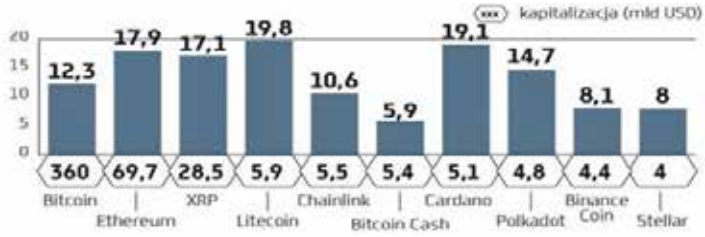
[30] https://www.parkiet.com/Profesjonalny-inwestor/312049991-Bitcoin-przy-cenowym-suficie-Przebije-go-czy-to-koniec-hossy.html?preview=&remainingPreview=&grantedBy=preview& [dostęp: 10 V 2021]. Termin „token" ma wiele znaczeń. Na potrzeby niniejszego artykułu autor przyjął, że jest to wirtualny żeton, który reprezentuje jakąś wartość. Zob. https://tokeny.pl/token/; https://e-kursy-walut.pl/warto-wiedziec/co-to-jest-token/ [dostęp: 10 V 2021].

[31] https://businessinsider.com.pl/finanse/kryptowaluty/kryptowaluty-traca-przez-koronawirusa-bitcoin-najtanszy-od-miesiecy/9xylt6e [dostęp: 10 V 2021].

[32] https://www.parkiet.com/Kryptowaluty/312179951-WykresDnia-Bitcoin-na-fali-Kryptowaluta-przebila-22-tys.html [dostęp: 10 V 2021].

[33] https://kryptobot.net/news/pandemia-covid-19-a-kryptowaluty/ [dostęp: 10 V 2021].

[34] https://www.revolut.com/pl-PL [dostęp: 10 V 2021].



Wykres. 2. Tygodniowa zmiana kursów najpopularniejszych kryptowalut w stosunku do dolara (w procentach). Stan na 3 grudnia 2020 r.

Źródło: https://www.parkiet.com/Profesjonalny-inwestor/312049991-Bitcoin-przy-cenowym-suficie-Przebije-go-czy-to-koniec-hossy.html?preview=&remainingPreview=&grantedBy=preview& [dostęp: 10 V 2021].

Waluty wirtualne – zagadnienia ogólne

Waluty wirtualne (*virtual currencies*, VC)[35] są produktami finansowymi tylko częściowo regulowanymi w UE, co może narażać klientów na ryzyko[36]. Europejski Urząd Nadzoru Bankowego (European Banking Authority, EBA[37]) od lat publikuje raporty wskazujące na zagrożenia związane z walutami wirtualnymi (takie jak: brak stabilności kursu, brak płynności)[38].

Europejski Bank Centralny definiuje kryptowaluty jako: (…) *cyfrowo prezentowaną wartość, która nie została wyemitowana przez bank centralny, instytucję kredytową, jak i instytucję pieniądza elektronicznego, która w pewnych okolicznościach może być wykorzystana jako alternatywa wobec pieniądza*[39]. Warto zaznaczyć, że ta definicja nie ma charakteru wiążącego państwa członkowskie UE, a wyłącznie pomocniczy.

---

[35] Zob. D. Gradzi, *FinTech/RegTech. Ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu wynikające z nowych technologii w obszarze płatności elektronicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, także: https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-14/1658,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-22-12-2020.html [dostęp: 10 V 2021].

[36] Zob. *Opinia EBA o walutach wirtualnych EBA z 4 lutego 2014 roku*, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [dostęp: 10 V 2021].

[37] https://www.eba.europa.eu [dostęp: 10 V 2021].

[38] Zob. http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies [dostęp: 10 V 2021]; http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+-Currencies.pdf [dostęp: 10 V 2021]; https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+t o+bring+virtual+currency+entities+into+the+scope+of+4AMLD [dostęp: 10 V 2021]; https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [dostęp: 10 V 2021].

[39] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 25.

Waluty wirtualne dzieli się na[40]:

- kryptowaluty,
- żetony – akceptowane głównie przez członków wirtualnych społeczności, które są emitowane i kontrolowane przez jego twórców, np. twórców gier komputerowych (Amazon Coins lub wycofane już żetony Facebook Credits).

Tym, co odróżnia waluty wirtualne od tradycyjnych walut fiat[41], jest model obrotu walutami[42]. Model ten dzieli się na:

- rozproszony. Nie występuje tu hierarchizacja, nie ma tu żadnej jednostki centralnej. Żadna z jednostek nie pozostaje wobec siebie w relacji: nadrzędność–podrzędność. Każdy uczestnik obrotu ma możliwość kontaktu z pozostałymi. Każdy uczestnik może być emitentem waluty, może nadzorować obrót oraz dysponować rejestrem wszystkich transakcji w systemie (ten system jest właściwy dla obrotu walutami wirtualnymi);
- scentralizowany. Istnieje jeden podmiot odpowiadający za emisję i kontrolę obrotu określoną walutą. Transakcje są realizowane wyłącznie za pośrednictwem tego podmiotu, podmiot zaś prowadzi rejestr wszystkich transakcji;
- zdecentralizowany. Podmiot centralny przekazuje podległym mu strukturom część kompetencji i zadań do wykonania.

Najbardziej rozpoznawalnym i medialnym przykładem waluty wirtualnej jest bitcoin. Założenia systemu Bitcoin zostały przedstawione w pracy pt. *Bitcoin: A Peer-to-Peer Electronic Cash System*, anonimowego autora występującego pod pseudonimem „Satoshi Nakamoto". Niektórzy uważają, że pod tym pseudonimem kryją się korporacje technologiczne: SAmsung, TOSHIba, NAKAmichi, MOTOrola[43]. Inne teorie mówią, że twórcą Bitcoina był Elon Musk[44] lub Nick Szabo[45]. Twórca lub twórcy systemu Bitcoina do dziś pozostają niezidentyfikowani.

Zastosowanie systemu Bitcoin[46] miało pozwalać na realizowanie bezpośrednich i anonimowych transakcji w handlu elektronicznym. Miał on być niezależny od tradycyjnych instytucji finansowych, a operacje finansowe miały się odbywać w izolacji od ogólnoświatowych systemów finansowych oraz centralnych systemów rozliczeniowych[47]. David Chaum, uznawany za „ojca pieniądza elektronicznego i anonimowości w Internecie"[48] zauważył, że konieczne jest ograniczenie wiedzy

---

[40] Tamże, s. 15.

[41] Pieniądz fiducjarny (łac. *fides* – wiara), legalny środek płatniczy. Zob. https://academy.binance.com/pl/articles/what-is-fiat-currency [dostęp: 10 V 2021].

[42] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 19.

[43] Tamże, s. 34–37.

[44] https://pl.wikipedia.org/wiki/Elon_Musk [dostęp: 29 VII 2021].

[45] https://en.wikipedia.org/wiki/Nick_Szabo [dostęp: 29 VII 2021].

[46] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 34–37.

[47] Szerzej: D. Gradzi, *FinTech/RegTech. Ryzyko związane z praniem pieniędzy*…

[48] Tamże, s. 30.

pośrednika finansowego co do czasu, miejsca, wartości i przedmiotu dokonywanej płatności, a także ograniczenie (uniemożliwienie) mu analizy zbyt wielu metadanych (*big data*[49]). Dane sensytywne (wrażliwe) powiązane z dokonywaną płatnością są zbędne dla pośrednika finansowego, zwłaszcza gdy dotyczą: lokalizacji osoby, jej stylu życia (płatności dokonywanych podczas podróży, np. za hotel, w restauracji, za żywność, leki, prasę), wsparcia instytucji politycznych i religijnych. Obecnie wszystkie te dane są przetwarzane przez pośredników finansowych i nie budzi to większej refleksji osób korzystających z nowych technologii[50]. Z drugiej jednak strony powyższe dane są niezbędne i wykorzystywane przez większość systemów do wykrywania oszustw płatniczych oraz przeciwdziałania praniu pieniędzy (*anti money laundering*, AML) i zwalczania finansowania terroryzmu (*counter terrorist financing*, CTF).

Waluty wirtualne a pieniądz elektroniczny[51]

Waluty wirtualne są potocznie mylnie utożsamiane z tzw. pieniądzem elektronicznym[52]. Różnica między walutami wirtualnymi a pieniądzem elektronicznym poza sferą regulacyjną[53] sprowadza się do tego, że waluta wirtualna jest sztuczną jednostką rozliczeniową, a jednostka rozliczeniowa pieniądza elektronicznego jest wyrażona w jednostce mającej status prawnego środka płatniczego (*fiat currency*).

Czynnikiem wyróżniającym technologicznie kryptowaluty jest otwartość kodu źródłowego, tzw. otwarte oprogramowanie (*open source*)[54].

Za zakwalifikowaniem danego instrumentu do kryptowalut przemawia:

- zastosowanie rozproszonego systemu transakcji,
- oparcie konstrukcji na kryptografii.

---

[49] Używanie zaawansowanych technik w celu analizowania dużych zasobów zdywersyfikowanych danych, które mogą nie być ustrukturyzowane i mogą pochodzić z różnych źródeł. Zob. https://www.ibm.com/analytics/hadoop/big-data-analytics [dostęp: 10 V 2021].

[50] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 30–31.

[51] Komisja Nadzoru Finansowego w piśmie do banków z 10 VII 2015 r. przedstawiła wyniki analizy prawnej dotyczącej emisji pieniądza elektronicznego. Zob. https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 10 V 2021].

[52] W rozumieniu *Ustawy z dnia 19 sierpnia 2011* r. *o usługach płatniczych* (t.j.: DzU z 2020 r. poz. 794, ze zm.) oraz *Dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE* (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

[53] Art. 2 ust. 2 pkt 26) lit c) *Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (t.j.: DzU z 2021 r. poz. 1132, ze zm.) wprost stanowi, że waluta wirtualna nie jest pieniądzem elektronicznym.

[54] Produkty, które zezwalają na używanie ich kodu źródłowego. Zob. https://pl.wikipedia.org/wiki/Otwarte_oprogramowanie [dostęp: 10 V 2021].

Warunkiem jest też istnienie globalnej, publicznej oraz rozproszonej bazy danych obejmującej transakcje zrealizowane przy użyciu kryptowaluty.

Bitcoin umożliwia przeprowadzanie bezpośrednich transakcji pomiędzy użytkownikami Internetu przez wykorzystanie protokołu komunikacyjnego *peer-to-peer*[55]. Oznacza to brak konieczności funkcjonowania centralnego serwera (repozytorium informacji o transakcjach) oraz brak potrzeby korzystania z pośrednika transakcji[56]. Nie występuje pośrednictwo tzw. zaufanej trzeciej strony. W ramach systemu Bitcoin nie funkcjonuje żadna jednostka centralna ani żaden organ nadzorczy, z zastrzeżeniem regulacji wprowadzonych przez V Dyrektywę AML[57] (dalej: AMLD5) i polskie przepisy implementujące tę dyrektywę, a także regulacji zawartych w projekcie rozporządzenia w sprawie rynku kryptoaktywów (*Markets in Crypto-Asssets*, MiCA, dalej: rozporządzenie MiCA[58]), o których jest mowa dalej.

Transakcje dokonywane kryptowalutami bitcoin są odnotowywane w blokach, które następnie łączą się w rejestr zatwierdzonych transakcji – blockchain. Tworzą one publiczną księgę (bazę danych) przechowywaną przez wszystkie komputery użytkowników sieci Bitcoin, tzw. *public ledger*. W łańcuchu bloków funkcjonujących w ramach publicznego rozproszonego rejestru transakcji w systemie Bitcoin nie jest możliwe wycofanie transakcji, co jest korzystne dla akceptantów płatności (np. sklepu przyjmującego płatność w kryptowalucie), ale może być ryzykowne dla płatnika[59].

Regulacje prawne dotyczące walut wirtualnych – nowe trendy regulacyjne AML/CTF

Wśród nowych regulacji w zakresie AML/CTF dotyczących walut wirtualnych należy wyróżnić:

- *Ustawę z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw*[60],

[55] Oznacza równorzędność uczestników sieci, tj. każdy komputer podłączony do sieci może wysyłać i odbierać dane w sieci, co umożliwia pobieranie plików oraz ich udostępnienie komputerom podłączonym do tej sieci. Zob. https://poradnikprzedsiebiorcy.pl/-peer-to-peer-definicja-historia-powstania-i-wplyw-na-rozwoj-internetu-cz-1 [dostęp: 10 V 2021].

[56] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 35.

[57] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE* (Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

[58] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie rynku kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937* – projekt, https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0014.02/DOC_1&format=PDF [dostęp: 13 V 2021].

[59] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowania*…, s. 51–53.

[60] DzU z 2021 r. poz. 815, ze zm.

implementującą do polskiego porządku prawnego AMLD5 (dalej: znowelizowana ustawa AML);
- pakiet finansów cyfrowych przyjęty przez Komisję Europejską 24 września 2020 r.[61], na który składa się:
  – strategia finansów cyfrowych,
  – strategia płatności detalicznych,
  – propozycje ustawodawcze co do unijnych ram regulacyjnych dotyczących kryptoaktywów i operacyjnej odporności cyfrowej.

Aspekty prawne zarządzania ryzykiem związanym z praniem pieniędzy i finansowaniem terroryzmu są regulowane w UE za pomocą dyrektyw[62]. Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu (*terrorist financing*, TF) aktualnie jest normowane przez AMLD5, która zmieniła IV Dyrektywę AML (dalej: AMLD4)[63]. W dyrektywach AML są zawarte przepisy kompleksowej integracji systemu AML/CTF z międzynarodowymi standardami zwalczania prania pieniędzy i finasowania terroryzmu, przyjętymi przez FATF (Financial Action Task Force)[64].

W AMLD4 przyjęto jako zasadę podejście oparte na ryzyku (*risked-based approach*)[65]. Ryzyko ML/TF jest różne w poszczególnych krajach. Z tego powodu poszczególne kraje i ich organy nadzorcze (*competent authotities*, CA) oraz uczestnicy obrotu prawnego muszą je zidentyfikować oraz nimi zarządzać, tj. podejmować odpowiednie i adekwatne środki prawne.

W dniu 30 maja 2018 r. została uchwalona V Dyrektywa AML z datą implementowania przez państwa członkowskie UE do 10 stycznia 2020 r.[66] Ustawa implementująca AMLD5 została uchwalona przez Sejm RP 30 marca 2021 r. i podpisana przez prezydenta 8 kwietnia 2021 r.[67]. Ustawa weszła w życie w całości w 2021 r.

---

[61] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en [dostęp: 10 V 2021].

[62] Dyrektywa Unii Europejskiej – akt prawa pochodnego Unii Europejskiej, na podstawie którego prawodawcy państw członkowskich UE zostają zobowiązani do wprowadzenia (transpozycji) określonych regulacji prawnych, służących osiągnięciu celu wskazanego w dyrektywie. Zob. https://pl.wikipedia.org/wiki/Dyrektywa_(Unia_Europejska).

[63] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE* (tj.: Dz. Urz. UE L 141/73 z 5 VI 2015 r., s. 73).

[64] Międzynarodowa organizacja, znana także jako Groupe d'action financiere (GAFI), licząca 39 członków, założona w 1989 r. w celu rozwoju praktyk zwalczanie prania pieniędzy. FATF publikuje w powyższym zakresie rekomendacje. Polska nie jest członkiem FATF, ale stosuje się do jej rekomendacji i aspiruje do członkostwa. Zob. http://www.fatf-gafi.org/about/ [dostęp: 10 V 2021].

[65] Działanie oparte na ryzyku.

[66] *Dyrektywa PE i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego*…, s. 43.

[67] Patrz przypis 60 (przyp. red.).

W dyrektywie AMLD5 wprowadzono definicję legalną walut wirtualnych, określając je jako cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny i nie muszą być powiązane z walutą prawnie obowiązującą, a także nie mają prawnego statusu waluty lub pieniądza, lecz są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną. W Polsce obowiązuje definicja walut wirtualnych określona w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[68] (dalej: ustawa AML). Pod pojęciem „waluty wirtualne" rozumie się cyfrowe odwzorowanie wartości, które nie jest:

- prawnym środkiem płatniczym emitowanym przez zagraniczne banki centralne lub inne organy administracji publicznej,
- międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
- pieniądzem elektronicznym w rozumieniu ustawy o usługach płatniczych,
- instrumentem finansowym w rozumieniu ustawy o obrocie instrumentami finansowymi,
- wekslem lub czekiem,

oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany.

Waluty wirtualne zalicza się do tzw. wartości majątkowych[69], do których należą także prawa majątkowe, inne mienie ruchome lub nieruchomości, środki płatnicze, instrumenty finansowe w rozumieniu ustawy o obrocie instrumentami finansowymi, inne papiery wartościowe oraz wartości dewizowe.

Regulacje AML/CTF dotyczą wyłącznie tzw. instytucji obowiązanych, za które na gruncie ustawy AML[70] (w zakresie istotnym z punktu widzenia przedmiotu niniejszego opracowania) uznaje się m.in.:

- podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług:
  - wymiany między walutami wirtualnymi a środkami płatniczymi,
  - wymiany między poszczególnymi walutami wirtualnymi,
  - pośrednictwa w wymianach, o których mowa powyżej,
  - prowadzenia rachunków[71];
- banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, instytucje finansowe mające siedzibę na terytorium RP;

[68] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, art. 2 ust. 1 pkt 26.

[69] Tamże, art. 2 ust. 2 pkt 27.

[70] Tamże, art. 2 ust. 1.

[71] Tamże, art. 2 ust. 2 pkt 17 lit. e. W wymienionym artykule zdefiniowano rachunek jako prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji wymiany.

- spółdzielcze kasy oszczędnościowo-kredytowe oraz Krajową Spółdzielczą Kasę Oszczędnościowo-Kredytową;
- krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego, oddziały unijnych instytucji płatniczych, oddziały unijnych i zagranicznych instytucji pieniądza elektronicznego, małe instytucje płatnicze, biura usług płatniczych oraz agentów rozliczeniowych;
- firmy inwestycyjne, banki powiernicze;
- zagraniczne osoby prawne prowadzące na terytorium RP działalność maklerską;
- spółki prowadzące rynek regulowany;
- fundusze inwestycyjne, alternatywne spółki inwestycyjne, towarzystwa funduszy inwestycyjnych, zarządzających alternatywnymi spółkami inwestycyjnymi;
- zakłady ubezpieczeń;
- Krajowy Depozyt Papierów Wartościowych S.A.;
- przedsiębiorców prowadzących działalność kantorową;
- przedsiębiorców, niebędących innymi instytucjami obowiązanymi, świadczących usługi polegające na:
  - tworzeniu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej,
  - pełnieniu funkcji członka zarządu bądź umożliwianiu innej osobie pełnienia tej funkcji, podobnej funkcji w osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - zapewnianiu siedziby, adresu prowadzenia działalności lub adresu korespondencyjnego oraz innych pokrewnych usług osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - działaniu lub umożliwieniu działania innej osobie jako powiernik trustu, który powstał w drodze czynności prawnej,
  - działaniu lub umożliwieniu innej osobie działania jako osoba wykonująca prawa z akcji lub udziałów na rzecz podmiotu innego niż spółka notowana na rynku regulowanym podlegającym wymogom dotyczącym ujawniania informacji zgodnie z prawem UE lub podlegająca równoważnym standardom międzynarodowym,
- fundacje, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- stowarzyszenia posiadające osobowość prawną, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- przedsiębiorców, w zakresie, w jakim przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- instytucje pożyczkowe.

Na podstawie wspólnej opinii Europejskich Organów Nadzorczych (European Supervisory Authorities, ESA)[72] dotyczącej różnych rodzajów ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, mających wpływ na sektor finansowy UE, wspólnych dla wszystkich sektorów finansowych UE, można wyróżnić m.in.[73]:

- ryzyko związane z rozwojem nowych technologii (*new technologies risk*),
- ryzyko związane z walutami wirtualnymi (*virtual currencies risk*),
- ryzyko związane z rozbieżnością legislacyjną państw UE oraz odmiennymi praktykami nadzoru (*legislative divergence risk and divergnet supervisory practices risk*),
- ryzyko związane ze słabością kontroli wewnętrznej (*weaknesses in internal controls risk*),
- ryzyko związane ze zjawiskiem de-riskingu (*de-risking risk*)[74],
- ryzyko związane z finansowaniem terroryzmu (*terrorist financing risk*).

Nie można definiować walut wirtualnych bez przybliżenia pojęć „FinTech" oraz „RegTech", które od wielu lat są obecne w sferze finansów cyfrowych. Z tymi zagadnieniami, stosownie do wspólnej opinii Europejskich Organów Nadzorczych[75], wiążą się określone ryzyka wpisane w rozwój nowych technologii[76].

Wśród rozwiązań fintechowych należy wyróżnić:

- usługi online – pożyczki lub *faktoring* online, aplikacje do oceny zdolności kredytowej (płatniczej) klienta. Wspomniana ocena odbywa się elektronicznie i zdalnie, a dostawcy tych usług korzystają z baz danych biur informacji gospodarczej, portali społecznościowych typu Facebook, LinkedIn lub Instagram;
- aplikacje mobilne[77] dla banków.

FinTech[78] jest definiowane jako stosowanie rozwiązań technologicznych w innowacjach finansowych, prowadzące do powstania nowych modeli biznesowych

---

[72] Na ESA składają się: European Securities & Markets Authority (ESMA) – europejski nadzór giełd i papierów wartościowych, European Insurance & Pensions Authority (EIOPA) – europejski nadzór ubezpieczeniowy i emerytalny oraz European Banking Authority (EBA) – europejski nadzór bankowy.

[73] *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, s. 1, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 10 V 2021].

[74] „*De-risking*" to ograniczenie lub całkowite zaprzestanie przez instytucje obowiązane prowadzenia działalności generującej obowiązki na podstawie AMLD4, co w praktyce oznacza odmowę świadczenia usług podmiotom z obszarów, na których występuje zwiększone ryzyko ML i TF.

[75] *Joint Opinion of the European Supervisory Authorities*…, s. 12.

[76] Na temat ryzyka związanego z wprowadzaniem nowych technologii w firmach działających wyłącznie w sieci (tzw. fintechów) zob. D. Gradzi, *FinTech/RegTech. Ryzyko związane z praniem pieniędzy*… (przyp. red.).

[77] Aplikacje płatnicze do integracji z urządzeniami mobilnymi (np. telefon, iPad).

[78] Zob. *Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention*, raport Financial Stability Board (FSB) w sprawie implikacji FinTechu dla

(np. systemu płatności BLIK[79], systemów płatności na urządzeniach mobilnych: Apple Pay, Google Pay, Samsung Pay[80]). Najważniejszymi podmiotami fintechowymi, które mają siedzibę w Polsce, są: PayU, Blue Media, Polish Payment Standard – Polski Standard Płatności (BLIK), CurrencyOne, Finanteq, VoicePIN, ZenCard. Wśród zagranicznych podmiotów należy wskazać Revolut[81] oraz N26[82].

RegTech[83] to wykorzystanie nowych technologii do wsparcia i spełnienia wymogów regulacyjnych[84]. Narzędzia RegTech[85] służą przede wszystkim do analizy danych, umożliwiają podmiotom szybsze, tańsze i łatwiejsze ich gromadzenie oraz analizowanie[86]. Ma to szczególne znaczenie przy zwalczaniu prania pieniędzy i finansowania terroryzmu dzięki zwiększeniu transparentności operacji finansowych. Przykładem stosowania narzędzia RegTech jest zautomatyzowana weryfikacja list osób zajmujących eksponowane stanowisko polityczne (*politically exposed person*, PEP), do których, zgodnie z AMLD5, zalicza się m.in. prezydentów, premierów, posłów, ministrów i ich rodziny.

Strategia finansów cyfrowych (pakiet finansów cyfrowych, *Digital Finance Package*)

W pakiecie finansów cyfrowych[87] przedstawiono kierunki działań UE w odniesieniu do technologii FinTech. Przepisy unijne mają być adaptowane do wymogów stawianych przez nowe technologie. Transformacja cyfrowa powinna się zakończyć do 2024 r., m.in. dzięki adaptacji rozwiązań opartych na sztucznej inteligencji (*artificial intelligence*, AI) i rozproszonych rejestrach (jednym z przykładów takich rejestrów jest

stabilności finansowej, 27 VI 2017 r., https://www.fsb.org/wp-content/uploads/R270617.pdf, s. 33 [dostęp: 10 V 2021].

79 https://blikmobile.pl [dostęp: 10 V 2021].

80 Są to płatności dokonywane przy użyciu mobilnego urządzenia wyposażonego w system operacyjny, z multimedialnym interfejsem z wykorzystaniem technologii radiowej, bezprzewodowych sieci telekomunikacyjnych (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth). Zob. https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [dostęp: 10 V 2021].

81 https://www.revolut.com/pl-PL [dostęp: 10 V 2021].

82 https://n26.com/en-eu [dostęp: 10 V 2021].

83 Zob. *Financial Stability Implications from FinTech*…, s. 34.

84 Definicja RegTech została opracowana przez Międzynarodowy Instytut Finansów (Institute of International Finance). Zob. https://www.iif.com/Innovation/Regtech [dostęp: 10 V 2021].

85 http://fintechpoland.com/raport-regtech-znaczenie-innowacji-regulacyjnych-dla-sektora-finansowego-i-panstwa/ [dostęp: 11 V 2021].

86 https://medium.com/blog-transparent-data/co-to-jest-regtech-i-jak-ma-się-do-fintech-f27bab5a3a55 [dostęp: 10 V 2021].

87 Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych*, Bruksela, 24 IX 2020 r., COM(2020) 591 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591 [dostęp: 10 V 2021].

blockchain). Założeniem strategicznym jest upowszechnienie zarządzania finansami korzystnego dla konsumentów i przedsiębiorstw oraz wdrożenie solidnych ram prawnych, które umożliwią wykorzystanie interoperacyjnych rozwiązań w zakresie tożsamości cyfrowych. Dzięki nim konsument uzyska łatwiejszy dostęp do usług finansowych (tzw. *onboarding*[88]).

W ramach strategii położono nacisk na cztery priorytety:

- zapewnienie, aby uchwalane regulacje ułatwiały, a nie blokowały rozwijanie innowacji cyfrowych,
- wyeliminowanie rozdrobnienia jednolitego rynku cyfrowego usług finansowych,
- sprostanie zagrożeniom i wyzwaniom dotyczącym transformacji cyfrowej,
- utworzenie europejskiego obszaru danych finansowych służącego promowaniu innowacji opartych na danych, w tym zwiększenie dostępu do danych i udostępnianie danych w ramach sektora finansowego.

Strategię należy ocenić pozytywnie w zakresie, w jakim próbuje ona zestandaryzować dla UE problematykę finansów cyfrowych (zwłaszcza cyfrowej tożsamości i identyfikacji).

Strategia płatności detalicznych

Priorytetem UE w strategii płatności detalicznych[89] jest zwiększenie szybkości płatności detalicznych bezgotówkowych. Płatności natychmiastowe mają być standardem w transakcjach płatniczych. W tym celu niezbędne jest spowodowanie wzrostu zaufania konsumentów do tego rodzaju płatności oraz wykorzystanie potencjału identyfikacji elektronicznej do celów uwierzytelnienia klienta.

Wymieniona strategia nie ma bezpośredniego wpływu na kryptowaluty, ogranicza się wyłącznie do wskazania, że ich rola będzie rosła i będą stanowić konkurencję dla tradycyjnych środków płatniczych (waluty wymienialne) i metod płatności (przelew bankowy, karta płatnicza). Należy stwierdzić, że im bardzie będziej popularyzowany obrót kryptowalutami przy płatnościach detalicznych, tym szybciej zajdzie konieczność zmiany tej strategii i ujęcia w niej aspektu kryptowalut.

Rozporządzenie MiCA – propozycje regulacyjne

Wspomniane rozporządzenie jest pierwszą próbą unormowania problematyki dotyczącej dóbr opartych na technologii rozproszonych rejestrów (*distributed ledger technology*, DLT) oraz metod pozyskiwania kapitału w postaci aktywów wirtualnych

[88] Nawiązywanie relacji biznesowej z nowym klientem.

[89] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie unijnej strategii w zakresie płatności detalicznych*, Bruksela, 24 IX 2020 r., COM(2020) 592 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0592 [dostęp: 10 V 2021].

(np. *Initial Coin Offering,* ICO). Obecnie każde z państw UE reguluje tę materię odrębnie. Wspólnym mianownikiem jest pomijanie zagadnień dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, które są normowane przez UE dyrektywami AML. Taka sytuacja powoduje, że podmioty prowadzące działalność związaną z obrotem kryptoaktywami funkcjonują prawnie w sprzyjających im jurysdykcjach prawnych (Estonia, Litwa, Malta)[90].

Rozporządzenie MiCA odnosi się do[91]:

- wymogów dotyczących przejrzystości i ujawniania informacji w odniesieniu do emisji kryptoaktywów i dopuszczania kryptoaktywów do obrotu,
- udzielania zezwolenia dostawcom usług w zakresie kryptoaktywów, emitentom tokenów powiązanych z aktywami oraz emitentom tokenów będących pieniądzem elektronicznym,
- sprawowania nadzoru nad powyższymi emitentami,
- emitentów tokenów powiązanych z aktywami, emitentów tokenów będących pieniądzem elektronicznym oraz dostawców usług w zakresie kryptoaktywów, pod kątem ich działalności, organizacji ich działań i stosowanych przez nich zasad zarządzania,
- przepisów dotyczących ochrony konsumentów inwestujących w kryptokatywa,
- środków zapobiegania nadużyciom na rynku kryptoaktywów.

Rozporządzenie MiCA wprowadza także definicję usług związanych z kryptoaktywami, przez które rozumie się jakiekolwiek usługi lub działalności związane z kryptoaktywami, m.in.:

- przechowywanie kryptoaktywów i zarządzanie nimi w imieniu osób trzecich,
- prowadzenie platformy obrotu kryptoaktywami,
- wymianę kryptoaktywów na walutę fiat będącą prawnym środkiem płatniczym,
- wymianę kryptoaktywów na inne kryptoaktywa,
- wykonywanie zleceń związanych z kryptoaktywami osób trzecich,
- subemisję kryptoaktywów,
- przyjmowanie i przekazywanie w imieniu osób trzecich zleceń związanych z kryptoaktywami,
- doradztwo w zakresie kryptoaktywów.

Zgodnie z rozporządzeniem MiCA „kryptoaktywo" to cyfrowe odzwierciedlenie wartości lub praw, które można przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii. Obecnie na rynku wśród najpopularniejszych kryptoaktywów należy wyróżnić m.in. waluty wirtualne (bitcoin, ethereum)[92].

---

[90] https://www.parp.gov.pl/component/content/article/68825:rozporzadzenie-MiCA-nowe-mozliwosci-dla-innowacyjnych-przedsiebiorstw#_edn5 [dostęp: 10 V 2021].

[91] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie rynku kryptoaktywów*…, art. 1.

[92] https://www.parp.gov.pl/component/content/article/68825:rozporzadzenie-MiCA-nowe-mozliwosci-dla-innowacyjnych-przedsiebiorstw#_edn5 [dostęp: 10 V 2021].

W rozumieniu rozporządzenia MiCA technologia rozproszonego rejestru to rodzaj technologii wspierającej rozproszone rejestrowanie zaszyfrowanych danych. W rozporządzeniu MiCA podzielono kryptoaktywa na trzy kategorie (zaszeregowanie do określonej kategorii pociąga za sobą zróżnicowane wymagania formalne):

- tokeny użytkowe – rodzaj kryptoaktywów, które mają zapewnić dostęp cyfrowy do danego towaru lub usługi; są one dostępne w technologii rozproszonego rejestru, akceptowane wyłącznie przez emitenta tego tokena;
- tokeny powiązane z aktywami – rodzaj kryptoaktywów, które mają utrzymywać stabilną wartość dzięki temu, że są powiązane z:
  – wartością kilku walut fiat będących prawnymi środkami płatniczymi,
  – wartością co najmniej jednego towaru,
  – wartością co najmniej jednego kryptoaktywa lub połączenia takich aktywów;
- tokeny będące e-pieniądzem – rodzaj kryptoaktywów, które mają być wykorzystywane głównie jako środek wymiany; mają one utrzymywać stabilną wartość dzięki temu, że są powiązane z walutą fiat będącą prawnym środkiem płatniczym.

Głównym celem wprowadzenia rozporządzenia MiCA jest zapewnienie bezpieczeństwa i transparentności dla użytkowników kryptoaktywów, dlatego na ich emitentów oraz przedsiębiorców świadczących usługi związane z obrotem nimi nałożono określone obowiązki.

Jednym z podstawowych założeń rozporządzenia MiCA jest wprowadzenie wymogu oferty publicznej[93] przy oferowaniu kryptoaktywów, od której mogą zaistnieć odstępstwa. W zależności od rodzajów tokenów rozporządzenie MiCA nakłada różne obowiązki na ich emitentów. Wspólnym obowiązkiem wszystkich emitentów będzie podanie do publicznej wiadomości dokumentu zawierającego podstawowe i najważniejsze informacje dotyczące projektu (tzw. *white paper*), co już obecnie się odbywa, jednak ilość podawanych informacji jest bardzo zróżnicowana.

Rozporządzenie MiCA standaryzuje wygląd i treść[94] takiego dokumentu informacyjnego. Dokument informacyjny nie będzie konieczny, w przypadku gdy całkowita wartość oferty kryptoaktywów nie przekroczy 1 mln euro w ciągu 12 miesięcy lub gdy będą one oferowane nieodpłatnie, oferta będzie kierowana do inwestorów kwalifikowanych, a także do mniej niż 150 osób fizycznych lub prawnych.

Najmniejsze restrykcje nakłada się na emitentów tokenów użytkowych. Są oni zobowiązani do zapewnienia inwestorom pełnych, jasnych, rzetelnych i niewprowadzających w błąd informacji za pośrednictwem materiałów marketingowych[95] oraz tzw. dokumentu informacyjnego. Dokument informacyjny nie jest zatwierdzany *ex ante* przez właściwe organy państwowe, a wymaga jedynie zgłoszenia.

---

[93] W myśl art. 3 ust. 1 pkt 7 rozporządzenia MiCA „oferta publiczna" to oferowanie osobom trzecim możliwości nabycia kryptoaktywów w zamian za walutę fiat lub za inne kryptoaktywa.

[94] W art. 5 rozporządzenia MiCA określono m.in. objętość dokumentu, rozmiar, układ, czcionki, co ma na celu zwiększenie jego przejrzystości i przystępności dla jego adresatów.

[95] Rozporządzenie MiCA, art. 6.

W rozporządzeniu MiCA istotne jest także uprawnienie każdego konsumenta do wycofania zgody na nabycie kryptoaktywów w terminie 14 dni od dnia wyrażenia zgody na ich zakup. W tym wypadku wszystkie płatności podlegają zwrotowi na rzecz konsumenta. To uprawnienie nie dotyczy sytuacji, w której kryptoaktywa są dopuszczone do obrotu na platformie obrotu kryptoaktywami.

Inaczej sytuacja wygląda w przypadku emitentów tokenów będących e-pieniądzem i tokenów powiązanych z aktywami. Tego rodzaju emitenci są zobowiązani do:

- uzyskania zezwolenia właściwego organu na złożenie oferty publicznej kryptoaktywów; zezwolenie będzie wydawane przez organ państwa, w którym emitent ma swoją siedzibę i będzie obowiązywało w całej UE na zasadzie tzw. jednolitego paszportu. Zezwolenie nie będzie wymagane w przypadku ofert publicznych kryptoaktywów, gdy w ciągu 12 miesięcy średnia wartość tokenów nie przekracza kwoty 5 mln euro lub gdy oferta jest skierowana wyłącznie do inwestorów kwalifikowanych;
- sporządzenia i opublikowania dokumentu informacyjnego (zgodnie ze standardami wyznaczonymi w rozporządzeniu) dotyczącego oferowanych kryptoaktywów;
- sporządzenia wyraźnie oznaczonych materiałów marketingowych, w których informacje są rzetelne, jasne i niewprowadzające w błąd;
- wdrożenia odpowiednich mechanizmów zarządzania płynnością;
- posiadania polityki wewnętrznej i zasad jej regulacji, a także odpowiedniej struktury organizacyjnej. Członkowie organu zarządzającego emitenta będą musieli wykazać się odpowiednim doświadczeniem, umiejętnościami i wiedzą, z uwzględnieniem także przepisów AML/CTF. Dostawcy usług w zakresie kryptoaktywów będą mieli obowiązek przeciwdziałania różnym rodzajom ryzyka, z którymi wiążą się technologie informacyjno-komunikacyjne (*information and communication technologies*)[96];
- wdrożenia skutecznego mechanizmu zapobiegania konfliktom interesów, ich identyfikowania i ujawniania;
- posiadania odpowiednich funduszy własnych i aktywów rezerwowych.

W rozporządzeniu MiCA przewidziano także możliwość czasowego odstępstwa od stosowania jego postanowień w przypadku przedsiębiorców zamierzających testować pewne modele biznesowe (w fazie start-up) pod nadzorem właściwych organów nadzorczych.

Rozporządzanie MiCA stanowi przejaw inflacji prawa[97] i z tego względu należy ocenić je krytycznie. Wprowadza ono zbyt dużo obowiązków formalnych związanych

[96] Ten obowiązek wynika także z projektu *Rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595 [dostęp: 13 V 2021].

[97] https://pl.wikipedia.org/wiki/Inflacja_prawa [dostęp: 30 VII 2021].

z oferowaniem kryptoaktywów (dostrzegalna jest tutaj analogia do podobnych regulacji na rynkach regulowanych, giełdach, gdzie jest dokonywany obrót papierami wartościowymi). Zdaniem autora będzie to stanowiło istotną barierę wejścia na rynek oraz będzie generowało wysokie koszty takiego wejścia (związane np. z doradztwem prawnym i ekonomicznym).

Ustawa AML

Obecnie większość platform obrotu kryptowalutami znajduje się na liście ostrzeżeń publicznych Komisji Nadzoru Finansowego[98]. Te platformy nie musiały wcześniej stosować żadnych środków AML/CTF (w tym identyfikować i weryfikować klienta), co niejednokrotnie prowadziło do sytuacji, w której środki pochodzące z tzw. nieautoryzowanych transakcji płatniczych na skutek przywłaszczenia danych dostępowych do rachunku bankowego były transferowane przez systemy płatności natychmiastowych na te platformy i następnie lokowane w bitcoiny. Taki zabieg powodował, że niemożliwe było ustalenie sprawców przywłaszczenia oraz pociągnięcie ich do odpowiedzialności karnej, a postępowania były umarzane na etapie postępowań przygotowawczych w sprawie.

W znowelizowanej ustawie AML ustawodawca uregulował działalność takich podmiotów, jak: kantory walut wirtualnych, giełdy walut wirtualnych oraz dostawców portfeli do przechowywania walut wirtualnych[99].

Przed uchwaleniem znowelizowanej ustawy AML polskie i europejskie prawodawstwo miało zastosowanie do walut wirtualnych w odniesieniu do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu jedynie częściowo przez uznanie pewnych kategorii podmiotów za instytucje obowiązane. Powodowało to między innymi konieczność stosowania przez nie tzw. środków bezpieczeństwa finansowego w postaci identyfikacji i weryfikacji klienta oraz posiadania odpowiednich procedur AML/CTF.

W znowelizowanej ustawie AML znacznie rozszerzono zakres tych obowiązków przez:

- wprowadzenie wymogu rejestracji dostawców świadczących usługi w zakresie walut wirtualnych[100] w rejestrze działalności w zakresie walut wirtualnych[101] (będzie to zatem działalność gospodarcza),
- wprowadzenie określonych wymogów dla podmiotów świadczących usługi w zakresie walut wirtualnych oraz osób fizycznych nimi zarządzających (wymóg braku skazania za określone przestępstwo). Powyższe wymogi dotyczą także zarządzających osobami prawnymi (spółki z ograniczoną odpowiedzialnością,

[98] Lista jest dostępna pod linkiem: https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne [dostęp: 10 V 2021].

[99] https://msztax.pl/nowe-przepisy-aml-a-dzialalnosc-w-zakresie-kryptowalut/ [dostęp: 10 V 2021].

[100] Ustawa AML, art. 129m.

[101] Tamże, art. 129p i dalsze.

spółki akcyjne) i wspólników jednostek organizacyjnych nieposiadających osobowości prawnej, ale mających zdolność prawną (spółki jawne, komandytowe),
- wprowadzenie wymogów reputacyjnych i kompetencyjnych dla osób prowadzących działalność gospodarczą w zakresie walut wirtualnych,
- wprowadzenie konieczności stosowania środków bezpieczeństwa finansowego przy przeprowadzaniu transakcji okazjonalnej w zakresie walut wirtualnych o równowartości 1 tys. euro lub większej.

Działalność obejmująca obrót walutami wirtualnymi może być wykonywana przez:
- osobę fizyczną, która nie została prawomocnie skazana za przestępstwa przeciw działalności instytucji państwowych i samorządu terytorialnego, wymiarowi sprawiedliwości, wiarygodności dokumentów, mieniu, obrotowi gospodarczemu i interesom majątkowym w obrocie cywilnoprawnym, obrotowi pieniędzmi i papierami wartościowymi, za finansowanie terroryzmu[102], za przestępstwo popełnione w celu osiągnięcia korzyści majątkowej lub osobistej bądź za umyślne przestępstwo skarbowe,
- osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, w której wspólnicy, którym powierzono prowadzenie spraw spółki lub uprawnienie do reprezentacji spółki, lub członkowie organów zarządzających nie zostali skazani za wyżej określone kategorie przestępstw.

Nowością jest to, że wymienione wymogi niekaralności mają zastosowanie także do osób, które w tych podmiotach kierują wykonywaniem czynności związanych z prowadzeniem działalności w zakresie walut wirtualnych (np. menedżerowie, dyrektorzy) oraz do beneficjentów rzeczywistych podmiotu prowadzącego taką działalność (np. do wspólników spółek z ograniczoną odpowiedzialnością oraz do akcjonariuszy spółek akcyjnych)[103].

Znowelizowana ustawa AML nakłada na osoby fizyczne zajmujące się wspomnianą działalnością obowiązek posiadania wiedzy lub doświadczenia związanego z tego rodzaju działalnością. Ten obowiązek może zostać spełniony przez:
- wykonywanie przez co najmniej rok czynności związanych z działalnością powiązaną z walutami wirtualnymi, co będzie potwierdzone odpowiednimi dokumentami,
- ukończenie szkolenia lub kursu obejmującego prawne lub praktyczne zagadnienia związane z działalnością w zakresie walut wirtualnych.

Organem właściwym w sprawach rejestrowych jest minister do spraw finansów publicznych (w drodze rozporządzenia te uprawnienia mogą zostać powierzone organowi Krajowej Administracji Skarbowej). Minister jako organ rejestrowy:
- prowadzi rejestr,
- przetwarza informacje o podmiotach do niego wpisanych,

---

[102] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.), art. 165a.

[103] Ustawa AML, art. 129n.

- rozpatruje wnioski o wpis do rejestru,
- nakłada kary pieniężne do wysokości 100 tys. zł na podmioty, które wbrew przepisom art. 153b znowelizowanej ustawy AML nie dopełniły obowiązku uzyskania wpisu do rejestru działalności w zakresie walut wirtualnych.

Poza ściśle administracyjnymi uprawnieniami organ rejestrowy ma także szczególne kompetencje mogące skutkować uniemożliwieniem prowadzenia działalności w zakresie walut wirtualnych podmiotowi, który:

- nie spełnia warunków wymaganych prawem do wykonywania działalności w zakresie walut wirtualnych,
- składa niezgodne ze stanem faktycznym oświadczenie[104] o zgodności z prawdą wniosku o wpis do rejestru oraz o jego kompletności, o znajomości warunków wykonywania działalności w zakresie walut wirtualnych, a także świadomości karnej za złożenie nieprawdziwego oświadczenia.

Wydaje się, że wysokość kary administracyjnej na poziomie 100 tys. zł jest całkowicie nieadekwatna do wolumenów kwotowych (ilości i wartości) transakcji zakupu lub sprzedaży walut wirtualnych. Przy obecnym kursie bitcoina stanowi ona niespełna połowę wysokości notowania jednej jednostki bitcoin[105]. Dużo bardziej efektywnym narzędziem do egzekwowania naruszeń przepisów AML/CTF wydają się przepisy rozporządzenia w sprawie współpracy organów krajowych odpowiedzialnych za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[106] (zwane rozporządzeniem CPC), w którym przewiduje się możliwość blokowania treści stron internetowych w przypadku naruszeń interesów konsumentów w przestrzeni cyfrowej (w Polsce takie uprawnienia są przewidziane dla Prezesa Urzędu Ochrony Konkurencji i Konsumentów). W polskim prawie funkcjonuje już regulacja dotycząca blokowania stron internetowych oferujących gry hazardowe niezgodnie z przepisami prawa, do czego są zobowiązani przedsiębiorcy telekomunikacyjni[107].

Znowelizowana ustawa AML w zakresie dodanej do niej treści (zgodnie z AMLD5) wzmacnia aktualnie obowiązujące przepisy w Polsce dotyczące AML/CTF. Zgodnie z nimi narażeniu na ryzyko prania pieniędzy i finansowania terroryzmu w obrocie walutami wirtualnymi przeciwdziała się przez uznanie za instytucje obowiązane[108] podmiotów, które prowadzą działalność gospodarczą polegającą na:

- wymianie walut wirtualnych na środki płatnicze,
- wymianie między walutami wirtualnymi,

---

[104] Ustawa, AML art. 129r ust. 2.

[105] Dane na 10 maja 2021 r.

[106] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004* (Dz. Urz. UE L 345 z 27 XII 2017 r., s. 1, ze zm.).

[107] *Ustawa z dnia 19 listopada 2009 r. o grach hazardowych* (t.j.: DzU z 2020 r. poz. 2094), art. 15f.

[108] Ustawa AML, art. 2 ust. 1 pkt 12.

- pośrednictwie we wskazanych wymianach,
- prowadzeniu rachunków w formie elektronicznej jako zbioru danych identyfikacyjnych, zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany.

Dotychczasowa praktyka i bieżące regulacje prawne w zakresie AML/CTF były podstawą wypracowania przez polskie organy ścigania metodologii pracy, na którą składa się[109]:

- wszczynanie procedury blokady środków pochodzących z przestępstwa,
- określenie charakteru platform wykorzystywanych do przestępczej działalności,
- poznanie polityki oceny ryzyka prania pieniędzy oraz finansowania terroryzmu, zapoznanie się z procedurami AML/CTF danej organizacji oraz ich analiza pod kątem dostosowania się przez organizację do tych regulacji w konkretnym przypadku,
- zwrócenie się do organizacji o zabezpieczenie śladów cyfrowych pozostawionych przez sprawców,
- rozważenie powołania biegłego z zakresu informatyki śledczej w celu zbadania śladów cyfrowych,
- rozważenie celowości podjęcia współpracy z innymi podmiotami, których ustawowym zadaniem jest AML/CTF.

Podsumowanie

Tryb i czas konsultacji, opiniowania i procedowania przepisów regulujących materię walut wirtualnych oraz związane z tym regulacje AML/CTF powodują, że w momencie ich wejścia w życie będą one całkowicie nieadekwatne do zmienionej rzeczywistości. Decydenci europejscy próbują dostosować przepisy prawne do zjawisk, których rozwój następuje w tempie geometrycznym, co – niestety – jest z góry skazane na niepowodzenie. Należy dostrzec pozytywne rozwiązania polegające na przyjęciu w znowelizowanej ustawie AML przepisów mających na celu zwiększenie wiarygodności i transparentności działań dostawców usług w zakresie walut wirtualnych przez wprowadzenie wymogu ich rejestracji, nastąpiło to jednak dopiero po wielu latach ich funkcjonowania na rynku europejskim, w tym polskim.

Rynek kryptoaktywów należy ucywilizować, trzeba jednak pamiętać, że obecne unormowania mogą doprowadzić do jego dysfunkcjonalności (np. przez wpisywanie – niejako automatycznie przez KNF – na listę ostrzeżeń publicznych większości platform, na których dokonuje się obrót kryptoaktywami) i ucieczki inwestorów i pieniędzy na rynki azjatyckie, co już następuje.

Obecne normy prawne stanowią przejaw wszechobecnej regulacji i inflacji prawa, która nie będzie długofalowo sprzyjać rozwojowi technologicznemu. Rozporządzanie

[109] P. Opitek, *Przeciwdziałanie praniu pieniędzy*…, s. 68.

MiCA jest przejawem inflacji prawa[110] i z tego względu należy ocenić je krytycznie. Wprowadza ono zbyt dużo wymagań formalnych związanych z oferowaniem kryptoaktywów. Zdaniem autora wymagania zawarte w rozporządzeniu MiCA będą istotną barierą wejścia na te rynki oraz będą generowały wysokie koszty takiego wejścia (związane np. z doradztwem prawnym i ekonomicznym), a ostatecznie spowodują odejście dostawców kryptoaktywów do bardziej przyjaznych jurysdykcji prawnych.

Bibliografia

Opitek P., *Przeciwdziałanie praniu pieniędzy wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70.

Pasternak Ł., *Kryptowaluta i pieniądz wirtualny jako przedmiot przestępstwa z art. 310 § 1 k.k.*, „Prokuratura i Prawo" 2017, nr 4, s. 77–94.

Piotrowska A., *Bitcoin. Płatnicze i inwestycyjne zastosowania kryptowaluty*, Warszawa 2018, CeDeWu.

Źródła internetowe

EBA Opinion on 'virtual currencies', European Banking Authority, 4 VII 2014 r., https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [dostęp: 10 V 2021].

ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies, The European Securities and Markets Authority, the European Banking Authority and the European Insurance and Occupational Pensions Authority, https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [dostęp: 10 V 2021].

Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention, raport Financial Stability Board (FSB) w sprawie implikacji FinTechu dla stabilności finansowej, 27 VI 2017 r., https://www.fsb.org/wp-content/uploads/R270617.pdf [dostęp: 10 V 2021].

Gradzi D., *FinTech/RegTech. Ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu wynikające z nowych technologii w obszarze płatności elektronicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, http://abw-portal.jskinternet.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-14/1658,PrzegladBezpieczenstwaWewnetrznego-nr-22-12-2020.html [dostęp: 10 V 2021].

[110] https://pl.wikipedia.org/wiki/Inflacja_prawa [dostęp: 30 VII 2021].

Informacja o kartach płatniczych. IV kwartał 2020 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/karty/q_04_2020.pdf [dostęp: 10 V 2021].

Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector (Wspólna opinia Europejskich Organów Nadzorczych w przedmiocie ryzyk związanych z praniem pieniędzy i finansowaniem terroryzmu wpływających na sektor finansowy UE z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 10 V 2021].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych, Komisja Europejska, Bruksela, 24 IX 2020 r, COM(2020) 591 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0591&from=EN [dostęp: 13 V 2021].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie unijnej strategii w zakresie płatności detalicznych, Komisja Europejska, Bruksela, 24 IX 2020 r, COM(2020) 592 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0592&from=EN [dostęp: 13 V 2021].

Liberadzki J., *Karnoprawne aspekty walut kryptograficznych (bitcoin jako przedmiot przestępstwa)*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2019, nr 3; https://www.czpk.pl/index.php/zeszyty-archiwum/zeszyt-2019-3 [dostęp: 11 V 2021].

Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2020 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/ocena/ocena2020_1.pdf [dostęp: 10 V 2021].

Polasik M., *Jak bardzo Polska jest bezgotówkowa? Zwyczaje płatnicze a rozwój sieci akceptacji kart. Wybrane wyniki badań realizowanych na rzecz Programu Polska Bezgotówkowa* (prezentacja) https://www.cashlesscongress.pl/wp-content/uploads/2020/09/Dzie%C5%84-1-Micha%C5%-82-Polasik-POLASIK-Research-Jak-bardzo-Polska-jest-bezgot%C3%B3wkowa.pdf [dostęp: 10 V 2021]

Raport z prac Zespołu ds. innowacji finansowych FinTech, Komisja Nadzoru Finansowego 12 V 2021 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_z_prac_Zespolu_ds_rozwoju_innowacji_finansowych_73565.pdf [dostęp: 13 V 2021].

Recommendations for The Security of Mobile Payments, European Central Bank, https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [dostęp: 10 V 2021].

Stanowisko w sprawie wydawania kart przepłaconych, Komisja Nadzoru Finansowego, 10 VII 2015 r., https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 10 V 2021].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie rynku kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937 (projekt), https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0014.02/DOC_1&format=PDF [dostęp: 13 V 2021].

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2021, (UE) nr 600/2014 oraz (UE) nr 909/2014 – projekt, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0595&from=EN [dostęp: 13 V 2021].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz. Urz. UE L 345 z 27 XII 2017 r., s. 1, ze zm.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) nr 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (tj.: Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE, (tj.: Dz. Urz. UE L 141/73 z 5 VI 2015 r., s. 73).

Dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (DzU z 2021 r. poz. 815, ze zm.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2020 r. poz. 971, ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j.: DzU z 2020 r. poz. 794, ze zm.).

Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (t.j.: DzU z 2020 r. poz. 2094).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

Abstrakt

W ostatnich latach nic tak bardzo nie przyczyniło się do rozwoju i cyfrowej ekspansji technologicznej, w tym w zakresie obrotu bezgotówkowego, jak sytuacja wywołana ogólnoświatową pandemią COVID-19. Bardziej natężony ruch w sferze płatności elektronicznych i walut wirtualnych może powodować większe zainteresowanie tymi obszarami ze strony grup przestępczych. Liczba transakcji oszukańczych dokonanych kartami w pierwszym półroczu 2020 r. w porównaniu z drugim półroczem 2019 r. wzrosła o 11,4 proc. Wśród nowych kierunków zmian w przepisach regulujących obrót walutami wirtualnymi pod kątem ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu należy wyróżnić pakiet finansów cyfrowych, na który składają się m.in. projekt rozporządzenia Parlamentu Europejskiego w sprawie rynku kryptoaktywów i znowelizowana ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Te regulacje przez swoją szczegółowość i formalizm oraz wiążące się z tym koszty operacyjne działalności mogą doprowadzić do istotnej zapaści na rynku walut wirtualnych i ucieczki inwestorów oraz wyprowadzenia pieniędzy na rynki azjatyckie. Obecne regulacje stanowią przejaw regulacji totalnej, która nie będzie sprzyjać rozwojowi technologicznemu.

Słowa kluczowe: AML, CTF, przeciwdziałanie praniu pieniędzy, przeciwdziałanie finansowaniu terroryzmu, KNF (PFSA), FinTech, RegTech, rozporządzenie MiCA.

The latest trends in regulatory changes for virtual currencies with regard to counteracting money laundering and financing of terrorism as well as the increase of cash-less transactions resulting from the COVID-19 pandemic

Abstract

In recent years, nothing has contributed so much to the development and digital expansion of technology, including the field of cashless transactions, as the situation caused by the global COVID-19 pandemic. Increased traffic of electronic payments and virtual currencies may generate more interest in these areas from criminal groups. The number of fraudulent card transactions in the first half of 2020 increased by 11.4% compared to the second half of 2019. Among the new regulatory trends in AML/CTF in the field of virtual currencies, the Digital Finance Package should be distinguished. It consists of the Proposal for a Regulation of the European Parliament on markets in

crypto-assets and amendments to the AML/CTF Act. The specificity and formalism of these rules, but also the related operating costs, may lead to a significant collapse in the virtual currencies market and the escape of investors and money to Asian markets. The current regulations are a manifestation of a total legal solution, which will not favour technological development.

Keywords: AML/CTF, anti-money laundering, countering the financing of terrorism, KNF (PFSA), FinTech, RegTech, Regulation on Markets in Crypto-assets.

MACIEJ GURTOWSKI
ORCID: 0000-0002-2990-9088

JAN WASZEWSKI
ORCID: 0000-0002-7370-3714

DOI: 10.4467/20801335PBW.21.021.14298

Niewidzialna infrastruktura Internetu – usługi chmurowe jako krytyczny element środowiska bezpieczeństwa. Przypadek Amazona

Na wstępie warto przeprowadzić pewien eksperyment myślowy: wyobraźmy sobie, że z powodu awarii, sabotażu lub celowych sankcji Polska zostaje pozbawiona możliwości korzystania z zasobów amerykańskich gigantów technologicznych z grupy GAFAM[1]. Jakie będą konsekwencje awarii i czy instytucje państwowe, podmioty prywatne oraz zwykli użytkownicy byliby w stanie w takiej sytuacji funkcjonować bez poważnych zakłóceń? Łatwo przewidzieć, że niemożność korzystania z chociażby samych systemów operacyjnych: Windows, Android czy MacOS/iOS miałaby katastrofalne następstwa. Mniej oczywiste, co nie znaczy, że mniej istotne, byłyby skutki zablokowania innych funkcjonalności, takich jak usługi chmurowe gigantów technologicznych. Właśnie temu mniej oczywistemu problemowi uzależnienia od usług chmurowych poświęcono niniejszy artykuł.

Na początku 2019 r. amerykańska dziennikarka Kashmir Hill w cyklu artykułów zatytułowanych *Żegnaj wielka piątko*[2] przedstawiła eksperyment, który przeprowadziła. Za pomocą informatycznych narzędzi zablokowała sobie dostęp do infrastruktury i usług kolejnych członków GAFAM. W pierwszym etapie zrezygnowała z produktów

[1] Akronim został stworzony z pierwszych liter nazw najważniejszych amerykańskich firm z branży nowych technologii, tj. Google, Amazon, Facebook, Apple i Microsoft. Inne określenie tej grupy to Big Tech.

[2] K. Hill, *Goodbye Big Five*, Gizmodo, 7 II 2019 r., https://gizmodo.com/c/goodbye-big-five [dostęp: 4 III 2021]. Tłumaczenia w artykule pochodzą od autorów (przyp. red.).

Amazona, jego usług streamingu filmów i seriali oraz ze sklepu internetowego. W kolejnym kroku odcięła się od wszystkich stron internetowych i aplikacji, które korzystają z usług chmurowych Amazona. Dość szybko okazało się, że wiele firm, również konkurencyjnych dla Amazona, opiera swoją działalność na jego infrastrukturze. W krótkim czasie dziennikarka zrozumiała, że: *Amazon jest głęboko zakorzeniony w jej życiu. Używa go wielokrotnie każdego dnia świadomie i nieświadomie. Nie jest w stanie bez niego normalnie funkcjonować*[3].

W niniejszym artykule autorzy przyjęli systemową koncepcję środowiska bezpieczeństwa[4]. Jest ona przeciwstawiana bardziej rozpowszechnionemu, intuicyjnemu podejściu do spraw bezpieczeństwa, w którym uwaga jest skupiana na jego bezpośrednich zagrożeniach. W przypadku bezpieczeństwa ograniczanie się do badania zagrożeń, bez uwzględniania towarzyszących im kontekstów, może prowadzić do błędów poznawczych. W podejściu systemowym właśnie konteksty stają się właściwym przedmiotem analizy. Zgodnie z przyjętym podejściem środowisko bezpieczeństwa ma naturę systemową, a zatem jego analiza powinna uwzględniać wiele czynników oraz dynamiczne interakcje między nimi. Jednym z najważniejszych jest technologia[5]. W analizie systemowej przyjmuje się, że środowisko bezpieczeństwa jest aktywnie, intencjonalnie i nieintencjonalnie kształtowane przez państwa i inne wpływowe podmioty. Autorzy artykułu skoncentrowali się na amerykańskich gigantach technologicznych.

Przedmiotem analizy jest jeden z głównych zasobów GAFAM, tj. usługi chmurowe, oraz aktualnie największy ich globalny dostawca – firma Amazon Web Services[6] (dalej: AWS), działająca od 2002 r. spółka zależna Amazona, która oferuje takie usługi od 2006 r. W czwartym kwartale 2020 r. miała ona w tym sektorze usług 32 proc. udziału w rynku światowym[7]. Druga w kolejności firma – Microsoft Azure dysponowała w tym samym czasie 20-procentowym udziałem w rynku, Google Cloud – 7-procentowym, a chiński Alibaba Cloud – 6-procentowym. Pozostałą część tego rynku kontrolowały drobniejsze podmioty. Można powiedzieć, że infrastruktura dostarczana przez Amazona i innych dostawców usług chmurowych w coraz większym stopniu

---

[3] K. Hill, *I Tried to Block Amazon From My Life. It Was Impossible*, Gizmodo, 22 I 2019 r., https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336 [dostęp: 24 III 2021].

[4] S. Tang, *A systemic theory of the security environment*, „Journal of Strategic Studies" 2004, nr 1, s. 1–3; por. G.H. Turbiville, W.W. Mendel, J.W. Kipp, *The Changing security environment*, „Military Review" 1997, nr 77, s. 5–10.

[5] S. Tang, *A systemic theory of the security environment*…, s. 2–3, 7; Centrum Doktryn i Szkolenia Sił Zbrojnych, *Analiza środowiska bezpieczeństwa w perspektywie 2035 r.*, Bydgoszcz 2020, https://cdissz.wp.mil.pl/pl/articlespublikacje_cdissz/analiza-srodowiska-bezpieczenstwa-w-perspektywie-2035-roku-pl/ [dostęp: 24 III 2021].

[6] Wyróżnienia w tekście pochodzą od autorów (przyp. red.).

[7] *Global cloud services market Q4 2020*, Canalys, 2 II 2021 r., https://www.canalys.com/newsroom/global-cloud-market-q4-2020 [dostęp: 5 III 2021].

pełni funkcję niewidzialnej infrastruktury Internetu[8]. Z usług chmurowych tej spółki korzysta tak wiele firm i instytucji, że awarie występujące u amerykańskiego giganta handlu internetowego były opisywane jako awarie całego Internetu[9]. Biorąc pod uwagę pozycję rynkową Amazona, autorzy artykułu podjęli decyzję, że w ramach studiów przypadków[10] zostaną przedstawione działania właśnie tej spółki. Wyzwania związane z usługami chmurowymi nie dotyczą jednak tylko AWS i innych członków GAFAM czy też firmy Alibaba Cloud.

W artykule zostają postawione dwa pytania badawcze:

1. W jaki sposób rozpowszechnienie się korzystania z usług chmurowych wpływa na globalne środowisko bezpieczeństwa?
2. Jakie zagrożenia stwarza zjawisko monopolizacji usług chmurowych?

W odpowiedzi na te pytania autorzy rozważą następujące hipotezy:

1. Rozpowszechnienie korzystania z usług chmurowych sprawia, że podmioty je oferujące zyskują narzędzia inwigilacji i potężnego, dyskrecjonalnego wpływu na swoich klientów (użytkowników) i relacje między nimi.
2. Monopolizacja usług chmurowych prowadzi do centralizacji struktury Internetu, tworząc nowe źródła podatności sieci na zakłócenia jej działania, związane z rosnącą zależnością coraz większej liczby użytkowników od coraz mniejszej liczby dostawców usług w chmurze.

W metodologii wykorzystanej w artykule studia przypadków odgrywają rolę uchwytnych empirycznie i przez to możliwych do uściślenia lub podważenia egzemplifikacji problemu przekształceń środowiska bezpieczeństwa, wynikających z rozpowszechnienia się korzystania z usług chmurowych.

Artykuł ma następującą strukturę. Na początku przedstawiono rozważania definicyjne porządkujące poruszane zagadnienia. W dalszej części tekstu odwołano się do literatury przedmiotu dotyczącej typowych sposobów analizowania zagrożeń związanych ze stosowaniem chmury obliczeniowej. Następnie zaprezentowano dwa krótkie

---

[8] M. Day, *Amazon Cloud Outage Hits Customers Including Roku, Adobe*, Bloomberg, 25 XI 2020 r., https://www.bloomberg.com/news/articles/2020-11-25/amazon-web-services-outage-hits-cloud-customers [dostęp: 7 XII 2020].

[9] J. Del Rey, *Amazon's massive AWS outage was caused by human error*, „Recode", 2 III 2017 r., https://www.vox.com/2017/3/2/14792636/amazon-aws-internetoutage-cause-human-error-incorrect-command [dostęp: 11 XII 2020]; K. Hill, *I Tried to Block Amazon…*

[10] Są to konkretnie instrumentalne studia przypadków (*instrumental case study*), które są jednym ze sposobów podejścia do analizy przypadku (wszystkie wyrazy i zwroty obcojęzyczne w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje za każdym razem tej informacji – dop. red.). To podejście służy jak najbardziej wyrazistemu zilustrowaniu danego zjawiska, jego przyczyn i skutków. Sam przypadek odgrywa w nim rolę pomocniczą. Zob. R.E. Stake, *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim, Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 627–629.

Punktem wyjścia dla studiów przypadków zawartych w niniejszym artykule były analizy prowadzone przez autorów w ramach ich pracy w Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej w Warszawie.

studia przypadków, które ilustrują zagrożenia związane z rozwojem usług chmurowych. W kolejnym kroku pokazano, że znaczenie takiej chmury dla środowiska bezpieczeństwa stale rośnie. Na podstawie m.in. ustaleń amerykańskiej parlamentarnej podkomisji antytrustowej wykazano, że głównych dostawców chmury trudno nazwać partnerami, co do których wiarygodności nie ma poważnych wątpliwości. Artykuł kończą wnioski, zawierające syntezę przeprowadzonych rozważań.

Czym jest i jak działa chmura? Najważniejsze pojęcia

W celu uporządkowania niniejszego wywodu warto przyjrzeć się najważniejszym pojęciom związanym z systemem usług chmurowych.

Koncepcję uruchomienia chmury obliczeniowej w jej współczesnym rozumieniu przypisuje się właśnie Amazonowi[11]. Około 2003 r. spółka uznała, że skoro posiada dużą liczbę komputerów połączonych w sieć, które np. nocą nie są w USA w pełni wykorzystywane, to można je zdalnie i odpłatnie udostępnić komuś z innych części świata. W 2006 r. powstał system łączący dostępne zdalnie komputery (w nomenklaturze AWS jest to usługa E2C), magazyny danych (usługa S3) oraz narzędzie do wynajmowania ludzi do realizowania zdalnie zadań, których obecnie nie można wykonać automatycznie (usługa *Mechanical Turk*)[12].

Zgodnie z ogólnie przyjętą definicją zaproponowaną przez amerykański Narodowy Instytut Standardów i Technologii (National Institute of Standards and Technology, NIST): (…) *chmura obliczeniowa* [*cloud computing*] *to model* [działania] *pozwalający na osiągalny wszędzie i na żądanie wygodny dostęp za pomocą sieci do podzielanej puli możliwych do skonfigurowania zasobów (np. sieci, serwerów, przestrzeni magazynowej, aplikacji i usług), które mogą być szybko dostarczane i uaktywniane z minimalnym wysiłkiem zarządczym lub niewielkim kontaktem z dostawcą*[13]. Innymi słowy, „chmura obliczeniowa" to dostępne zdalnie komputery, podłączone do nich dyski twarde i obecne na nich oprogramowanie, które klienci mogą łatwo wykorzystać do realizowania swoich potrzeb. Ich zaspokajanie jest skalowalne – można wynajmować aktualnie potrzebną ilość mocy obliczeniowej czy przestrzeni do magazynowania danych. Serwerownie lub centra danych, w których mieszczą się komputery wchodzące w skład chmury, mogą korzystać z efektu skali. Duża liczba znajdujących się w jednym miejscu komputerów

[11] Ryan Ko, Kim-Kwang Raymond Choo, *Cloud Security Ecosystem*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 1.

[12] Tamże, s. 2.

[13] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, wrzesień 2011 r., https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp: 4 III 2021]. Również *Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"* (MP z 2019 r. poz. 862) wydaje się w części słownikowej korzystać z definicji NIST dotyczących chmury obliczeniowej i innych pojęć z nią związanych.

sprawia, że spadają np. koszty ich serwisowania i chłodzenia, energii elektrycznej oraz zwiększania lub zmniejszania zasobów dostępnych dla klientów wraz z ich rosnącymi lub malejącymi potrzebami.

Standardowo chmury dzieli się pod kątem tego, kto ma bezpośrednią kontrolę nad infrastrukturą i do jak daleko idącego *outsourcingu* usług informatycznych dochodzi. W dużym uproszczeniu podział opiera się więc na tym, kto ma fizyczny dostęp do serwerów i odpowiada za ich działanie. W wypadku chmury prywatnej kontrolę nad nią dzierżą firmy lub osoby fizyczne, które zbudowały dla siebie serwerownię czy centrum danych. Chmura społecznościowa znajduje się pod kontrolą użytkowników z różnych organizacji, które podzielają pewien cel, ideę lub zadania publiczne. Chmura publiczna oznacza infrastrukturę znajdującą się na serwerach dostawcy i dostępną praktycznie dla każdego, kto zakupi do niej dostęp. Chmura może być również hybrydowa, czyli łączyć różne cechy wcześniej wymienionych typów.

Przyjmuje się, że istnieją trzy główne modele realizowania usług chmurowych:

1) infrastruktura jako usługa (*Infrastructure as a Service*, IaaS),
2) platforma jako usługa (*Platform as a Service*, PaaS),
3) oprogramowanie jako usługa (*Software as a Service*, SaaS).

Kolejność wymienienia tych modeli jest zgodna z rosnącym zakresem kontroli powierzonej dostawcy nad oferowanymi rozwiązaniami. W wypadku IaaS chmura to tylko czysta infrastruktura, to znaczy dostępne zdalnie komputery. PaaS daje użytkownikowi kontrolę również nad swoimi aplikacjami i konfiguracją komputerów, ale już system operacyjny, narzędzia w niego wbudowane i obsługa języków programowania są dostarczane przez dostawcę usług chmurowych. Z kolei w modelu SaaS użytkownik korzysta z aplikacji działających w chmurze za pomocą interfejsu, takiego jak np. przeglądarka internetowa, i ma wpływ tylko na minimalną liczbę ustawień.

Obecnie zachodzą duże zmiany strukturalne w sposobach tworzenia oprogramowania[14]. Jedną z najważniejszych jest przejście z software'u działającego na urządzeniach użytkowników na usługi chmurowe. Dzięki tym usługom zaistniały i nabrały rozmachu opisane w artykule zjawiska, wskazywane w różnych analizach dotyczących IaaS, PaaS czy SaaS. Pojawiły się również m.in. usługi chmurowe w postaci analizy danych jako usługi (*Data as a Service*, DaaS), bezpieczeństwa jako usługi (*Security as a Service*, SECaaS[15]), platform kontenerowych[16] czy dostępnych zdalnie systemów

[14] S. Gürses, J. Van Hoboken, *Privacy After the Agile Turn*, w: *Cambridge Handbook of Consumer Privacy*, J. Polonetsky, O. Tene, E. Selinger (red.), Cambridge 2017, https://osf.io/preprints/socarxiv/9gy73/ lub https://osf.io/ufdvb/ [dostęp: 22 III 2021].

[15] B. Delamore, Ryan K.L. Ko, *Security as a service (SECaaS) – An overview*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 187–202.

[16] Są to zamknięte środowiska służące do uruchamiania aplikacji na różnych systemach operacyjnych. Jest to możliwe dzięki temu, że w „kontenerze" znajdują się wszystkie elementy potrzebne aplikacji do pracy (zob. np. *Co to jest kontener?*, https://azure.microsoft.com/pl-pl/overview/what-is-a-container/ [dostęp: 24 III 2021]).

sztucznej inteligencji[17]. Każdy z tych typów usług chmurowych ma niebagatelny wpływ na to, jak działa współczesny sprzęt komputerowy (hardware) oraz oprogramowanie, a tym samym na korzystające z nich podmioty (gospodarcze, publiczne). Podsumowując, zgodnie z aktualnymi konwencjami terminologicznymi chmura to nie tylko infrastruktura oraz programy (proces ich tworzenia, modyfikowania i wykorzystywania), lecz także analiza danych, *outsourcing* cyberbezpieczeństwa, wykrywanie wzorców i automatyzacja różnych działań za pomocą systemów sztucznej inteligencji (jako przykład można wskazać system JEDI opisany w dalszej części artykułu).

Innym ważnym pojęciem jest „*multicloud*", czyli bazowanie na zasobach wielu chmur, aby wykorzystać najbardziej użyteczne rozwiązania dostarczane przez różnych dostawców i nie uzależniać się od jednego z nich. *Multicloud* jest zagrożeniem modelu biznesowego dostawców usług chmurowych, którzy chcieliby kompleksowo zaspokajać potrzeby klientów i być za to opłacani. W takim modelu dąży się do uniknięcia sytuacji, w której klient może z łatwością zrezygnować z usług danego dostawcy lub z ich części.

Obowiązującym obecnie standardem dla publicznej chmury obliczeniowej jest zapewnianie klientom złożonych systemów usług, powiązanych ze sobą i wspierających się nawzajem. W opisanych poniżej studiach przypadków zostały przedstawione dwa typy znanych zagrożeń wynikających ze złożoności chmury. Po pierwsze, są to jej awarie (*outage*), które w połączeniu z możliwymi efektami kaskadowymi prowadzą do rozchwiania, a nawet załamania się części lub całości wspomnianego systemu[18]. Drugim znanym rodzajem zagrożenia jest uzależnienie się od usług stworzonych przez danego dostawcę (*vendor lock-in*)[19]. Ze względu na złożoność systemów poszczególnych dostawców utrudnione – a nawet niemożliwe – staje się sprawne odbudowanie funkcjonalności systemu klienta po zakończeniu przez niego współpracy z danym dostawcą chmury. Z tego powodu już na etapie planowania korzystania z chmury należy ustalić, czy będzie możliwe przejście do innego dostawcy usług chmurowych lub powrócenie do korzystania z własnych systemów[20].

Na poziomie ogólnych zasad działania rozwiązania chmurowe są stosunkowo proste. Korzystanie z nich wiąże się jednak z ryzykiem i wieloma zagrożeniami. W niniejszym artykule omówiono je na podstawie przeglądu literatury.

---

[17] Pod pojęciem „sztucznej inteligencji" jako usługi chmurowej należy rozumieć usługę zdalnej analizy danych w celu np. rozpoznawania obrazów (w tym identyfikowania ludzi na podstawie ich zdjęć czy odczytywania tablic rejestracyjnych), przekładanie wypowiadanych słów na tekst, udzielanie odpowiedzi przez bota na zadane mu pytania itp.

[18] Z pogłębioną, jednak pochodzącą sprzed pięciu lat, analizą przyczyn zakłóceń działania chmury można zapoznać się w: H.S. Gunawi i in., *Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages*, w: *Proceedings of the Seventh ACM Symposium on Cloud Computing (SoCC '16)*, New York 2016, s. 1–16.

[19] T. Kemmericha, V. Agrawala, C. Momsen, *Secure migration to the cloud – In and out*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 205–230.

[20] Tamże, s. 214–215.

Analizy zagrożeń związanych z rozwiązaniami chmurowymi w literaturze przedmiotu

W 2009 r. Bruce Schneier, znany amerykański badacz zagadnień związanych z cyberbezpieczeństwem, zwrócił uwagę na bardzo ważny aspekt działania chmury obliczeniowej, jakim jest konieczność posiadania zaufania do dostawcy usług[21]. Ważne są cztery filary tego zaufania, tj. bezpieczeństwo, odporność, dostępność i trwałość działalności gospodarczej dostawcy. Pierwsze trzy z tych czynników dotyczą problemów wynikających z awarii i działań służących ograniczeniu ich odległych konsekwencji. Czwarty czynnik obejmuje zagadnienia związane z *vendor lock-in*, czyli wspomniane wyżej problemy wynikające z zakończenia współpracy z danym dostawcą – nie tylko z powodu zaprzestania przez niego działalności.

Trzy najczęściej cytowane artykuły naukowe na temat bezpieczeństwa chmur obliczeniowych pochodzą z lat 2009–2010[22]. Ich wspólnym elementem jest wskazanie, że korzystanie z rozwiązań chmurowych wiąże się z przyjęciem określonego ryzyka. Tymczasem można odnieść wrażenie, że chociaż coraz więcej poważnych przedsięwzięć w sieci opiera się na korzystaniu z chmury, to wiele podmiotów zdaje się to ryzyko ignorować.

Opublikowana w 2015 r. praca zbiorowa zatytułowana *Cloud Security Ecosystem* pokazuje, jak bardzo wielowymiarowy staje się problem uwzględnienia różnych aspektów bezpieczeństwa chmury obliczeniowej[23]. W 22 rozdziałach wspomnianej publikacji zagrożenia są analizowane z perspektywy m.in. technologii, prawa, zarządzania oraz działalności gospodarczej.

Rola gigantów internetowych, w tym spółek amerykańskich określanych jako GAFAM oraz chińskich, których pierwsze litery nazw łączą się w często używany akronim BATX (Baidu, Alibaba, Tencent, Xiaomi), jest we współczesnym świecie na tyle duża, że ich działalność analizuje się także z perspektywy pełnienia przez nie funkcji publicznych[24]. Cztery z dziewięciu wspomnianych spółek, tj. Amazon, Google,

---

[21] B. Schneier, *Cloud Computing*, Schneier on Security, 4 VI 2009 r., https://www.schneier.com/blog/archives/2009/06/cloud_computing.html [dostęp: 17 III 2021].

[22] Zgodnie z informacjami z wyszukiwarki Google Scholar. Wyszukiwana fraza to „cloud security". Stan na 23 III 2021 r. Wspomniane artykuły to: B.R. Kandukuri, R.V. Paturi, A. Rakshit, *Cloud Security Issues*, w: *Procedings of the 2009 IEEE International Conference on Services Computing*, Washington 2009, s. 517–520, https://ieeexplore.ieee.org/document/5283911 [dostęp: 23 III 2021]; S. Ramgovind, M.M. Eloff, E. Smith, *The Management of Security in Cloud Computing*, w: *2010 Information Security for South Africa (ISSA 2010)*, 2010 r., s. 1–7; M. Almorsy, J. Grundy, I. Müller, *An analysis of the cloud computing security problem*, w: *Proceedings of the APSEC 2010 Cloud Workshop*, Sydney 2010, s. 6. Te trzy artykuły miały odpowiednio 847, 584 i 497 cytowań.

[23] *The Cloud Security Ecosystem*…

[24] L. Taylor, *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, „Philosophy & Technology", 20 I 2021 r., https://link.springer.com/article/10.1007/s13347-020-00441-4 [dostęp: 22 III 2021]. Por. M. Gurtowski i J. Waszewski, *Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon*, „Kwartalnik Bellona" 2020, nr 3, s. 37–56.

Microsoft i Alibaba, są największymi globalnymi dostawcami usług chmurowych. Te z kolei w coraz większym stopniu są wykorzystywane także do realizowania funkcji publicznych, bardzo ważnych dla współczesnego globalnego środowiska bezpieczeństwa. Tym samym zakłócenia w ich działaniu są naruszeniem niewidzialnej, bo często pomijanej (pomimo ostrzeżeń oraz dobrych praktyk przywołanych w dalszej części artykułu), infrastruktury Internetu. Eksperci nie stawiają w sposób systemowy pytań o władzę, jaką dysponują firmy technologiczne, i o rolę, jaką chmura obliczeniowa odgrywa we współczesnej infrastrukturze krytycznej. Zdaniem autorów artykułu jest to poważna luka w literaturze przedmiotu.

Nie tylko badacze i analitycy, lecz także różne instytucje i urzędy na świecie zgodnie wskazują na wiele korzyści i zagrożeń związanych z korzystaniem z chmury obliczeniowej. Przykładowo, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, dalej: ENISA – akronim pochodzi od wcześniejszej nazwy Agencji – European Network and Information Security Agency, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji) przygotowuje analizy oraz wyznacza standardy dotyczące usług chmurowych[25]. Warto zwrócić uwagę na opracowany przez nią dokument z grudnia 2012 r., w którym przeanalizowano korzyści i ryzyko związane z korzystaniem z tego rodzaju usług w kontekście bezpieczeństwa informacji[26]. Według wspomnianej agencji główne niebezpieczeństwa wiążą się m.in. z uzależnieniem od jednego dostawcy i brakiem możliwości przeprowadzania pełnego audytu ochrony danych wrażliwych. Inne zagrożenia wskazane w tym dokumencie w odpowiednich okolicznościach mogą wywołać awarie, a nawet efekty kaskadowe. W analizie poświęconej chmurze obliczeniowej jako infrastrukturze krytycznej ENISA przypomina również, że jest ona mieczem obosiecznym[27]. Z jednej strony najwięksi dostawcy dzięki rozproszeniu kosztów mogą oferować najlepsze i najnowocześniejsze środki zwiększające bezpieczeństwo i odporność, z drugiej jednak strony, (…) *jeśli pojawi się awaria lub włamanie, to konsekwencje również będą większe, wpływając jednocześnie na większą ilość danych, wiele organizacji i wielu obywateli*[28].

W styczniu 2020 r. amerykańska Agencja Bezpieczeństwa Narodowego (National Security Agency, dalej: NSA) opublikowała informacje na temat dobrych praktyk mających służyć minimalizowaniu zagrożeń związanych z korzystaniem z chmury

---

[25] European Union Agency for Cybersecurity, *Cloud and Big Data*, https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security [dostęp: 22 III 2021].

[26] European Network and Information Security Agency, *Cloud Computing. Benefits, risks and recommendations for information security*, rev. B z grudnia 2012 r., https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security [dostęp: 22 III 2021].

[27] European Network and Information Security Agency, *Critical Cloud Computing. A CIIP perspective on cloud computing services*, wersja 1.0 z listopada 2012 r., opublikowana 14 II 2013 r., https://www.enisa.europa.eu/publications/critical-cloud-computing [dostęp: 22 III 2021].

[28] Tamże, s. 6.

obliczeniowej[29]. Propozycje dotyczą jednak głównie powstrzymywania cyberataków. Z zaleceń NSA wynika, że zakłócenia w działalności chmury mogą być wywołane przez wiele rodzajów ataków.

Polskie organy nadzoru również wydają wytyczne w tym zakresie. Na przykład w styczniu 2020 r. Komisja Nadzoru Finansowego (KNF) opublikowała komunikat dotyczący przetwarzania informacji w chmurze obliczeniowej przez nadzorowane przez nią instytucje[30]. Wśród wytycznych związanych z szacowaniem ryzyka wymieniono potrzebę przeprowadzenia oceny, czy stosowane rozwiązania mogą skutkować ryzykiem uzależnienia się od jednego dostawcy. Użytkownik chmury obliczeniowej kontrolowany przez KNF powinien dysponować dokumentacją, która zwiera m.in. scenariusze awaryjne.

Polska planuje wykorzystanie możliwości oferowanych przez rozwiązania chmurowe i stworzenie Rządowej Chmury Obliczeniowej. W związku z tym Rada Ministrów przyjęła we wrześniu 2019 r. uchwałę w sprawie inicjatywy określanej jako „Wspólna Infrastruktura Informatyczna Państwa" (dalej: WIIP). Jednym z pierwszych etapów wprowadzania jej w życie było opublikowanie przez Ministerstwo Cyfryzacji w lutym 2020 r. standardów dotyczących cyberbezpieczeństwa chmur obliczeniowych[31]. Dokument przedstawia wymagania prawne, organizacyjne i techniczne, które muszą zostać spełnione w trakcie projektów wdrażających WIIP. Ze wspomnianej uchwały i standardów wynika, że przynajmniej w sferze deklaratywnej Polska nie tyle chce się uniezależnić od zewnętrznych rozwiązań chmurowych, ile budować je na bazie tych dostarczanych przez dostawców godnych zaufania, pilnować stabilności systemów i na każdym etapie wdrażać zasady cyberbezpieczeństwa.

W sierpniu 2020 r. amerykański think tank Carnegie Endowment for International Peace opublikował materiał na temat bezpieczeństwa chmury, zawierający porady dla polityków[32]. Godny uwagi jest m.in. załącznik, w którym opisano incydenty związane z chmurą i jej awariami[33]. Przedstawiono w nim np. konsekwencje błędu (literówki zrobionej przez programistę Amazona), który w 2017 r. doprowadził do awarii AWS obejmującej całe wschodnie wybrzeże USA. W ostatnich latach do awarii na skalę

---

[29] National Security Agency, *Mitigating Cloud Vulnerabilities*, styczeń 2020 r., https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF [dostęp: 3 III 2021].

[30] *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, 23 I 2020 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf [dostęp: 22 III 2021].

[31] *Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v. 1.00 – luty 2020*, https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf [dostęp: 7 VI 2021].

[32] Zob. np. T. Maurer, G. Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, sierpień 2020, https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf [dostęp: 23 III 2021].

[33] Tamże, s. 50–58.

regionalną lub globalną dochodziło także m.in. w wyniku wyładowań atmosferycznych, zmian w konfiguracji serwerów czy nawet zmiany protokołu przesyłania danych przez dostawcę usług internetowych w Nigerii (dane wędrowały okrężną drogą przez Chiny).

Z przedstawionego powyżej przeglądu wynika, że istnieje pewien konsensus na temat tego, że korzystanie z usług chmurowych wiąże się z dwoma poważnymi rodzajami ryzyka. Po pierwsze, usługi chmurowe są narażone na wiele właściwych sobie podatności na błędy i awarie zakłócające ich działanie. Po drugie, dostawca usług chmurowych ma duże możliwości dyskrecjonalnego wpływu na sposób i zakres świadczonych usług. Dlatego tak ważne jest zaufanie do dostawcy, który powinien być partnerem sprawdzonym, rzetelnym i przewidywalnym. Szczególną ostrożność powinno się zachować wobec amerykańskich gigantów technologicznych, o czym przekonują wyniki prac amerykańskiej podkomisji antytrustowej, opisane w dalszej części niniejszego artykułu.

Można zauważyć, że w analizowanej literaturze przedmiotu uwaga została skupiona na bezpośrednich zagrożeniach. Pojawiają się również postulaty akcentujące potrzebę prowadzenia wielopoziomowej analizy problematyki usług chmurowych i zwrócenia uwagi na rosnące znaczenie gospodarcze i polityczne gigantów technologicznych. W przedstawionych poniżej studiach przypadków uwidacznia się problem połączenia czterech filarów zaufania do dostawcy chmury (wskazany przez Schneiera i w pewnym zakresie przez ENISĘ) ze wspomnianym wcześniej trendem dotyczącym konsolidacji zasobów Internetu w rękach wyłaniającego się oligopolu grupy gigantów technologicznych. Wartością dodaną będzie przeanalizowanie, co się dzieje w praktyce, gdy filary zaufania skonceptualizowane przez Schneiera zostają zachwiane przez jedną z najpotężniejszych firm na świecie.

Awaria chmury i efekty kaskadowe jako zakłócenie działania całego Internetu

W dniu 25 listopada 2020 r. w tysiącach gospodarstw domowych na wschodnim wybrzeżu USA przestały działać m.in. inteligentne odkurzacze – roboty sprzątające. Zapewne niewielu ich użytkowników było wtedy świadomych, że przyczyną problemów z domowym AGD jest awaria, która zaistniała u dostawcy usług chmurowych. Skutkiem trwającego kilka godzin uszkodzenia jednej z usług chmurowych Amazona było pojawienie się efektu kaskadowego[34]. Usterka, do której doszło w centrum danych obsługującym wschodnią część USA, zakłóciła działanie aż 27 kolejnych systemów tej firmy związanych z usługami chmurowymi[35]. W konsekwencji ok. 25 firm, także o globalnym zasięgu działania, nie mogło przez co najmniej kilka godzin dostarczać swoim

[34] M. Day, *Amazon Cloud Outage Hits Customers…*

[35] C. Cimpanu, *AWS outage impacts thousands of online services*, Zdnet, 25 XI 2020 r., https://www.zdnet.com/article/aws-outage-impacts-thousands-ofonline-services/ [dostęp: 7 XII 2020].

klientom usług internetowych. Problemy pojawiły się m.in. u dostawców oprogramowania, producenta urządzeń do streamingu telewizji, w urządzeniach Internetu rzeczy (RTV/AGD podłączonych do sieci, w tym we wspomnianych odkurzaczach) oraz u wydawców portali internetowych. Przestały działać również tzw. inteligentne dzwonki do drzwi połączone z kamerami monitoringu, które są produkowane i obsługiwane przez Amazon Ring, spółkę zależną Amazona[36]. Przykład tej awarii pokazuje, że jedna usterka w chmurze obliczeniowej czy też błąd programisty aktualizującego daną usługę może wywołać, niczym poruszenie jednej kostki domina, negatywne skutki w wielu innych elementach struktury.

Podobną reakcję, chociaż na mniejszą skalę, wywołał pożar, który wybuchł w marcu 2021 r. w centrum danych spółki OVH w Strasburgu[37], będącej jednym z mniejszych dostawców usług chmurowych. Wspomniana firma jest jednym z podmiotów zaangażowanych w tworzenie europejskiej chmury w ramach projektu GAIA-X (więcej na temat tego projektu w dalszej części artykułu). Pożar zniszczył jedno centrum danych, a trzy kolejne zostały odcięte od prądu[38]. Z tego powodu wiele portali internetowych doświadczyło przerw w funkcjonowaniu. O nieprzygotowaniu na tego typu awarie wymownie świadczy to, że w jej wyniku administratorzy strony jednej z instytucji publicznych w Polsce – Rzecznika Finansowego – przez kilka dni byli w stanie udostępnić jedynie elementy archiwalnej wersji strony, zachowane dzięki serwisowi Web Archive[39].

Tego rodzaju awarie nie są czymś wyjątkowym. Istotne w powyższych przykładach jest to, że pokazują one rosnącą złożoność usług chmurowych i zależności wynikające z ich wzajemnych połączeń. Im więcej różnych urządzeń jest podłączonych do sieci i im więcej form aktywności człowieka jest realizowanych w sposób zapośredniczony cyfrowo, tym bardziej dalekosiężne i destruktywne mogą być konsekwencje zakłóceń w działaniu chmury.

---

[36] *AWS: Amazon web outage breaks vacuums and doorbells*, BBC, 26 XI 2020 r., https://www.bbc.com/news/technology-55087054 [dostęp: 7 XII 2020].

[37] Zob. np. P. Judge, *Fire destroys OVHCloud's SBG2 data center in Strasbourg*, Data Center Dynamics, 10 III 2021 r., https://www.datacenterdynamics.com/en/news/fire-destroys-ovhclouds-sbg2-data-center-strasbourg/ [dostęp: 24 III 2021].

[38] Jak się później okazało, jeszcze jedno centrum danych nie mogło wznowić działalności. Zob. P. Judge, *OVH fire: OVHcloud abandons efforts to restart SBG1 data center in Strasbourg*, Data Center Dynamics, 21 III 2021 r., https://www.datacenterdynamics.com/en/news/ovh-fire-ovhcloud-abandons-efforts-restart-sbg1-strasbourg/ [dostęp: 24 III 2021].

[39] Zob. https://web.archive.org/web/20210129150346if_/https://rf.gov.pl/ [dostęp: 12 III 2021]. Sprawa została opisana 12 III 2021 r. na blogu „Problemy Polskiej Branży IT", w tekście pt. *Dlaczego admin Rzecznika Finansowego powinien dostać podwyżkę?*, https://ppbit.pl/news/dlaczego-admin-rzecznika-finansowego-powinien-dostac-podwyzke/ [dostęp: 12 III 2021].

Wyłączenie sieci społecznościowej Parler

Na początku stycznia 2021 r., tuż po wtargnięciu tłumu demonstrantów na amerykański Kapitol i zawieszeniu kont Donalda Trumpa w mediach społecznościowych, doszło do zablokowania działania sieci społecznościowej Parler[40]. Skupiała ona m.in. zwolenników kończącego kadencję prezydenta Trumpa, przyciągniętych obietnicą swobodnej wymiany informacji, moderowanej tylko w niewielkim stopniu. Działający od 2018 r. Parler już w listopadzie 2020 r. miał ok. 10 mln użytkowników, z których część została wcześniej usunięta z innych mediów społecznościowych z powodu łamania ich regulaminów[41]. Parler zachęcał do korzystania ze swoich usług, podkreślając, że stosuje liberalne zasady moderacji treści. Miały one bazować głównie na zgłoszeniach od innych użytkowników, którym dane treści wydały się nieodpowiednie. Największy wpływ na zablokowanie Parlera miała decyzja Amazona o zawieszeniu działania infrastruktury tego medium społecznościowego, wykorzystującej chmurę amerykańskiego giganta internetowego. Wspomnianą decyzję ogłoszono bardzo późno – niewiele ponad dobę przed wyłączeniem usług. Amerykańskie media cytowały e-mail wysłany do Parlera przez firmę Amazon[42]. Przedstawicielka tej drugiej spółki wskazywała, że problemem nie było polityczne zaangażowanie użytkowników Parlera, lecz brak odpowiednich mechanizmów blokowania nawoływań do przemocy. W ciągu kilku tygodni poprzedzających zawieszenie Parler miał nie zareagować na 98 zastrzeżeń zgłoszonych przez Amazona do publikowanych na nim treści.

Parler pozwał Amazona i zażądał wstrzymania zawieszenia świadczenia usług chmurowych[43]. Firma argumentowała, że blokada ma podłoże polityczne – jako nowe, konserwatywne medium społecznościowe Parler zaczął się stawać konkurencją dla liberalnego Twittera, który również korzysta z chmury Amazona. Tymczasem, jak można wnioskować z argumentacji Parlera, Twitter także ma problemy z moderacją treści. Decyzja o zawieszeniu Parlera miała wynikać przede wszystkim z chęci uniemożliwienia mu konkurowania z Twitterem. Zgodnie z treścią pozwu zablokowanie korzystania z chmury miało być równoznaczne z (…) *wyciągnięciem wtyczki z maszyny podtrzymującej życie*

[40] B. Fung, *Parler has now been booted by Amazon, Apple and Google*, CNN, 11 I 2021 r., https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html [dostęp: 11 I 2021].

[41] J. Schieber, *Parler jumps to No. 1 on App Store after Facebook and Twitter ban Trump*, Tech Crunch, 9 I 2021 r., https://techcrunch.com/2021/01/09/parler-jumps-to-no-1-on-app-store-after-facebook-and-twitter-bans/ [dostęp: 11 I 2021].

[42] Zob. m.in.: J. Paczkowski, R. Mac, *Amazon Is Booting Parler Off Of Its Web Hosting Service*, BuzzFeed, 9 I 2021 r., https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws [dostęp: 11 I 2021].

[43] Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021]. Jedną z analiz pozwu i zawartych w nim argumentów prawnych opracował Mike Masnick. Zob. tenże, *Parler's Laughably Bad Antitrust Lawsuit Against Amazon*, Techdirt, 13 I 2021 r., https://www.techdirt.com/articles/20210113/11333746046/parlers-laughably-bad-antitrust-lawsuit-against-amazon.shtml [dostęp: 14 I 2021].

pacjenta na intensywnej terapii[44]. To porównanie obrazuje niezbędność infrastruktury Amazona dla platformy Parler. Od samego początku jej oprogramowanie i aplikacje na urządzenia mobilne miały być tworzone wyłącznie z myślą o usługach chmurowych Amazona[45]. Nie było więc możliwości ich łatwego przetransferowania na inne platformy, a wybór innego dostawcy wymagał dużych zmian w oprogramowaniu[46]. Parler początkowo twierdził, że jest w stanie bez problemu przejść do innego dostawcy usług chmurowych[47]. Świadczyłoby to o korzystaniu jedynie z infrastruktury AWS. Jednak w pozwach przeciwko Amazonowi firma podkreślała, że jego aplikacja korzystała z rozwiązań typowych dla tego dostawcy usług chmurowych. Oznaczałoby to, że przynajmniej pewne elementy Parlera działały w modelu PaaS.

W odpowiedzi na pozew Parlera Amazon odrzucił wszystkie zarzuty[48]. Dnia 21 stycznia 2021 r. sąd stwierdził, że wniosek o przywrócenie wykonywania usług nie jest zasadny[49]. Do końca stycznia 2021 r. Parlerowi udało się przywrócić działanie portalu tylko w szczątkowej formie[50]. Kolejne amerykańskie firmy dostarczające kompleksowe usługi chmurowe odmówiły z nim współpracy. Konieczne stało się poszukanie mniejszych dostawców poszczególnych usług niezbędnych do reaktywacji portalu. Przykładowo, do zapewnienia ochrony portalu przed atakami typu DDoS (*distributed denial of service*, czyli rozproszona odmowa usługi) Parler wykorzystał rosyjską firmę, która świadczyła usługi m.in. dla Ministerstwa Obrony Federacji Rosyjskiej, spółki zależnej Sbierbanku oraz państwowego dostawcy usług telekomunikacyjnych współpracującego z rosyjskimi służbami specjalnymi[51].

---

[44] Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021].

[45] Tamże, s. 5.

[46] Por. D. Cameron, *Every Deleted Parler Post, Many With Users' Location Data, Has Been Archived*, Gizmodo, 11 I 2021 r., https://gizmodo.com/every-deleted-parler-post-many-with-users-location-dat-1846032466 [dostęp: 12 I 2021].

[47] Por. M. Branscombe, *Why Parler Can't Rebuild a Scalable Cloud Service from Scratch*, The New Stack, 19 I 2021 r., https://thenewstack.io/why-parler-cant-rebuild-a-scalable-cloud-service-from-scratch/ [dostęp: 24 III 2021].

[48] Odpowiedź Amazona z 12 I 2021 r. na pozew Parlera, https://beta.documentcloud.org/documents/20449127-amazon_response [dostęp: 13 I 2021]. Por. komentarz do pozwu: T. Sonnemaker, *Amazon hits back at Parler's antitrust lawsuit with extensive examples of its violent content, including death threats against politicians, tech CEOs, and BLM supporters*, Business Inside, 13 I 2021 r., https://www.businessinsider.com/amazon-responds-to-parler-lawsuit-cites-violent-content-section-230-2021-1?IR=T [dostęp: 13 I 2021].

[49] B. Allyn, *Judge Refuses To Reinstate Parler After Amazon Shut It Down*, NPR, 21 I 2021 r., https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down [dostęp: 23 I 2021].

[50] J. Newman, *Here's why Parler is still struggling to come back online*, Fast Company, 21 I 2021 r., https://www.fastcompany.com/90596427/parler-coming-back-after-aws-ban [dostęp: 23 I 2021].

[51] K. Mehorota, *Parler's New Partner Has Ties to the Russian Government*, Bloomberg, 22 I 2021 r., https://www.bloomberg.com/news/articles/2021-01-22/parler-s-new-partner-has-ties-to-the-russian-government [dostęp: 23 I 2021].

Bezpośrednio przed decyzją Amazona dostęp do aplikacji umożliwiającej korzystanie z Parlera na urządzeniach mobilnych został zawieszony w sklepach z aplikacjami Google Play Store i App Store, z których najłatwiej jest pobrać oprogramowanie na najpopularniejsze urządzenia mobilne (czyli te z systemami operacyjnymi Android oraz iOS). Do zablokowania aplikacji doszło akurat wtedy, gdy w następstwie zawieszenia kont należących do Trumpa Parler stał się najczęściej pobieraną aplikacją w tych dwóch sklepach[52]. O ile usunięcie Parlera ze sklepów z aplikacjami utrudniło dostęp do niego głównie nowym użytkownikom, o tyle zablokowanie możliwości korzystania z chmury Amazona odcięło od tego medium społecznościowego również jego wcześniejszych użytkowników.

Zawieszenie Parlera nie było pierwszą sytuacją, w której doszło do odmowy realizowania usług na rzecz serwisu internetowego przez dostawców infrastruktury sieciowej[53]. Z podobnym problemem nie musiały się jednak mierzyć nigdy dotąd, przynajmniej w USA, największe portale: Facebook, Twitter i YouTube – i to pomimo kłopotów, które te platformy miały w przeszłości i mają obecnie z moderowaniem treści[54]. Przykładowo, w 2018 r. śledczy ONZ zarzucili Facebookowi, że za jego pomocą rozpowszechniano mowę nienawiści, która przyczyniła się do ludobójstwa w Birmie (Mjanma) w 2017 r.[55]

W połowie lutego 2021 r. Parler ponownie uruchomił swoją stronę internetową. Spółka zadeklarowała, że będzie budować infrastrukturę samodzielnie, z pominięciem zasobów Big Tech[56]. Jak się jednak okazało, był to powrót jedynie do nielicznych usług portalu – bez możliwości zapisywania się nowych użytkowników i bez dostępu do archiwalnych dyskusji. To pokazuje, jak trudno jest obecnie samodzielnie zapewnić świadczenie wysokiej jakości usług cyfrowych, bez płacenia za gotową infrastrukturę gigantów cyfrowych. W lutym 2021 r. Apple odmówiło Parlerowi zgody na powrót jego aplikacji do sklepu App Store[57]. Regulamin Parlera w dalszym ciągu miał być w niewystarczającym stopniu zgodny z wymaganiami tego sklepu. W marcu 2021 r. Parler po raz kolejny pozwał Amazona[58]. Zarzucił mu, że wspólnie z innymi (spółki wymienione

---

52 Tamże.

53 G. Edelman, *The Parler Bans Open a New Front in the 'Free Speech' Wars*, Wired, 13 I 2021 r., https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/ [dostęp: 13 I 2021].

54 Tamże.

55 T. Miles, *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters, 12 III 2018 r., https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN [dostęp: 14 I 2021].

56 J. Brodkin, *Parler says it's back without 'Big Tech' after being kicked off Amazon*, Ars Technica, 15 II 2021 r., https://arstechnica.com/tech-policy/2021/02/parler-says-its-back-without-big-tech-after-being-kicked-off-amazon/ [dostęp: 3 III 2021].

57 W. Turton, M. Gurman, *Parler Blocked on Apple's App Store After Capitol Riot Review*, Bloomberg, 10 III 2021 r., https://www.bloomberg.com/news/articles/2021-03-10/parler-cuts-ios-team-after-apple-blocks-return-to-app-store [dostęp: 11 III 2021].

58 K. Cox, *Parler sues Amazon (again), claims AWS ban sank a billion-dollar valuation*, Ars Technica, 3 III 2021 r., https://arstechnica.com/tech-policy/2021/03/parler-sues-amazon-again-claims-aws-ban-sank-a-billion-dollar-valuation/ [dostęp: 4 III 2021].

w pozwie to: Twitter, Facebook i Google) postanowił zniszczyć go jako konkurencję[59]. Na skutek zmowy Parler miał stracić szanse na zdobycie inwestorów i to w momencie, gdy był wyceniany na ponad miliard dolarów. Usunięcie go z chmury Amazona sprawiło, że przez ponad miesiąc nie mógł wznowić działalności, stracił klientów i wartość.

Dla niniejszego wywodu nie jest istotne, jak ocenia się działalność Parlera i zagrożenia związane z tą siecią społecznościową. Ważne jest to, że sprawa zablokowania mu możliwości prowadzenia działalności unaoczniła, jak wielką władzę mają dostawcy usług chmurowych. Na przykładzie Parlera widać, że są oni w stanie sparaliżować funkcjonowanie legalnie działającej firmy, która im zaufała. Użyty przez Amazona arbitralny argument o złych mechanizmach moderacji treści, który stał się przesłanką do odcięcia Parlera od usługi chmurowej, może w przyszłości zostać wykorzystany również wobec innych użytkowników chmury Amazona czy innych dostawców. I podobnie jak w wypadku Parlera może się okazać, że oprogramowanie zablokowanego podmiotu było od podstaw zbudowane pod kątem chmury jednego dostawcy. Sama możliwość zaistnienia takiej sytuacji wskazuje na asymetrię relacji pomiędzy dostawcami usług chmurowych a ich klientami.

Funkcjonowanie chmury Amazona w ocenie amerykańskiej podkomisji antytrustowej

W październiku 2020 r. zakończyła swoje postępowanie amerykańska parlamentarna Specjalna Podkomisja ds. Antytrustowych, Konkurencji i Prawa Administracyjnego (Subcommittee on Antitrust, Commercial and Administrative Law), która zbadała działalność Google'a, Apple'a, Facebooka i Amazona pod kątem zagrożeń wolnej konkurencji. W raporcie końcowym stwierdzono, że (…) *firmy te wykorzystują swoją dominację w sposób, który niszczy konkurencyjność, zagraża prywatności Amerykanów w sieci, prowadzi do zaniku wolnych i spluralizowanych mediów. Efektem jest spadek innowacyjności, mniejsza różnorodność oferty rynkowej i osłabienie demokracji* (…). *Potęga tych firm jest zbyt wielka i musi zostać okiełznana poprzez objęcie ich odpowiednim nadzorem i sankcjami*[60].

Przedmiotem badań podkomisji była także działalność chmury Amazona. Jest ona coraz bardziej zyskownym obszarem działalności firmy, gdyż zapewniając 15 proc. przychodów, jednocześnie generuje aż połowę jej dochodu operacyjnego (dane za 2019 r.)[61]. W odniesieniu do AWS we wspomnianym raporcie stwierdza się, że istotnym

[59] Pozew Parlera przeciwko AWS złożony 2 III 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/03/parler-llc-v-amazon.pdf [dostęp: 4 III 2021].

[60] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020 r., https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf, s. 7 [dostęp: 12 III 2020].

[61] Tamże, s. 316.

problemem jest brak możliwości przenoszenia danych użytkowników między chmurami. Firmy, które próbowały migrować z chmury Amazona do innej, wskazywały, że jest to bardzo trudne i kosztowne[62]. Przyczyną tego zjawiska jest brak interoperacyjności różnych systemów chmurowych. Monopolistyczną pozycję Amazona w tym segmencie rynku utrwala także to, że specjalistów umiejących obsługiwać chmurę tej firmy jest najwięcej, co wynika z jej popularności. Konkurencja wypada pod tym względem znacznie gorzej i jest to kolejna przyczyna, dla której firmom tak trudno jest się przenieść na inne platformy[63]. Dla wielu klientów taka migracja byłaby kosztowna również ze względu na wymuszony przestój w prowadzeniu działalności. W raporcie podkomisja wskazała ponadto, że dzięki wglądowi w szczegóły funkcjonowania infrastruktury chmurowej Amazon ma szeroki dostęp (*near perfect intelligence*) do informacji o całokształcie działalności użytkowników, co zapewnia mu nieuczciwą przewagę nad nimi[64]. Co więcej, firma celowo analizuje działalność swoich kontrahentów, aby tworzyć własną, konkurencyjną ofertę[65]. Klienci usług chmurowych Amazona są często jednocześnie jego konkurentami[66]. Przykładowo, Netflix w 2018 r. zapłacił za korzystanie z chmury AWS pół miliarda dolarów i jednocześnie rywalizował z jego usługą streamingu filmów Amazon Prime Video[67]. Stwierdzono również, że chociaż trudno jest ustalić, jaki dokładnie udział w zapewnianiu usług w chmurze w USA w ramach kontraktów rządowych ma Amazon, to istniejące dane wskazują, że prawdopodobnie jest on największym ich dostawcą. Ponadto jest on (…) *jedynym dostawcą usług w chmurze zapewniającym infrastrukturę niejawną*[68]. Podsumowując wątek Amazona, podkomisja podkreśliła w raporcie: *Ponieważ chmura jest rdzeniem infrastruktury, na której opiera się gospodarka cyfrowa, zapewnienie jej otwartości i konkurencyjności jest najważniejsze*[69]. Tymczasem jak wskazuje przykład Parlera, chmura tej firmy może obecnie nie spełniać tych kryteriów. Można odnieść wrażenie, że przy ustalaniu warunków świadczenia usługi chmurowej Amazon kieruje się dużą uznaniowością w interpretowaniu zapisów umów z klientami.

Kontrakt JEDI na usługi chmurowe dla Departamentu Obrony USA

Ogromnego znaczenia usług w chmurze dla bezpieczeństwa państwa dowodzi kontrakt z 2019 r. dotyczący świadczenia takich usług Departamentowi Obrony USA.

62 Tamże, s. 119.

63 Tamże, s. 319.

64 Tamże, s. 43.

65 Tamże, s. 276.

66 Tamże, s. 318.

67 Tamże, s. 252.

68 Tamże, s. 318.

69 Tamże, s. 325.

Planowanysystem nazwano JEDI (nazwa kojarzy się z filmem *Gwiezdne wojny*). Jest to akronim od *Joint Enterprise Defense Infrastructure*, co można przetłumaczyć jako: infrastruktura dla połączonych przedsięwzięć obronnych. Wartość dziesięcioletniego kontraktu wyceniono na 10 mld dolarów. Zgodnie z oficjalnymi informacjami:

> Chmura JEDI jest inicjatywą, która (…) rozwinie główny system technologii chmurowej dla całego Departamentu [Obrony], ze szczególnym uwzględnieniem dostępności w obszarach, gdzie operują nasze wojska – od działań frontowych do szczebla taktycznego włącznie. Chmura JEDI zapewni (…) usługi dla użytkowników o wszystkich poziomach dostępu do informacji niejawnych. Inicjatywa ta stworzy fundament do skutecznej wymiany informacji poprzez ewolucyjne łączenie różnych domen, zaawansowane zdolności analizy danych i najwyższy poziom cyberbezpieczeństwa[70].

Na zdobywcę tego lukratywnego kontraktu typowano Amazona z uwagi na jego wcześniejsze doświadczenia. W 2013 r. firma podpisała bowiem dziewięcioletni kontrakt na chmurę dla służb specjalnych USA[71]. Wbrew przewidywaniom kontrakt JEDI przypadł Microsoftowi. W marcu 2021 r. nadal trwał spór sądowy pomiędzy tymi firmami dotyczący wspomnianego kontraktu[72], co na pewien czas sparaliżowało postęp prac nad jego wdrożeniem[73].

Atrakcyjność kontraktu JEDI nie wynika wyłącznie z jego wartości finansowej. Wygrywająca go firma stałaby się na dekadę najważniejszym zaufanym partnerem amerykańskiego sektora bezpieczeństwa. W ten sposób zyskałaby szczególną pozycję, nie tylko gospodarczą, lecz także polityczną. Nie bez znaczenia byłaby także możliwość wglądu w kluczowy element infrastruktury krytycznej państwa oraz uzyskanie pewnego zakresu kontroli nad nim.

Wnioski

Jeśli korzystanie z chmury niesie za sobą tyle problemów i zagrożeń, to z czego wynika atrakcyjność rynkowa tego rozwiązania? Światło na to zagadnienie rzuca wywiad

---

[70] *About JEDI Cloud*, https://www.cloud.mil/JEDI-Cloud/ [dostęp: 12 III 2021].

[71] C. Metz, *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired, 18 VI 2013 r., https://www.wired.com/2013/06/amazon-cia [dostęp: 6 XI 2020].

[72] Amerykańska armia anulowała zawarty z Microsoftem kontrakt z uwagi na nowe potrzeby armii. Zob. M. Duszczyk, *Pentagon ma problem z Jedi. Amazon bije się z Microsoftem*, cyfrowa.rp.pl, 7 VII 2021 r., https://cyfrowa.rp.pl/globalne-interesy/65535-pentagon-ma-problem-z-jedi-amazon-bije-sie-z-microsoftem [dostęp: 30 VII 2021] – przyp. red.

[73] A. Gregg, *With a $10 billion cloud-computing deal snarled in court, the Pentagon may move forward without it*, „Washington Post", 10 II 2021 r., https://www.washingtonpost.com/business/2021/02/10/jedi-contract-pentagon-biden/ [dostęp: 12 III 2021].

z anonimowym pracownikiem Amazona opublikowany w grudniu 2020 r.[74] Ukazano w nim podejście firmy do jej usług chmurowych. Warto krytycznie odnieść się do tej rozmowy, pamiętając, że strategie tej firmy są zapewne punktem odniesienia dla jej konkurencji.

Do klienta AWS zainteresowanego skorzystaniem z usług chmurowych firmy jest przysyłana (…) *osiemnastokołowa ciężarówka* (…), *modularne centrum danych na kołach, wypełnione dyskami twardymi i przystosowane do podłączenia do centrum danych klienta kablami światłowodowymi. Ta ciężarówka jest strzeżona w czasie transferu i transportu danych przez uzbrojonych strażników*. Jak zauważył pracownik Amazona: (…) *łatwo jest to sprzedać. Jeśli klient przygląda się dostępnym opcjom, to oczywiście, że powie, iż chce wielkiej ciężarówki i uzbrojonych ochroniarzy do transportu danych, a nie jakiś chałowaty system, który opracują na własną rękę*[75]. Ponadto AWS sprzedaje specjalne usługi ułatwiające audyt konfiguracji chmury i rekomendujące możliwości poprawienia ustawień. W ten sposób sprawia, że jego klienci nie muszą dbać o zatrudnianie fachowców, którzy byliby w stanie sami przeprowadzić taką analizę i następnie wdrożyć odpowiednie rozwiązania. Ponadto chmura Amazona pozwala klientom na *outsourcing* przestrzegania regulacji związanych z prywatnością danych. Chodzi tu także o europejskie przepisy, takie jak RODO czy prawo do bycia zapomnianym, rozumiane jako prawo do usunięcia linków do określonych stron z wyników wyszukiwania w danej wyszukiwarce.

Podmiot chcący konkurować w ramach współczesnej gospodarki cyfrowej stoi przed dylematem. Jeśli chce zapewnić jakość usług, do której coraz więcej klientów jest przyzwyczajonych, to przede wszystkim musi zadbać o szybkość i płynność działania interfejsu, jego dostępność z poziomu różnych typów urządzeń, stabilność, niezawodność i bezpieczeństwo danych oraz dokonywanych transakcji. Samodzielne rozwijanie takiego systemu przekracza możliwości wielu nawet dużych podmiotów, a ponadto tego typu próby są obarczone dużym ryzykiem porażki. Alternatywą jest zdanie się na gotowy system, sprawdzony i gwarantowany przez renomowanych dostawców usług chmurowych.

Przed podobnymi dylematami jak firmy stoją państwa i organizacje międzynarodowe. Polski projekt Chmury Krajowej i europejska inicjatywa chmury obliczeniowej znana pod nazwą GAIA-X (wspierana przez Komisję Europejską) to przykłady poważnych trudności z uniezależnieniem się od usług chmurowych oferowanych przez Big Tech. Przedstawiciele rządów oraz firm sektora IT z Niemiec i Francji opublikowali w lutym 2020 r. standardy, według których mógłby funkcjonować projekt GAIA-X[76]. Obejmują one m.in. możliwość zmiany operatora usług chmurowych, europejski system certyfikacji dostawców oraz ochronę przed dostępem do danych przechowywanych

[74] *Inside the Whale: An Interview with an Anonymous Amazonian*, „Logic" 2020, nr 12, 20 XII 2020 r., https://logicmag.io/commons/inside-the-whale-an-interview-with-an-anonymous-amazonian/ [dostęp: 20 III 2021].

[75] Tamże.

[76] *Franco-German Position on GAIA-X*, 19 II 2020 r., https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10 [dostęp: 9 III 2020].

w europejskiej chmurze państw spoza Unii. GAIA-X od początku jej tworzenia ma zakładać suwerenność danych (*data sovereignty by design*). W lutym 2020 r. Microsoft ujawnił, że prowadzi negocjacje z niemieckim ministerstwem gospodarki w sprawie możliwego udziału w GAIA-X[77]. Europejski projekt miał być próbą stworzenia konkurencji dla amerykańskich dostawców, dla których jedyną realną alternatywą jest obecnie chiński Alibaba. Udział Microsoftu w projekcie budzi jednak wątpliwości co do prawdziwości deklaracji o dążeniu do zapewnienia autonomii strategicznym usługom chmurowym. Podobnie jest w przypadku projektu polskiej Chmury Krajowej, w którym partnerami strategicznymi są Microsoft i Google Cloud[78].

Na przykładzie przedsięwzięć GAIA-X oraz Chmura Krajowa widać, że dążenia do suwerenności cyfrowej polegające na opracowywaniu własnych rozwiązań chmurowych napotykają duże trudności w postaci braku samowystarczalności w tym zakresie. W praktyce oznacza to skazanie na korzystanie z oferty amerykańskich, chińskich czy rosyjskich gigantów technologicznych. Fakt, że globalny rynek usług chmurowych jest w rzeczywistości oligopolem zdominowanym przez kilka podmiotów, każe zastanowić się nad kierunkiem, w którym podążają zmiany w strukturze współczesnej sieci. Internet powstał jako sieć zdecentralizowana i rozproszona, a więc taka, w której awaria czy zniszczenie poszczególnych węzłów nie powinny mieć istotnego znaczenia dla funkcjonowania całości. Opisane w niniejszym artykule awarie usług chmurowych Amazona oraz konsekwencje jego arbitralnej decyzji o zakończeniu realizowania usługi dla klienta mogą być uznane za symptomy niebezpiecznej ewolucji Internetu w stronę struktury bardziej scentralizowanej, a zatem w większym stopniu podatnej na awarie najważniejszych węzłów, sabotaż czy cyberataki. Obecnie nie można określić, jak poważne konsekwencje mogłaby mieć awaria chmury Amazona lub jego – niekoniecznie największych – konkurentów.

Trend nieoczekiwanej recentralizacji struktury sieci jest szerszy i nie dotyczy tylko usług chmurowych. Eksperci wskazują na pojawienie się zjawiska określanego jako Splinternet[79], bałkanizacja sieci[80] lub nacjonalizacja – czyli wydzielenie się Internetu chińskiego, rosyjskiego czy też ostatnio indyjskiego. Im więcej sfer życia współczesnego człowieka jest zapośredniczanych cyfrowo przez korzystanie z urządzeń podłączonych do sieci, tym większe znaczenie dla globalnego środowiska bezpieczeństwa

---

[77] S. Stolton, *Microsoft 'in discussions' with Germans on Gaia-X participation*, 25 II 2020 r., https://www.euractiv.com/section/digital/news/microsoft-in-discussions-with-germans-on-gaia-x-participation/ [dostęp: 9 III 2020].

[78] A. Marczyński, *Na Podsłuchu, odcinek 33 – ten o Chmurze Krajowej i jej bezpieczeństwie*, rozmawiał Piotr Konieczny, Niebezpiecznik, 24 III 2021 r., https://niebezpiecznik.pl/post/na-podsluchu-odcinek-33-ten-o-chmurze-krajowej-i-jej-bezpieczenstwie/ [dostęp: 29 III 2021]; por. https://chmura-krajowa.pl/dlaczego-chmura-krajowa/ [dostęp: 29 III 2021].

[79] L.S., *What is the 'splinternet'?*, „The Economist", 22 XI 2016 r., https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [dostęp: 29 III 2021].

[80] B. Sajduk, *Chiński krok w stronę bałkanizacji Internetu*, Nowa Konfederacja, 14 IX 2020 r., https://nowakonfederacja.pl/chinski-krok-w-strone-balkanizacji-internetu/ [dostęp: 29 III 2021].

ma niezakłócone funkcjonowanie Internetu. Trend polegający na jego strukturalnej recentralizacji w postaci umacniania się oligopolu dostawców usług chmurowych zwiększa podatność na destabilizację. Jeżeli do wywołania efektu kaskadowego paraliżującego działania dużych obszarów sieci może przyczynić się prosty błąd programisty, to należy się spodziewać, że podobny efekt może być wywołany intencjonalnie – przez cyberatak. W tym sensie zjawisko polegające na tym, że usługi w chmurze stają się w coraz większym stopniu niewidzialną infrastrukturą Internetu, prowadzi do powstania nowych podatności na destabilizację globalnego środowiska bezpieczeństwa.

Bibliografia

Almorsy M., Grundy J., Müller I., *An analysis of the cloud computing security problem*, w: *Proceedings of the APSEC 2010 Cloud Workshop*, Sydney 2010.

Delamore B., Ko Ryan K.L., *Security as a service (SECaaS) – An overview*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 187–202.

Gunawi H.S. i in., *Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages*, w: *Proceedings of the Seventh ACM Symposium on Cloud Computing (SoCC '16)*, New York 2016, Association for Computing Machinery, s. 1–16.

Gurtowski M., Waszewski J., *Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon*, „Kwartalnik Bellona" 2020, nr 3, s. 37–56.

Kandukuri B.R., Paturi R.V., Rakshit A., *Cloud Security Issues*, w: *Procedings of the 2009 IEEE International Conference on Services Computing*, Washington 2009, IEEE Computer Society, s. 517–520, https://ieeexplore.ieee.org/document/5283911 [dostęp: 23 VII 2021].

Kemmericha T., Agrawala V., Momsen C., *Secure migration to the cloud – In and out*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 205–230.

Ko Ryan, Choo Kim-Kwang Raymond, *Cloud Security Ecosystem*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 1–14.

Ramgovind S., Eloff M.M., Smith E., *The Management of Security in Cloud Computing*, w: *2010 Information Security for South Africa (ISSA 2010)*, 2010 r., Institute of Electrical and Electronics Engineers.

Stake R.E., *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim, Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 623–654.

Tang S., *A systemic theory of the security environment*, „Journal of Strategic Studies" 2004, nr 1, s. 1–34.

The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress.

Turbiville G.H., Mendel W.W., Kipp J.W., *The Changing security environment*, „Military Review" 1997, nr 77, s. 5–10.

Źródła internetowe

About JEDI Cloud, https://www.cloud.mil/JEDI-Cloud/ [dostęp: 12 III 2021].

Allyn B., *Judge Refuses To Reinstate Parler After Amazon Shut It Down*, NPR, 21 I 2021 r., https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down [dostęp: 23 I 2021].

AWS: Amazon web outage breaks vacuums and doorbells, BBC, 26 XI 2020 r., https://www.bbc.com/news/technology-55087054 [dostęp: 7 XII 2020].

Branscombe M., *Why Parler Can't Rebuild a Scalable Cloud Service from Scratch*, The New Stack, 19 I 2021 r., https://thenewstack.io/why-parler-cant-rebuild-a-scalable-cloud-service-from-scratch/ [dostęp: 24 III 2021].

Brodkin J., *Parler says it's back without 'Big Tech' after being kicked off Amazon*, Ars Technica, 15 II 2021 r., https://arstechnica.com/tech-policy/2021/02/parler-says-its-back-without-big-tech-after-being-kicked-off-amazon/ [dostęp: 3 III 2021].

Cameron D., *Every Deleted Parler Post, Many With Users' Location Data, Has Been Archived*, Gizmodo, 11 I 2021 r., https://gizmodo.com/every-deleted-parler-post-many-with-users-location-dat-1846032466 [dostęp: 12 I 2021].

Centrum Doktryn i Szkolenia Sił Zbrojnych, *Analiza środowiska bezpieczeństwa w perspektywie 2035 r.*, Bydgoszcz 2020, https://cdissz.wp.mil.pl/pl/articlespublikacje_cdissz/analiza-srodowiska-bezpieczenstwa-w-perspektywie-2035-roku-pl/ [dostęp: 24 III 2021].

Cimpanu C., *AWS outage impacts thousands of online services*, Zdnet, 25 XI 2020 r., https://www.zdnet.com/article/aws-outage-impacts-thousands-ofonline-services/ [dostęp: 7 XII 2020].

Co to jest kontener?, https://azure.microsoft.com/pl-pl/overview/what-is-a-container/ [dostęp: 24 III 2021].

Cox K., *Parler sues Amazon (again), claims AWS ban sank a billion-dollar valuation*, Ars Technica, 3 III 2021 r., https://arstechnica.com/tech-policy/2021/03/parler-sues-amazon-again-claims-aws-ban-sank-a-billion-dollar-valuation/ [dostęp: 4 III 2021].

Day M., *Amazon Cloud Outage Hits Customers Including Roku, Adobe*, Bloomberg, 25 XI 2020 r., https://www.bloomberg.com/news/articles/2020-11-25/amazon-web-services-outage-hits-cloud-customers [dostęp: 7 XII 2020].

Del Rey J., *Amazon's massive AWS outage was caused by human error*, Recode, 2 III 2017 r., https://www.vox.com/2017/3/2/14792636/amazon-aws-internetoutage-cause-human-error-incorrect-command [dostęp: 11 XII 2020].

Duszczyk M., *Pentagon ma problem z Jedi. Amazon bije się z Microsoftem*, cyfrowa.rp.pl, 7 VII 2021 r., https://cyfrowa.rp.pl/globalne-interesy/65535-pentagon-ma-problem-z-jedi-amazon-bije-sie-z-microsoftem [dostęp: 30 VII 2021].

Dlaczego admin Rzecznika Finansowego powinien dostać podwyżkę?, Problemy Polskiej Branży IT, 12 III 2021 r., https://ppbit.pl/news/dlaczego-admin-rzecznika-finansowego-powinien-dostac-podwyzke/ [dostęp: 12 III 2021].

Edelman G., *The Parler Bans Open a New Front in the 'Free Speech' Wars*, Wired, 13 I 2021 r., https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/ [dostęp: 13 I 2021].

European Network and Information Security Agency, *Cloud Computing. Benefits, risks and recommendations for information security*, rev. B z grudnia 2012 r., https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks--and-recommendations-for-information-security/at_download/file [dostęp: 22 III 2021].

European Network and Information Security Agency, *Critical Cloud Computing. A CIIP perspective on cloud computing services*, wersja 1.0 z listopada 2012 r., opublikowana 14 II 2013 r., https://www.enisa.europa.eu/publications/critical-cloud-computing/at_download/fullReport [dostęp: 22 III 2021].

Franco-German Position on GAIA-X, 19 II 2020 r., https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10 [dostęp: 9 III 2020].

Fung B., *Parler has now been booted by Amazon, Apple and Google*, CNN, 11 I 2021 r., https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html [dostęp: 11 I 2021].

Global cloud services market Q4 2020, Canalys, 2 II 2021 r., https://www.canalys.com/newsroom/global-cloud-market-q4-2020 [dostęp: 5 III 2021].

Gregg A., *With a $10 billion cloud-computing deal snarled in court, the Pentagon may move forward without it*, „Washington Post", 10 II 2021 r., https://www.washingtonpost.com/business/2021/02/10/jedi-contract-pentagon-biden/ [dostęp: 12 III 2021].

Gürses S., Van Hoboken J., *Privacy After the Agile Turn*, w: *Cambridge Handbook of Consumer Privacy*, J. Polonetsky, O. Tene, E. Selinger (red.), Cambridge 2017, Cambridge University Press, https://osf.io/preprints/socarxiv/9gy73/ lub https://osf.io/ufdvb/ [dostęp: 22 III 2021].

Hill K., *Goodbye Big Five*, Gizmodo, 7 II 2019 r., https://gizmodo.com/c/goodbye-big-five [dostęp: 4 III 2021].

Hill K., *I Tried to Block Amazon From My Life. It Was Impossible*, Gizmodo, 22 I 2019 r., https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336 [dostęp: 24 III 2021].

Inside the Whale: An Interview with an Anonymous Amazonian, „Logic" 2020, nr 12, https://logicmag.io/commons/inside-the-whale-an-interview-with-an-anonymous-amazonian/ [dostęp: 20 III 2021].

Judge P., *Fire destroys OVHCloud's SBG2 data center in Strasbourg*, Data Center Dynamics, 10 III 2021 r., https://www.datacenterdynamics.com/en/news/fire-destroys-ovhclouds-sbg2-data-center-strasbourg/ [dostęp: 24 III 2021].

Judge P., *OVH fire: OVHcloud abandons efforts to restart SBG1 data center in Strasbourg*, Data Center Dynamics, 21 III 2021 r., https://www.datacenterdynamics.com/en/news/ovh-fire-ovhcloud-abandons-efforts-restart-sbg1-strasbourg/ [dostęp: 24 III 2021].

Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, 23 I 2020 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf [dostęp: 22 III 2021].

L.S., *What is the "splinternet"?*, „The Economist", 22 XI 2016 r., https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [dostęp: 29 III 2021].

Marczyński A., *Na Podsłuchu, odcinek 33 – ten o Chmurze Krajowej i jej bezpieczeństwie*, Niebezpiecznik, 24 III 2021 r., https://niebezpiecznik.pl/post/na-podsluchu-odcinek-33-ten-o-chmurze-krajowej-i-jej-bezpieczenstwie/ [dostęp: 29 III 2021].

Masnick M., *Parler's Laughably Bad Antitrust Lawsuit Against Amazon*, Techdirt, 13 I 2021 r., https://www.techdirt.com/articles/20210113/11333746046/parlers-laughably-bad-antitrust-lawsuit-against-amazon.shtml [dostęp: 14 I 2021].

Maurer T., Hinck G., *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, sierpień 2020 r., https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf [dostęp: 23 III 2021].

Mehorota K., *Parler's New Partner Has Ties to the Russian Government*, Bloomberg, 22 I 2021 r., https://www.bloomberg.com/news/articles/2021-01-22/parler-s-new-partner-has-ties-to-the-russian-government [dostęp: 23 I 2021].

Mell P., Grance T., *The NIST Definition of Cloud Computing*, wrzesień 2011 r., https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp: 4 III 2021].

Metz C., *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired, 18 VI 2013 r., https://www.wired.com/2013/06/amazon-cia [dostęp: 6 XI 2020].

Miles T., *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters, 12 III 2018 r., https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN [dostęp: 14 I 2021].

Mitigating Cloud Vulnerabilities, National Security Agency, styczeń 2020 r., https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF [dostęp: 3 III 2021].

Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v. 1.00 – luty 2020, https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf [dostęp: 7 VI 2021].

Newman J., *Here's why Parler is still struggling to come back online*, Fast Company, 21 I 2021 r., https://www.fastcompany.com/90596427/parler-coming-back-after-aws-ban [dostęp: 23 I 2021].

Odpowiedź Amazona z 12 I 2021 r. na pozew Parlera, https://beta.documentcloud.org/documents/20449127-amazon_response [dostęp: 13 I 2021].

Paczkowski J., Mac R., *Amazon Is Booting Parler Off Of Its Web Hosting Service*, BuzzFeed, 9 I 2021 r., https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws [dostęp: 11 I 2021].

Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021].

Pozew Parlera przeciwko AWS złożony 2 III 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/03/parler-llc-v-amazon.pdf [dostęp: 4 III 2021].

Sajduk B., *Chiński krok w stronę bałkanizacji Internetu*, Nowa Konfederacja, 14 IX 2020 r., https://nowakonfederacja.pl/chinski-krok-w-strone-balkanizacji-internetu/ [dostęp: 29 III 2021].

Schieber J., *Parler jumps to No. 1 on App Store after Facebook and Twitter ban Trump*, Tech Crunch, 9 I 2021 r., https://techcrunch.com/2021/01/09/parler-jumps-to-no-1-on-app-store-after-facebook-and-twitter-bans/ [dostęp: 11 I 2021].

Schneier B., *Cloud Computing*, Schneier on Security, 4 VI 2009 r., https://www.schneier.com/blog/archives/2009/06/cloud_computing.html [dostęp: 17 III 2021].

Sonnemaker T., *Amazon hits back at Parler's antitrust lawsuit with extensive examples of its violent content, including death threats against politicians, tech CEOs, and BLM supporters*, Business Insider, 13 I 2021 r., https://www.businessinsider.com/amazon-responds-to-parler-lawsuit-cites-violent-content-section-230-2021-1?IR=T [dostęp: 13 I 2021].

Stolton S., *Microsoft 'in discussions' with Germans on Gaia-X participation*, 25 II 2020 r., https://www.euractiv.com/section/digital/news/microsoft-in-discussions-with-germans-on-gaia-x-participation/ [dostęp: 9 III 2020].

Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020 r., https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf [dostęp: 12 III 2020].

Taylor L., *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, „Philosophy & Technology", 20 I 2021 r., https://link.springer.com/article/10.1007/s13347-020-00441-4 [dostęp: 22 III 2021].

Turton W., Gurman M., *Parler Blocked on Apple's App Store After Capitol Riot Review*, Bloomberg, 10 III 2021 r., https://www.bloomberg.com/news/articles/2021-03-10/parler-cuts-ios-team-after-apple-blocks-return-to-app-store [dostęp: 11 III 2021].

Abstrakt

Zakłócenia w działaniu chmury obliczeniowej są bardzo ważnym zjawiskiem z perspektywy globalnego środowiska bezpieczeństwa. W artykule przedstawiono analizę tego problemu, wykorzystując w tym celu metodę studium przypadków. Opisano dwa incydenty o daleko idących konsekwencjach, które jednocześnie są dość typowe dla prezentowanych w literaturze przedmiotu. Po pierwsze, na przykładzie jednej z awarii globalnego dostawcy usług chmurowych omówiono problem rosnącej złożoności usług tego typu. Sprawia ona, że nawet drobna awaria jednego z elementów chmury może wywołać efekty kaskadowe i zakłócenia pracy wielu podmiotów. Po drugie, na przykładzie zablokowania działania sieci społecznościowej Parler przeanalizowano problem uzależnienia się klientów od usług danego dostawcy chmury. To powiązanie powoduje, że niezakłócona migracja do innego dostawcy jest utrudniona, jeśli w ogóle możliwa. Oba wskazane problemy były dotychczas analizowane głównie z perspektywy zagrożeń przedsiębiorstw, np. pod kątem kontynuacji działalności, cyberbezpieczeństwa lub naruszeń prywatności. Pomijany był natomiast fakt, że usługi chmurowe stają się stopniowo niewidzialną infrastrukturą Internetu, co ma niebagatelne znaczenie dla środowiska bezpieczeństwa.

Słowa kluczowe: chmura obliczeniowa, infrastruktura krytyczna, cyberbezpieczeństwo.

The invisible Internet infrastructure – cloud services as a critical element of the security environment. The Amazon case

Abstract

The disruptions in cloud computing are an important aspect in the global security environment. An instrumental case study method has been used to analyse this problem. Two relevant examples are discussed which are typical of literature in the field. Firstly, the problem of the growing complexity of the cloud is described. One of the service outages of a global cloud provider is used as an example. It indicates that even relatively small failures might trigger a cascade effect and far-reaching breakdowns. Secondly, the suspension and – as the result of this suspension – the standstill of the social media company Parler is analysed. It is used as the example of the so-called vendor lock-in problem in cloud computing, which renders undisrupted migration to other vendors particularly hard – and at times even impossible. Aforementioned issues have been so far studied mostly from the perspective of the continuity of enterprises, cybersecurity, or privacy. The key phenomenon crucial for the global security environment is usually omitted, namely that the cloud computing has become "the Internet's invisible infrastructure".

Keywords: cloud computing, critical infrastructure, cybersecurity.

REMIGIUSZ LEWANDOWSKI
ORCID: 0000-0001-7353-9742

DOI: 10.4467/20801335PBW.21.022.14299

Alternatywne narzędzia zdalnej identyfikacji

Przeobrażenia gospodarcze, w tym te wynikające z ograniczeń mających przeciwdziałać rozprzestrzenianiu się pandemii COVID-19, znacznie upowszechniły pracę realizowaną w trybie zdalnym i przyspieszyły cyfryzację gospodarki. Implikuje to jednak coraz większe zagrożenia wynikające z podatności procesów realizowanych w cyberprzestrzeni na różnego rodzaju ryzyko. W kontekście wspomnianych zjawisk szczególnie istotne są zagrożenia związane z tożsamością człowieka i możliwością kradzieży tej tożsamości, tj. bezprawnego wejścia w posiadanie danych osobowych określonej osoby i wykorzystywania ich wbrew jej woli lub poza jej wiedzą. Warto się zatem dogłębnie zastanowić nad adekwatnością środków zdalnej identyfikacji stosowanych obecnie i zasadnością proponowania nowych narzędzi w tym zakresie. Podjęcie refleksji naukowej na ten temat jest tym bardziej zasadne, że jednymi z najszybciej rozwijających się trendów technologicznych są sztuczna inteligencja (ang. *artificial intelligence*, AI) i algorytmizacja, które w coraz większym stopniu są wykorzystywane w działaniach gospodarczych, administracyjnych i dotyczących bezpieczeństwa. Rola AI nabiera szczególnego znaczenia w przypadku procesów związanych z zapewnieniem bezpieczeństwa tożsamości, w tym tych, w których wykorzystuje się algorytmy rozpoznawania twarzy. W niniejszym artykule omówiono problemy wynikające z obecnie stosowanych, klasycznych metod zdalnej identyfikacji tożsamości człowieka oraz przedstawiono propozycję alternatywnego podejścia, bazującego na wykorzystaniu cech biometrycznych i elektronicznego dowodu osobistego. Zastosowano strategię, której podstawą jest porównanie modelu zdalnej identyfikacji opartego na klasycznych metodach z proponowanym nowym modelem. Cechą tych modeli jest, z oczywistych względów, symplifikacja ujętych w nich zjawisk, co prowadzi do stworzenia prototypu rzeczywistości, przy maksymalnym odwzorowaniu tych właściwości, które są ważne z punktu widzenia analizy, oraz pominięciu tych, które są nieistotne[1].

[1] H.G. Adamkiewicz-Drwiłło, *Współczesna metodologia nauk ekonomicznych*, Toruń 2008, s. 172.

Pojęcie tożsamości

Bezpieczeństwo i komfort życia współczesnych społeczeństw zależą m.in. od poziomu rozwoju technologicznego. Jednym z ważniejszych aspektów bezpieczeństwa jest bezpieczeństwo tożsamości, czyli zapewnienie pewności, tj. jednoznacznej wiedzy, co do tożsamości danej osoby. Anglojęzycznym odpowiednikiem pojęcia „tożsamość" jest pojęcie „*identity*", słowo wywodzące się z łacińskiego *idem* oznaczającego „identyczność" oraz „ciągłość". *Merriam-Webster's Dictionary* wskazuje cztery główne znaczenia „*identity*"[2]. Są to: 1a) „wyróżniające cechy charakteru lub osobowość jednostki" albo 1b) „świadomość wspólnych cech określona przez psychologiczne identyfikowanie się"; 2) „stan bycia takim samym jak przedmiot opisu lub wskazania"; 3a) „identyczność istotnej lub wtórnej cechy w różnych warunkach" albo 3b)" identyczność we wszystkim, co składa się na obiektywną rzeczywistość przedmiotu"; 4) „równość dwóch wyrażeń, która zachodzi dla wszystkich wartości występujących w niej zmiennych"[3]. Z kolei *Słownik języka polskiego* PWN podaje pięć znaczeń terminu „tożsamość"[4]. Po pierwsze, oznacza on „identyczność". Jest to więc rozumienie analogiczne do drugiej i trzeciej definicji terminu „*identity*" ujętej w *Merriam-Webster's Dictionary*. Po drugie, jest to „świadomość siebie w odniesieniu do pojedynczego człowieka". Odpowiada to pierwszej definicji „*identity*". Po trzecie, są to „fakty, cechy i dane personalne pozwalające zidentyfikować jakąś osobę", co pozostaje bliskie pierwszej definicji anglojęzycznej ujętej w literze a. Po czwarte, jest to „w odniesieniu do społeczności: świadomość wspólnych cech i poczucie jedności", co odpowiada pierwszej definicji anglojęzycznej ujętej w literze b. Piąte znaczenie terminu „tożsamość" wymieniane przez SJP jest zgodne z objaśnieniem znaczenia „*identity*" podanym przez *Merriam-Webster's Dictionary* w punkcie 4.

W kontekście tematyki niniejszego artykułu istotne jest przede wszystkim ujęcie pojęcia tożsamości jako wiedzy o faktach, cechach i danych personalnych pozwalających zidentyfikować jakąś osobę. Mimo że jest to definicja słownikowa, a nie specjalistyczna i oparta na dogłębnych badaniach z dziedziny socjologii, nauk prawnych czy nauk o bezpieczeństwie, jest ona dość pojemna i kierunkowo prawidłowa, gdyż prowadzi do konkluzji, że tożsamość jest związana z potrzebą identyfikacji danej osoby, tj. zweryfikowania, czy jest ona tą, za którą się podaje, lub tą, za którą ją uważamy. Cechy biometryczne należą do szerszej kategorii danych personalnych i są jedną z podstaw identyfikacji lub weryfikacji tożsamości. Stanowią one część szerszego katalogu danych osobowych, które – zgodnie z rozporządzeniem PE i Rady UE nr 679 z 27 kwietnia 2016 r. – obejmują:

> (…) informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna

[2] https://www.merriam-webster.com/ [dostęp: 1 IX 2020].

[3] Wszystkie tłumaczenia w artykule pochodzą od autora (przyp. red.).

[4] https://sjp.pwn.pl/szukaj/tożsamość.html [dostęp: 1 IX 2020].

> to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[5].

Z kolei w rozporządzeniu PE i Rady UE nr 910 z 23 lipca 2014 r.[6] został sprecyzowany termin „identyfikacja elektroniczna". Zgodnie z art. 3 pkt 1 wspomnianego rozporządzenia oznacza on (…) *proces używania danych* w *postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną*. W Polskiej Normie PN-I-02000 „tożsamość" zdefiniowano natomiast jako (…) *element danych przypisany podmiotowi i wykorzystywany do jego identyfikowania*", a „identyfikowanie" jako (…) *proces zautomatyzowanego rozpoznania określonego użytkownika* w *systemie, możliwy do zrealizowania dzięki zastosowaniu unikalnych nazw*.

Katalog danych personalnych określony przepisami prawa jest otwarty i główną przesłanką jest to, czy dana informacja umożliwia pośrednie lub bezpośrednie zidentyfikowanie konkretnej osoby. W przypadku identyfikacji elektronicznej omawiane dane są zapisane w postaci elektronicznej i – co interesujące – ten katalog może się odnosić także do osób prawnych. Takie pojmowanie danych osobowych (w odniesieniu do osób fizycznych) jest w zasadzie spójne ze słownikowym rozumieniem tożsamości jako faktów, cech i danych personalnych pozwalających zidentyfikować jakąś osobę. Jest to jednak pojmowanie zbyt wąskie i nie obejmuje szczególnego atrybutu tożsamości, jakim jest jestestwo człowieka i to wszystko, co konstytuuje go jako jedną osobę, niepowtarzalną w wymiarze fizycznym i umysłowym. Jak wskazuje Olga Sakson-Obada, wymiar fizyczny jest istotny dla tożsamości, gdyż ciało każdego człowieka jest wyjątkowe, jedyne w swoim rodzaju i ma zestaw cech, jakich nie ma żadna inna istota ludzka[7]. Z kolei wymiar psychiczny ma, według Brunona Hołysta, ogromny wpływ na przebieg procesu stawania się sobą i obejmuje trzy najważniejsze poziomy: poziom przeszłości i pamięci, poziom teraźniejszości i tworzenia nowej wiedzy oraz poziom przyszłości – fantazji i wyobraźni[8].

---

[5] Art. 4 pkt 1) *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* – (Dz. Urz. UE L 119 z 4 V 2016 r.).

[6] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE* (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

[7] O. Sakson-Obada, *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne" 2008, nr 2, s. 29–31.

[8] B. Hołyst, *Bezpieczeństwo jednostki*, Warszawa 2014, s. 236–237.

W literaturze socjologicznej wskazuje się, że tożsamość, w tym tożsamość pojedynczego człowieka, jest zjawiskiem dynamicznym i ulega zmianom pod wpływem interakcji społecznych[9]. Równocześnie jednak tożsamość, zwłaszcza w odniesieniu do grup społecznych, pozostaje czynnikiem zapewniającym trwałość, stabilizację oraz ciągłość[10]. Można przyjąć, że gdy mówi się o dynamice tożsamości człowieka, ma się na myśli nie tylko wymiar kulturowy i światopoglądowy, lecz także biologiczny, związany choćby z procesem starzenia. Z upływem czasu człowiek podlega zmianom. Czy zatem tożsamość człowieka jest zmienna i nietrwała? Jeśli tak, to „ten sam", wydawałoby się, człowiek w perspektywie czasu nie będzie „tym samym" człowiekiem, ale kimś zgoła innym. Jego jednostkowe cechy określające fizyczną, fizjologiczną, genetyczną tożsamość mogą przecież ulec zmianie. Nawet tak, zdawałoby się, trwałe w czasie cechy biometryczne człowieka, jak odcisk jego palca czy nawet DNA[11], mogą się – w sposób intencjonalny lub nieintencjonalny – zmienić. Jak zatem zdefiniować tę tożsamość, pod którą – pomimo zmian zachodzących w czasie – kryje się ten sam człowiek?

Obecnie literatura przedmiotu nie dostarcza wystarczająco satysfakcjonującej definicji pojęcia „tożsamość" w odniesieniu do jednostki. Socjologowie wiążą ją z procesem nadawania ludziom społecznej egzystencji[12]. Krzysztof Gorazdowski łączy tożsamość z kształtującym ją zdobywaniem przez całe życie wiedzy i umiejętności, poszerzaniem zasobów intelektualnych oraz rozbudowywaniem strategii radzenia sobie w różnych sytuacjach życiowych[13]. Wskazuje ponadto na podstawową funkcję tożsamości, którą jest identyfikowanie osoby lub grupy na podstawie wybranych cech[14]. Izabela Jankowska ogranicza pojmowanie tożsamości praktycznie do danych osobowych zawartych w dokumentach tożsamości[15]. Podobne, równie wąskie rozumienie prezentuje Kamil Sowirka[16]. Definicja tożsamości, którą posługuje się Katarzyna Cygan, jest z kolei podobna do tej zawartej w *Słowniku języka polskiego.* Jej zdaniem są to (…) *fakty, cechy, dane personalne pozwalające zidentyfikować jakąś osobę, ale także świadomość siebie*[17].

---

[9] Z. Mach, *Przedmowa*, w: T. Paleczny, *Socjologia tożsamości*, „Rejony Humanistyki" 2015, nr 1, s. 9.

[10] E. Ardener, *Tożsamość i utożsamienie*, w: *Sytuacja mniejszościowa i tożsamość*, Z. Mach, A. Paluch (red.), Kraków 1992, s. 21–42; Z. Bokszański, *Tożsamość, interakcja, grupa: tożsamość jednostki w perspektywie teorii socjologicznej*, Łódź 1989, s. 206–207.

[11] Za prace nad metodami modyfikacji genomu (CRISPR/Cas9) Nagrodę Nobla w dziedzinie chemii otrzymały w 2020 r. Emmanuelle M. Charpentier i Jennifer A. Doudna.

[12] P.L. Callero, *The sociology of Self*, „Annual Review of Sociology" 2003, nr 29, s. 115–133.

[13] K. Gorazdowski, *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, „Studia Administracji i Bezpieczeństwa" 2017, nr 2, s. 91–92.

[14] Tamże, s. 92.

[15] I.M. Jankowska, *Ochrona dokumentów tożsamości w polskim prawie karnym*, „Studia Lubuskie" 2016, t. 12, s. 19.

[16] K. Sowirka, *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 65, 78.

[17] K. Cygan, *Czyn złośliwego podszywania się pod inną osobę*, „Studia Prawnoustrojowe" 2015, nr 29, s. 68.

Zasadne jest więc, zdaniem autora, zaproponowanie własnej definicji tożsamości człowieka. Stanowi ona całokształt wszystkich cech fizycznych, fizjologicznych, genetycznych i psychicznych oraz identyfikatorów w postaci imienia, nazwiska, jak również innych indywidualnie nadanych identyfikatorów, łącznie konstytuujących jego indywidualność i niepowtarzalność. Zgodnie z tą definicją to nie jeden czynnik ani nawet kilka czynników przesądza o tożsamości osoby, lecz ich całokształt. Jak wskazano wcześniej, cechy fizyczne, fizjologiczne oraz genetyczne człowieka mogą ulec zmianie. Dotyczy to również jego atrybutów psychicznych, w tym nawet – na skutek choroby – osobistych przekonań o własnej tożsamości. Te zmiany nie powodują jednak, że mamy do czynienia z nową tożsamością, nigdy nie odbywają się one bowiem *en bloc*. Zarówno naturalny proces starzenia, jak i choroby nie modyfikują wszystkich indywidualnych cech danego człowieka. Nawet celowa manipulacja tymi cechami, w tym interwencja medyczna, nie jest możliwa w stosunku do wszystkich cech konstytuujących indywidualność i niepowtarzalność danego człowieka. Stosunkowo łatwa natomiast może być próba dokonania zmiany identyfikatorów takich, jak imię i nazwisko czy numer PESEL lub innych indywidualnych identyfikatorów służących np. do uwiarygodniania się w systemach teleinformatycznych. To najczęściej spotykane przykłady kradzieży tożsamości, polegające na posłużeniu się cudzymi danymi osobowymi przez osobę nieupoważnioną i przybraniu cudzej tożsamości[18]. Jednak tego rodzaju zdarzenia stwarzają jedynie pozory nowej czy cudzej tożsamości. Przestępca przybierający cudze imię i nazwisko nie uzyskuje tożsamości prawowitego właściciela tych danych osobowych, nie jest bowiem w stanie przejąć całokształtu cech konstytuujących indywidualność i niepowtarzalność drugiego człowieka. Rację ma zatem Piotr Girdwoyń, który zwraca uwagę, że (…) *przypisywanie jakiejkolwiek cesze (lub zespołowi cech) obiektu identyfikowanego waloru unikalności nie wydaje się możliwe, gdyż zawsze jej rzadkość, stanowiąca podstawową przesłankę indywidualności, jest odnoszona w najlepszym wypadku jedynie do klasy wszystkich przebadanych obiektów danego rodzaju i nie musi mieć waloru uniwersalnego*[19]. Raz jeszcze należy więc podkreślić, że pewność co do tożsamości człowieka nie może być oparta wyłącznie na jednej czy kilku jego cechach lub identyfikatorach. Absolutną pewność może dać jedynie całokształt tych cech i identyfikatorów, chociaż w praktyce, z przyczyn pragmatycznych, mamy do czynienia z pewnością opartą na rachunku prawdopodobieństwa (o ile dane zjawisko jest możliwe do skwantyfikowania) lub zwykłym subiektywnym osądzie[20].

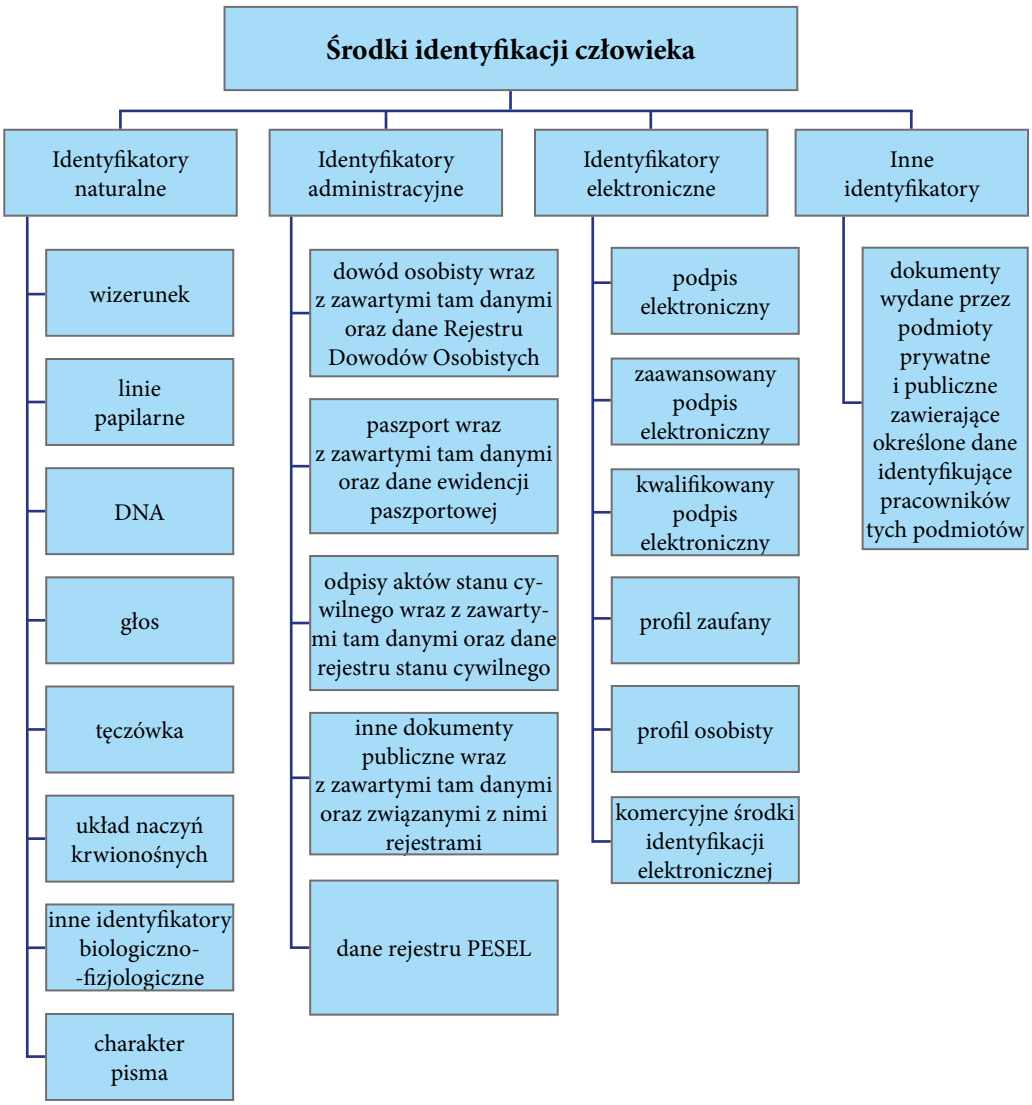
[18] A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 29.

[19] P. Girdwoyń, *Zarys kryminalistycznej taktyki obrony*, Kraków 2004, s. 223.

[20] J. Moszczyński, *Dylematy identyfikacji indywidualnej i grupowej*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, s. 184–185.

Zdalna identyfikacja

W praktyce do identyfikacji człowieka są wykorzystywane różne środki. Przedstawiono je na schemacie zamieszczonym poniżej.



Schemat. Klasyfikacja środków służących do identyfikacji człowieka.

Źródło: Opracowanie własne.

W przypadku środków identyfikacji elektronicznej należy wskazać podstawowe procesy, w których są one wykorzystywane. W literaturze przedmiotu najczęściej wymienia się cztery, tj.:

a) rejestrację,
b) weryfikację tożsamości i wydanie środków identyfikacji elektronicznej,
c) uwierzytelnienie,
d) autoryzację.

Powyższe procesy składają się na identyfikację zdalną. Etap rejestracji obejmuje deklarację tożsamości wraz z przekazaniem określonych atrybutów tożsamości, np. imienia i nazwiska (identyfikatorów administracyjnych) lub cech biometrycznych (identyfikatorów naturalnych) takich, jak wizerunek twarzy czy odciski palców. Najważniejszym zadaniem jest sprawdzenie, czy zadeklarowane dane rzeczywiście należą do osoby je przedstawiającej. Służy temu proces weryfikacji tożsamości, polegający na skonfrontowaniu deklarowanych danych z danymi ujętymi w wiarygodnych źródłach. Przykładowo, klasyczną metodą weryfikacji tożsamości jest porównanie deklarowanych danych osobowych z danymi w dowodzie osobistym oraz porównanie wizerunku twarzy osoby podlegającej weryfikacji z wizerunkiem widniejącym w jej dowodzie osobistym. Istotna w tym przypadku jest możliwość powiązania analizowanych danych osobowych z tożsamością fizyczną takiej osoby, stąd porównanie wizerunku twarzy jako cechy składającej się na tożsamość fizyczną. Możliwe jest wykorzystanie także innych niż dowód osobisty źródeł danych, z zastrzeżeniem jednak, że powinny one być wiarygodne i wymagać wykazania związku z tożsamością fizyczną (na etapie ich użycia w procesie weryfikacji lub na etapie ich wydania). Na podstawie pozytywnej weryfikacji tożsamości mogą zostać wydane środki identyfikacji elektronicznej, tj. materialne lub niematerialne jednostki zawierające dane identyfikujące osobę i używane do celów uwierzytelniania podczas usługi online. Powstaje w ten sposób tożsamość elektroniczna, która – poprzez użycie otrzymanych środków identyfikacji elektronicznej – może być wykorzystywana w cyberprzestrzeni, jednak każdorazowo będzie ona podlegać uwierzytelnieniu i autoryzacji. Należy przy tym podkreślić, że istnieją procesy identyfikacji elektronicznej, w których weryfikacja tożsamości nie następuje (są przyjmowane zadeklarowane dane osobowe), lub takie, w których weryfikacja ma bardzo uproszczoną formę, np. polega na przesłaniu pocztą elektroniczną skanu dowodu osobistego. Dotyczy to jednak sytuacji, w których poziom ryzyka wynikający z takich odstępstw jest akceptowalny.

Uwierzytelnienie oznacza weryfikację zadeklarowanej tożsamości elektronicznej, np. przez podanie właściwego hasła przypisanego do indywidualnego loginu osoby uprawnionej do korzystania z danego systemu lub zbioru danych czy też porównanie przekazywanych danych biometrycznych z danymi przyporządkowanymi do wskazanej tożsamości. Z kolei autoryzacja jest procesem potwierdzającym, czy użytkownik ma uprawnienie do wykonania określonej operacji (np. zlecenia transakcji przelewu) lub uprawnienie dostępu do określonego zasobu (np. pliku). Celem autoryzacji jest kontrola dostępu, a zatem następuje ona po uwierzytelnianiu. W art. 4 pkt 29 dyrektywy PE i Rady UE nr 2366 z 25 listopada 2015 r.[21] zdefiniowano jednak uwierzytelnienie

[21] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE,*

znacznie szerzej, jako (…) *procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika*.

Wskazane powyżej cztery procesy składają się na proces identyfikacji zdalnej, tj. sprawdzenie z odpowiednim poziomem ufności, czy dana osoba usiłująca dokonać określonej czynności w sposób zdalny jest osobą do tego uprawnioną, i pozyskanie informacji określających tożsamość tej osoby. Środki identyfikacji elektronicznej różnią się między sobą konstrukcją technologiczną i poziomem bezpieczeństwa. Powszechnie stosowane są środki identyfikacji polegające na indywidualnie przyporządkowanym do użytkownika loginie (i haśle), wydanym na podstawie samodzielnej rejestracji w określonym systemie informatycznym, z pominięciem etapu weryfikacji tożsamości. W kontaktach z podmiotami sektora publicznego środkiem identyfikacji elektronicznej szeroko stosowanym w Polsce jest profil zaufany. Znacznie rzadziej obywatele naszego kraju korzystający z usług tego sektora posługują się elektronicznym dowodem osobistym (profil osobisty). W sektorze komercyjnym klasycznymi środkami identyfikacji elektronicznej są elektroniczny podpis kwalifikowany oraz bankowe środki identyfikacji elektronicznej. Ponadto funkcjonuje wiele różnego rodzaju innych środków, których poziom bezpieczeństwa jest znacznie niższy.

Specyfika niektórych czynności realizowanych za pośrednictwem sieci wymaga uzyskania pewności co do tożsamości osoby, która je wykonuje. Dotyczy to zwłaszcza czynności prawnych (np. składanie oświadczeń woli), zatwierdzania określonych czynności w systemach teleinformatycznych organizacji i przeprowadzania transakcji finansowych w systemach bankowości internetowej lub mobilnej. Podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi zostały uregulowane w rozporządzeniu PE i Rady UE nr 910 z 23 lipca 2014 r.[22] Wybór określonego środka identyfikacji elektronicznej powinien być uzależniony od niezbędnego poziomu bezpieczeństwa dla danej czynności wymagającej uwierzytelnienia w cyberprzestrzeni. Poziom wymaganego bezpieczeństwa oznacza stopień, w jakim można mieć zaufanie do danego identyfikatora elektronicznego przy ustalaniu tożsamości osoby, która się nim posługuje. Poziom ten zależy zatem od stopnia zaufania do podawanej lub zgłaszanej tożsamości danej osoby zapewnianego przez ten identyfikator, przy uwzględnieniu określonych procesów (np. potwierdzanie i weryfikowanie tożsamości oraz uwierzytelnianie), działań zarządczych (np. działania jednostki wydającej identyfikator elektroniczny i procedury wydawania takich identyfikatorów) oraz stosowanych zabezpieczeń technicznych.

2009/110/ WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/ WE (Dz. Urz. UE L 337 z 23 XII 2015 r.).

[22] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE* (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

W przypadku notyfikowanego systemu identyfikacji elektronicznej istnieje wymóg określenia poziomu bezpieczeństwa środka identyfikacji elektronicznej wydanego w ramach tego systemu[23]. Niski poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia ograniczony stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest obniżenie ryzyka podszycia się lub modyfikacji tożsamości*[24]. Średni poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia średni stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest znaczne obniżenie ryzyka podszycia się lub modyfikacji tożsamości*[25]. Przykładem takiego środka jest profil zaufany. Wysoki poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia wyższy stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby niż środek identyfikacji elektronicznej o średnim poziomie pewności i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest zapobieganie podszyciu się lub modyfikacji tożsamości*[26]. Przykładami takich środków są profil osobisty oraz kwalifikowany podpis elektroniczny.

Szczegółowe, minimalne specyfikacje techniczne i procedury dotyczące poziomów zaufania w zakresie środków identyfikacji elektronicznej, zwłaszcza podpisu elektronicznego, zaawansowanego podpisu elektronicznego oraz kwalifikowanego podpisu elektronicznego, są określone w rozporządzeniu wykonawczym Komisji UE nr 1502 z 8 maja 2015 r.[27]

Weryfikacja tożsamości ma szczególne znaczenie, o czym już wspomniano, w sektorze bankowym. Zgodnie ze stanowiskiem Urzędu Komisji Nadzoru Finansowego (UKNF) z 5 czerwca 2019 r. w przypadku, gdy nie ma możliwości skorzystania z powyższych środków identyfikacji elektronicznej, bank powinien rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego[28]. Obowiązkiem banku jest ustalenie, jakimi dokumentami, danymi oraz informacjami (tj. materiałami weryfikacyjnymi) należy się w takiej sytuacji posługiwać w celu weryfikacji tożsamości klienta, a także jakie

[23] Tamże, art. 8 ust. 1.

[24] Tamże, art. 8 ust. 2 lit. a.

[25] Tamże, art. 8 ust. 2 lit. b.

[26] Tamże, art. 8 ust. 2 lit. c.

[27] *Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 maja 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym* (Dz. Urz. UE L 235 z 9 IX 2015 r.).

[28] https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf [dostęp: 1 IX 2020].

sposoby uzyskiwania dostępu do materiałów weryfikacyjnych będą stosowane. Ponadto w celu zdalnej weryfikacji tożsamości klienta bank powinien rozważyć posłużenie się różnymi materiałami weryfikacyjnymi pochodzącymi z wiarygodnych i niezależnych źródeł. W przypadku weryfikacji tożsamości osoby fizycznej przynajmniej jeden z materiałów weryfikacyjnych powinien być dokumentem stwierdzającym tożsamość (dowód osobisty, paszport, karta pobytu). Innym tego rodzaju materiałem wskazanym przez UKNF jest dokument ze zdjęciem, np. prawo jazdy. Za uzupełniające dokumenty potwierdzające tożsamość klienta i adres jego pobytu można uznać np. rachunki za media. Dodatkowym środkiem bezpieczeństwa, którego stosowanie jest oczekiwane przez UKNF, jest zrealizowanie pierwszej transakcji za pomocą przelewu bankowego z rachunku klienta (prowadzonego w innej instytucji obowiązanej) na rzecz banku weryfikującego jego tożsamość. Z uwagi jednak na minimalny zakres danych osobowych zawartych w informacji o przelewie, powinny one służyć pomocniczo do weryfikacji tożsamości klienta.

Metodą dopuszczoną przez UKNF jest także wideoweryfikacja. W tym przypadku konieczne jest przeprowadzenie analizy ryzyka, z uwzględnieniem m.in. modelu funkcjonowania usługi, możliwych do zastosowania technologii i dostosowanych do nich mechanizmów kontrolnych zapewniających odpowiedni poziom bezpieczeństwa usługi, zwłaszcza mitygowanie różnych rodzajów ryzyka[29] związanych z prawidłową identyfikacją i weryfikacją klienta (np. ryzyka kradzieży tożsamości), w tym odnoszących się do wiarygodności materiałów weryfikacyjnych. Zgodnie ze stanowiskiem UKNF bank może uzyskiwać dostęp do materiałów weryfikacyjnych za pomocą wideorozmowy, podczas której pracownik banku ma możliwość bliższej obserwacji klienta i przedstawionych przez niego oryginałów dokumentów, a także upewnienia się, że materiały weryfikacyjne nie zostały sfałszowane, porównania fotografii w dokumencie tożsamości z osobą, z którą rozmawia, oraz sprawdzenia klienta w wiarygodnych bazach danych. Niezależnie od powyższego bank powinien wziąć pod uwagę czynniki behawioralne, które mogą wskazywać, że klient np. jest pod wpływem środków odurzających, nie działa samodzielnie bądź nie jest świadomy, że nawiązuje relację z bankiem.

Zgodnie z art. 79 dyrektywy PE i Rady UE nr 2366 w sprawie usług płatniczych w ramach rynku wewnętrznego[30] państwa członkowskie mają zapewnić stosowanie przez dostawcę usług płatniczych silnego uwierzytelniania klienta, w przypadku gdy płatnik: a) uzyskuje dostęp do swojego rachunku płatniczego w trybie online; b) inicjuje elektroniczną transakcję płatniczą; c) przeprowadza czynność za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć. W sytuacji inicjowania elektronicznych transakcji płatniczych państwa członkowskie są natomiast zobowiązane do tego, aby w odniesieniu do elektronicznych zdalnych

[29] Mitygowanie ryzyka – podejmowanie działań zmierzających do obniżenia poziomu ryzyka do akceptowalnego poziomu (przyp. red.).

[30] Dyrektywa została implementowana do polskiego prawa w ramach znowelizowanej *Ustawy* z *dnia 19 sierpnia 2011 r.* o *usługach płatniczych* (DzU z 2011 r. nr 199 poz. 1175, ze zm.), a omawiany przepis tej dyrektywy ujęto w art. 32i wspomnianej ustawy.

transakcji płatniczych dostawcy usług płatniczych stosowali silne uwierzytelnianie klienta, obejmujące elementy, które dynamicznie łączą transakcję z określoną kwotą i określonym odbiorcą. Przez silne uwierzytelnianie klienta należy rozumieć uwierzytelnianie z wykorzystaniem co najmniej dwóch elementów (niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych) należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co ma wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających (art. 4 pkt 30 dyrektywy PE i Rady UE nr 2366).

Słabe strony zdalnej identyfikacji i związane z tym wyzwania

Podstawowym mankamentem współcześnie stosowanych środków identyfikacji elektronicznej jest to, że potwierdzają one jedynie fakt posiadania przez osobę identyfikującą się (uwierzytelniającą się lub autoryzującą określoną czynność) indywidualnych środków przypisanych uprawnionej osobie (loginów, haseł itd.). Wspomniane środki nie pozwalają bowiem na weryfikację, kto fizycznie się nimi posługuje. A zatem współczesna zdalna identyfikacja odbywa się na podstawie domniemania, że środki identyfikacji są zawsze w wyłącznym posiadaniu osób uprawnionych. Praktyka wskazuje natomiast, że jest możliwe przejęcie tego rodzaju danych pozwalających podszywać się pod inną osobę (kradzież tożsamości). Stosowane obecnie środki nie spełniają podstawowego celu uwierzytelnienia, którym jest weryfikacja tożsamości użytkownika usług, a jedynie weryfikują posiadanie przez użytkownika wymaganych indywidualnych danych. Ponieważ możliwe jest ich przejęcie przez przestępców, dlatego przy zdalnym dokonywaniu transakcji nie ma pewności, kto faktycznie dokonuje tych operacji. Wiadomo jedynie, że są one realizowane przez osobę dysponującą danymi uwierzytelniającymi, tj. indywidualnymi cechami zapewnianymi przez dostawcę usług użytkownikowi do celów uwierzytelnienia.

Należy zaznaczyć, że art. 66 dyrektywy PE i Rady UE nr 2366 dotyczący usług płatniczych realizowanych w ramach rynku wewnętrznego nakłada na dostawców usług inicjowania płatności obowiązek zapewnienia, aby indywidualne dane uwierzytelniające użytkownika usług płatniczych nie były – z wyjątkiem użytkownika i wydawcy takich indywidualnych danych uwierzytelniających – dostępne dla innych stron oraz by były przekazywane przez dostawcę świadczącego usługę inicjowania płatności za pośrednictwem bezpiecznych i wydajnych kanałów. Równocześnie, zgodnie z art. 69 wspomnianej dyrektywy, użytkownik usług płatniczych z chwilą otrzymania instrumentu płatniczego jest zobowiązany do podjęcia wszelkich racjonalnych kroków, aby chronić swoje indywidualne dane uwierzytelniające. Dostawca usług płatniczych wydający instrument płatniczy jest z kolei zobowiązany do upewnienia się, że indywidualne dane uwierzytelniające nie są dostępne dla stron innych niż użytkownik usług płatniczych, który jest uprawniony do używania tego instrumentu płatniczego (art. 70). Niemniej jednak te wymogi nie eliminują ryzyka przejęcia rzeczonych danych przez

przestępców. Przyczyną opisanych słabości zdalnej identyfikacji jest charakter weryfikowanych danych. Nawet po wdrożeniu procedur uwzględniających silne uwierzytelnienie banki najczęściej korzystają z cech należących wyłącznie do dwóch obszarów: coś, co wiem (np. hasło logowania) i coś, co posiadam (np. telefon komórkowy, na który przychodzą wiadomości SMS z kodami do autoryzacji, lub urządzenie mobilne, na którym jest zainstalowany program (token) wyświetlający kody do autoryzacji). Rzadko są uwzględniane cechy z obszaru: coś, czym jestem, tj. indywidualne cechy użytkownika, ograniczone w zasadzie do jego cech biometrycznych. Korzystanie z cech biometrycznych jest w omawianej sytuacji utrudnione, gdyż generuje wymóg dysponowania wzorcem, z którym należałoby porównywać weryfikowane dane. Z uwagi na wrażliwy charakter danych biometrycznych i społeczną niechęć do ich przekazywania nie są one przechowywane w bazach banków. W przypadkach stosowania biometrii w systemach bankowych (głównie w odniesieniu do aplikacji mobilnych) dane biometryczne (najczęściej odciski palców) nie są przechowywane w banku, lecz zapisane tylko i wyłącznie na karcie kryptograficznej, którą posiada użytkownik. Takie lokalne umieszczenie danych biometrycznych może wydawać się wygodne, lecz generuje ryzyko przejęcia tego wzorca przez przestępców i zastąpienia go danymi osoby nieuprawnionej, np. w celu uzyskania kontroli nad rachunkiem bankowym i wytransferowania z niego środków finansowych. Nie istnieje także krajowa baza danych biometrycznych wszystkich obywateli, która mogłaby służyć jako źródło omawianych wzorców.

Pewną alternatywną próbą wykorzystania biometrii w bankowości jest wspomniana już wideoweryfikacja, w ramach której pracownik banku w czasie rzeczywistym weryfikuje tożsamość klienta przez porównanie jego wizerunku z kamery z wizerunkiem widniejącym na fotografii dokumentu tożsamości okazanego także do kamery. Słabymi stronami tego rozwiązania są: stosunkowo długi czas weryfikacji (ograniczający stosowanie tej metody wyłącznie do nawiązywania relacji gospodarczych i wykluczający posługiwanie się nią w celu uwierzytelniania), trudność związana z poprawną zdalną weryfikacją autentyczności dowodu tożsamości (wyłącznie przez obraz z kamery), ograniczone zdolności pracowników banków w zakresie weryfikacji tożsamości na podstawie wizerunku. Omawianą metodę należy więc uznać za jedynie pozornie bezpieczną.

Nowy model zdalnej identyfikacji

Odpowiedzią na zdiagnozowane słabości stosowanych obecnie środków i metod identyfikacji elektronicznej może być przedstawiony w niniejszym artykule model bazujący na zdalnej identyfikacji za pomocą danych biometrycznych zapisanych w dokumencie tożsamości – elektronicznym dowodzie osobistym lub paszporcie. Zamysł tego rozwiązania opiera się na wykorzystaniu w procesie weryfikacji:

1) danej biometrycznej w postaci wizerunku twarzy pobieranego w czasie rzeczywistym w trakcie identyfikacji (uwierzytelniania lub autoryzacji) z kamery telefonu komórkowego lub komputera,

2) wzorca biometrycznego w postaci wizerunku twarzy zapisanego w mikroprocesorze dowodu osobistego[31] lub paszportu[32].

Proces weryfikacji tożsamości z zastosowaniem omawianego modelu obejmuje następujące kroki:

1. Pozyskanie dostępu aplikacji do mikroprocesora przez zdjęcie pola MRZ dokumentu.
2. Automatyczną weryfikację statusu dokumentu (certyfikatu na chipie CSCA/CVCA).
3. Automatyczny odczyt danych z mikroprocesora przy użyciu czytnika NFC wbudowanego w telefon lub laptop:
   – DG1: Wydawca dokumentu,
   – DG1: Numer dokumentu,
   – DG1: Data narodzin,
   – DG1: Płeć,
   – DG1: Data wygaśnięcia dokumentu,
   – DG1: Narodowość,
   – DG1: Imię i nazwisko posiadacza dokumentu,
   – DG2: Biometryczne zdjęcie twarzy posiadacza dokumentu.
4. Wykonanie fotografii twarzy przez użytkownika z techniczną pomocą aplikacji.
5. Weryfikację funkcji życiowych użytkownika (sprawdzenie wiarygodności danych uzyskanych dzięki działaniu wskazanemu w pkt 4, tzn. tego, czy przed telefonem lub laptopem jest faktycznie żywa osoba, czy też jest to podstawione zdjęcie lub obraz wideo).
6. Weryfikację tożsamości użytkownika na podstawie algorytmicznej analizy obrazów: wizerunku twarzy z mikroprocesora oraz wizerunku twarzy pobranej w czasie rzeczywistym z kamery.
7. Raportowanie wyniku weryfikacji: weryfikacja pozytywna lub weryfikacja negatywna.
8. Opcjonalną ponowną weryfikację tożsamości w przypadku negatywnego wyniku pierwszej weryfikacji lub wsparcie użytkownika w procesie weryfikacji przez zdalnego konsultanta.
9. Archiwizację procesu weryfikacji tożsamości w systemie bankowym.

Wyjątkowymi zaletami omawianego modelu są:

1) wykorzystanie zaufanego i powszechnego środka identyfikacji w postaci dowodu osobistego lub paszportu,

[31] Dowody osobiste wydawane obecnie w Polsce są wyposażone w mikroprocesory zawierające dane biometryczne. Od 2 sierpnia 2021 r. biometryczne dowody osobiste (z dwiema cechami) obowiązują na terenie całej UE.

[32] Wszystkie paszporty wydawane obecnie w kraju i na świecie są wyposażone w mikroprocesory zawierające dane biometryczne.

2) uniwersalny charakter wykorzystanego środka identyfikacji, tj. polskich i zagranicznych paszportów oraz dowodów osobistych,
3) wykorzystanie danych biometrycznych, dających wymaganą i obiektywną pewność co do wyniku weryfikacji tożsamości,
4) uzyskanie pewności co do autentyczności dowodu osobistego lub paszportu,
5) łatwość i szybkość procesu weryfikacji tożsamości, niewymagającego żadnego oprzyrządowania poza telefonem komórkowym lub laptopem z kamerą i czytnikiem NFC,
6) duża liczba różnego rodzaju zastosowań w sektorze bankowym i innych sektorach (pozyskiwanie nowych klientów, autoryzacja transakcji, uwierzytelnianie w kanałach zdalnych, identyfikacja w bankowości oddziałowej i inne),
7) niski poziom błędu.

Dzięki automatyzacji procesu oraz bazowaniu na danych zapisanych na mikroprocesorze w przedstawionym modelu zostaje wyeliminowany subiektywizm w ocenie autentyczności dokumentu oraz w ocenie zgodności wizerunku klienta z jego wizerunkiem w dowodzie tożsamości. W ten sposób można znacznie podnieść poziom bezpieczeństwa tożsamości i transakcji realizowanych w systemach bankowych oraz innego rodzaju transakcji wymagających pewności co do tożsamości wykonujących je osób. Poziom trafności modelu, tj. prawidłowe powiązanie wizerunku użytkownika w czasie rzeczywistym z jego zdjęciem z dowodu osobistego (lub paszportu), jest uzależniony od ustalonego przez bank minimalnego poziomu zgodności (pomiędzy zdjęciem „na żywo" a wzorcem wizerunku zapisanym na dokumencie) i wynika z zastosowanych bibliotek algorytmów rozpoznawania twarzy.

Bibliografia

Adamkiewicz-Drwiłło H.G., *Współczesna metodologia nauk ekonomicznych*, Toruń 2008, TNOiK.

Ardener E., *Tożsamość i utożsamienie*, w: *Sytuacja mniejszościowa i tożsamość*, Z. Mach, A. Paluch (red.), Kraków 1992, Wydawnictwo UJ, s. 21–42.

Bokszański Z., *Tożsamość, interakcja, grupa: tożsamość jednostki w perspektywie teorii socjologicznej*, Łódź 1989, Wydawnictwo UŁ.

Callero P.L., *The sociology of the Self*, „Annual Review of Sociology" 2003, nr 29, s. 115–133.

Cygan K., *Czyn złośliwego podszywania się pod inną osobę*, „Studia Prawnoustrojowe" 2015, nr 29, s. 59–79.

Girdwoyń P., *Zarys kryminalistycznej taktyki obrony*, Kraków 2004, Zakamycze.

Gorazdowski K., *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, „Studia Administracji i Bezpieczeństwa" 2017, nr 2, s. 89–102.

Hołyst B., *Bezpieczeństwo jednostki*, Warszawa 2014, Wydawnictwo Naukowe PWN.

Jankowska I.M., *Ochrona dokumentów tożsamości w polskim prawie karnym*, „Studia Lubuskie" 2016, t. 12, s. 13–28.

Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 29–39.

Mach Z., *Przedmowa*, w: T. Paleczny, *Socjologia tożsamości*, „Rejony Humanistyki" 2015, nr 1, s. 7–16.

Moszczyński J., *Dylematy identyfikacji indywidualnej i grupowej*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Volumina.pl.

Sakson-Obada O., *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne" 2008, nr 2, s. 27–44.

Sowirka K., *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 64–80.

Źródła internetowe

https://www.merriam-webster.com/.

Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf.

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – (Dz. Urz. UE L 119 z 4 V 2016 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23 XII 2015 r.).

Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 maja 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 9 IX 2015 r.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (DzU z 2011 r. nr 199 poz. 1175, ze zm.).

Abstrakt

W pracy przeanalizowano proces zdalnej identyfikacji w tej postaci, w jakiej jest on realizowany obecnie. Na tej podstawie zdiagnozowano najważniejsze słabe strony metod wykorzystywanych w tym procesie. W przypadku metod niebiometrycznych ich główną słabością jest ograniczenie ich stosowania do weryfikacji określonych danych uwierzytelniających posiadanych przez użytkownika (osobę weryfikującą się), a nie do weryfikacji tożsamości *per se*. Z kolei stosowane współcześnie metody biometryczne są czasochłonne i obarczone subiektywizmem w ocenie zgodności danych biometrycznych ze wzorcem. Alternatywę dla tych metod stanowi zaprezentowany w niniejszym artykule model, który jest oparty na w pełni zautomatyzowanej, zdalnej identyfikacji biometrycznej, wykorzystującej jako wzorzec dane biometryczne zawarte w dokumentach osobistych i paszportach. Model jest wolny od słabości i ograniczeń innych analizowanych biometrycznych i niebiometrycznych metod identyfikacji i charakteryzuje się bardzo niskim poziomem błędu.

Słowa kluczowe: biometria, identyfikacja, uwierzytelnienie, autoryzacja, tożsamość.

Alternative tools of remote identification and authentication

Abstract

The paper presents an analysis of the present-day process of remote identification. On this basis, the most important weaknesses of the methods were diagnosed. With regard to non-biometric methods, the main weakness and limitation is that they only verify

if the user (the person being verified) has appropriate credentials, and they do not verify the identity per se. On the other hand, the currently applied biometric methods are time-consuming and subjective in assessing the compliance of biometric data with the template. An alternative to these methods is a model, presented in this paper, which is based on fully automated, remote biometric identification using biometric data contained in IDs and passports as a template. The model is free from the weaknesses and limitations of other biometric and non-biometric identification methods analysed in this paper and has a very low error rate.

Keywords: biometrics, identification, authentication, authorization, identity.

ŁUKASZ SKONECZNY
ORCID: 0000-0003-1612-0915

BOGUSŁAW CACKO
ORCID: 0000-0002-6496-7005

DOI: 10.4467/20801335PBW.21.023.14300

Sharp power – wprowadzenie do problematyki

Od czasu powstania pierwszych greckich polis wspólnoty polityczne szukały skutecznych narzędzi oddziaływania zarówno na swoich wrogów, jak i sojuszników. Efektem tych wielowiekowych doświadczeń jest powstanie wielu wzorców potęgi państwa w relacjach z innymi podmiotami na arenie międzynarodowej. W niniejszym artykule skupiono się na przedstawieniu jej nowego rodzaju, jakim jest *sharp power*[1]. Podjęto próbę zdefiniowania tego zjawiska, przedstawienia jego charakterystycznych przejawów oraz zaproponowano metody minimalizowania jego negatywnych skutków dla bezpieczeństwa Rzeczpospolitej Polskiej.

Przeprowadzona przez autorów analiza problematyki dotyczącej potęgi państwa i różnych jej form pozwala postawić hipotezę, że obecnie jesteśmy świadkami kształtowania się kolejnego rodzaju oddziaływania reżimów politycznych na podmioty stosunków międzynarodowych, łączącego w sobie elementy przymusu i manipulacji. Nie można go zaszeregować w znanych dotychczas kategoriach *hard*, *soft* i *smart power*.

Istnieje wiele różnych definicji potęgi państwa[2]. Za klasyczną uznaje się definicję autorstwa Johna G. Stoessingera. Według amerykańskiego badacza to pojęcie oznacza (…) *zdolność państwa do użycia swoich materiałów* (…) *w sposób, który wpłynie na zachowanie innych państw*[3]. Taki sposób rozumienia, pomimo swojej ogólności,

[1] Wszystkie wyrazy i zwroty obcojęzyczne w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje za każdym razem tej informacji (przyp. red.).

[2] W artykule autorzy nie analizują dotychczasowego dorobku w zakresie teorii dotyczących potęgi państwa i jej różnych form. Prezentują jedynie teorie najbardziej reprezentatywne.

[3] J.G. Stoessinger, *The Might of Nation. World Politics in Our Times*, New York 1969, s. 26–27. Tłumaczenia w tekście pochodzą od autorów artykułu (przyp. red.).

wskazuje na konieczność dysponowania przez elity polityczne zapleczem gospodarczym, ideologicznym lub kulturowym, które będzie stanowiło fundament efektywnego oddziaływania na inne państwa. Jednocześnie autor wspomnianej definicji zakłada konieczność posiadania przez decydentów pogłębionej wiedzy na temat możliwości wpływania na aktywność innych podmiotów stosunków międzynarodowych. Warto zaznaczyć, że Stoessinger nie doprecyzował, jakie konkretnie elementy kryją się pod pojęciem „materiałów wpływających na inne państwo". Ten brak precyzji spowodował, że w literaturze przedmiotu upowszechniły się terminy „*soft power*" oraz „*hard power*". Ich twórcą jest Amerykanin Joseph S. Nye, autor licznych publikacji z zakresu bezpieczeństwa i polityki międzynarodowej. Koncepcja *soft power* miała być odpowiedzią państw Zachodu na zagrożenie militarne ze strony ZSRR. Amerykański uczony doszedł do wniosku, modyfikując wcześniejszą myśl Zbigniewa Brzezińskiego, który porównał politykę międzypaństwową do gry w szachy[4], że rywalizacja na arenie międzynarodowej jest obecnie prowadzona równolegle na trzech płaszczyznach. Są nimi: siła wojskowa, potęga ekonomiczna oraz *soft power*, czyli zdolność kształtowania preferencji innych podmiotów stosunków międzynarodowych[5]. Posługiwanie się miękką siłą jest utożsamiane głównie z państwami demokratycznymi. W uproszczeniu polega to na zachęcaniu – przy użyciu perswazji – uczestników relacji międzypaństwowych do akceptacji działań danego kraju. Według Nye'a głównymi źródłami *soft power* są trzy rodzaje zasobów każdego państwa: kulturowe, związane z jego wartościami politycznymi i z realizowaną przez nie polityką zagraniczną[6]. Czynnik kulturowy łączy się w tym przypadku z atrakcyjnością kultury danego kraju, przejawiającą się m.in. w wyznawanych i promowanych wartościach uniwersalnych. Nie oznacza to jednak, że można stawiać znak równości między miękką siłą a kulturą masową, będącą jedną z możliwych dróg transmisji idei. Z tego względu ten aspekt oddziaływania powinien być rozpatrywany szerzej i obejmować np. wymianę naukową czy współpracę biznesową[7]. W odniesieniu do dwóch pozostałych elementów *soft power* Nye pisał: (…) *polityka krajowa lub zagraniczna, jeśli jest pełna hipokryzji, arogancka, nie uwzględnia opinii innych albo opiera się na wąskim podejściu do narodowego interesu, może osłabić soft power.* (…) *Rząd swoim przykładem może przyciągać lub odstręczać*[8]. Należy jednak podkreślić, że ewentualne próby przejęcia przez reżim polityczny pełnej kontroli nad *soft power* będą napotykać – zwłaszcza w demokracji liberalnej – poważne przeszkody. Wynika to z tego, że duża część miękkiej siły jest rozproszona między różnego rodzaju

[4] Zob. Z. Brzeziński, *The Grand Chessboard: American Primacy And Its Geostrategic Imperatives*, New York 1997.

[5] J.S. Nye Jr., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007, s. 33–34.

[6] Tamże, s. 40.

[7] Tamże, s. 41.

[8] Tamże, s. 43–44.

podmiotami społecznymi (media, organizacje pozarządowe, przemysł rozrywkowy, środowiska artystyczne itd.), pozostającymi poza zasięgiem władz[9].

Przeciwieństwem strategii *soft power* jest *hard power*. Nye określił twardą siłę jako potencjał wynikający z czynników geopolitycznych oraz ekonomicznych[10]. Koncentruje się on na stosowaniu zachęt oraz gróźb użycia siły w relacjach międzypaństwowych. W tej strategii nie ma zatem mowy o pośrednim oddziaływaniu za pomocą kultury czy wartości, chodzi natomiast o wywieranie faktycznego wpływu na innych. Z tego powodu *hard power* pozostaje głównie domeną reżimów autorytarnych, których rozwiązania instytucjonalno-prawne oraz promowane wartości nie są atrakcyjne dla pozostałych państw. Należy również zaznaczyć, że *soft power* i *hard power* czasami wzmacniają się wzajemnie, a niekiedy ze sobą kolidują. Nie można jednak jednoznacznie wskazać, które z wymienionych podejść jest bardziej efektywne. Analizując te zagadnienia, Nye postawił tezę o możliwości łączenia skuteczności działań na arenie międzynarodowej z umiejętnością czerpania korzyści zarówno z jednej, jak i z drugiej strategii. Rezultatem tego podejścia było powstanie koncepcji *smart power*.

Smart power należy rozumieć jako efektywne zintegrowanie elementów miękkiej i twardej siły[11]. Ta strategia wymaga od decydentów umiejętności zręcznego posługiwania się dostępnymi instrumentami polityki zagranicznej, dostosowanymi zarówno do zaistniałej sytuacji międzynarodowej, jak i posiadanych możliwości działania. Dotyczy to zwłaszcza zdolności adaptacji do bieżących wydarzeń, koordynacji działań między poszczególnymi instytucjami państwowymi (w tym wyraźnego rozgraniczenia ich kompetencji), istnienia sprawnego obiegu informacji oraz odpowiednich procedur reagowania na potencjalne problemy[12].

Czym jest *sharp power*?

Zakończenie zimnej wojny, a przede wszystkim konflikt ukraiński rozpoczęty w 2014 r. ujawniły nowy trend w metodach i środkach stosowanych przez państwa w celu realizacji swoich interesów w środowisku międzynarodowym. Tych działań nie dało się zaklasyfikować do tradycyjnie rozumianych strategii *hard power* i *soft power*. Jako pierwsi zwrócili na to uwagę w 2017 r. amerykańscy badacze Christopher Walker i Jessica Ludwig w artykule *The Meaning of Sharp Power. How Authoritarian States Project Influence*[13]. W swojej

[9] Tamże, s. 44.

[10] Tamże, s. 34.

[11] *CSIS Commision on Smart Power: A Smarter, More Secure America*, R.L. Armitage, J.S. Nye Jr. (red.), Washington 2007, s. 7.

[12] J. Sadłocha, *Pomiędzy miękką a twardą siłą: smart power*, „Wrocławskie Studia Politologiczne" 2012, t. 13, s. 38–40.

[13] Ch. Walker, J. Ludwig, *The Meaning of Sharp Power. How Authoritarian States Project Influence*, „Foreign Affairs", 16 XI 2017 r., foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power [dostęp: 14 VI 2021].

publikacji wskazali oni na rosnącą aktywność państw autorytarnych na arenie międzynarodowej, która odbiega od działań dotychczas określanych przez kraje zachodnie jako elementy miękkiej siły. Jej celem nie jest zwiększenie atrakcyjności własnego wizerunku, tylko manipulowanie nastrojami społecznymi – zwłaszcza w obrębie postrzegania wartości charakterystycznych dla demokratycznego państwa prawa. W odniesieniu do tych działań amerykańscy badacze użyli terminu *sharp power*, mającego oznaczać penetrowanie przestrzeni informacyjnej i środowiska politycznego wybranego kraju w celu zdyskredytowania go w oczach krajowej i zagranicznej opinii publicznej (w oryginale: *Authoritarian influence efforts are „sharp" in the sense that they pierce, penetrate, or perforate the political and information environments in the targeted countries*)[14]. W ocenie autorów omawianego artykułu przykładami reżimów autorytarnych stosujących *sharp power* są Federacja Rosyjska i Chińska Republika Ludowa. Celem ich aktywności nie jest „zdobycie umysłów i serc", lecz wywoływanie lub podsycanie animozji wśród obywateli państw zachodnich. Jednocześnie Walker i Ludwig zwracają uwagę na brak adekwatnych mechanizmów obronnych Zachodu na działania podejmowane przez reżimy autorytarne. W tym kontekście postulują przede wszystkim demaskowanie wrogich działań informacyjnych oraz zwiększanie świadomości społecznej na ten temat[15]. Ważnym głosem w dyskusji o *sharp power* jest inny artykuł Nye'a, a mianowicie *How Sharp Power Threatens Soft Power. The Right and Wrong Ways to Respond to Authoritarian Influence*[16]. Jest on odpowiedzią na publikację Walkera i Ludwig. W ocenie amerykańskiego uczonego *sharp power* nie jest zjawiskiem wcześniej nieznanym. Jego zdaniem jest to nowy termin mający określać walkę informacyjną. Nye zaznacza także, że *sharp power* nie jest działaniem charakterystycznym wyłącznie dla reżimów autorytarnych. Tą strategią posługują się również kraje demokratyczne, a jako przykład wskazał aktywność USA wobec ZSRR w trakcie zimnej wojny. Amerykański politolog ostrzega również Zachód przed podejmowaniem prób wykorzystania *sharp power* przeciwko reżimom autorytarnym. Naraża to bowiem demokracje zachodnie na utratę wiarygodności i obniżenie ich własnego potencjału miękkiej siły. Dlatego też – według Nye'a – w przeciwdziałaniu *sharp power* najważniejsze jest zachowanie przez demokracje liberalne względnej otwartości w kontaktach z państwami autorytarnymi. W tym kontekście ważną rolę do odegrania mają przede wszystkim instytucje społeczeństwa obywatelskiego (m.in. mass media, środowiska naukowe, organizacje pozarządowe), które powinny upowszechniać wiedzę dotyczącą technik walki informacyjnej.

W debacie poświęconej *sharp power* pojawiają się również opinie krytyczne. Autorem jednej z nich jest Xin Liu, która w artykule *What sharp power? It's nothing but*

[14] Tamże.

[15] Tamże.

[16] J.S. Nye Jr., *How Sharp Power Threatens Soft Power. The Right and Wrong Ways to Respond to Authoritarian Influence*, „Foreign Affairs", 24 I 2018 r., foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power [dostęp: 14 VI 2021].

„unsmart" power[17] nie zgadza się ze stanowiskiem Walkera oraz Nye'a co do tego, że jest to jakościowo zupełnie nowe zjawisko. Jej zdaniem *sharp power* jest efektem nieumiejętnie realizowanego *smart power*, czyli niewłaściwego połączenia elementów miękkiej i twardej siły.

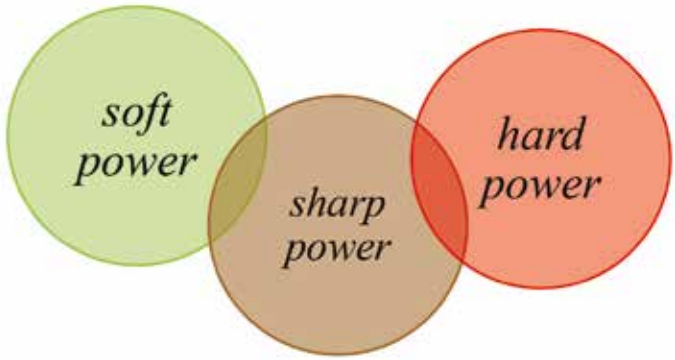
Podsumowując dotychczasowe rozważania na temat *sharp power*, należy stwierdzić, że pogląd, według którego jest to wyłącznie nowy termin określający znane już wcześniej zagrożenie, jakim jest wojna informacyjna, może budzić poważne wątpliwości. Prawdą jest, że manipulacja informacją stanowi główny komponent *sharp power*, nie jest to natomiast jedyne narzędzie wykorzystywane w ramach tej strategii. W dalszej części artykułu zostaną omówione inne metody zawierające się w tej koncepcji, które nie sprowadzają się wyłącznie do działań w przestrzeni informacyjnej.

Należy zgodzić się ze stanowiskiem Nye'a, że *sharp power* nie jest wyłączną domeną reżimów autorytarnych. Jak słusznie wskazał amerykański uczony, tę strategię stosują również władze państw demokratycznych. Warto natomiast rozważyć, dlaczego kraje o tendencjach autorytarnych zdecydowanie częściej decydują się na tego rodzaju działania. W ocenie autorów niniejszego artykułu największe znaczenie ma charakter liberalnego systemu społeczno-politycznego. Jego otwartość jest wykorzystywana przez reżimy autorytarne do prowadzenia działań o charakterze *sharp power.* Przez otwartość należy rozumieć takie cechy demokracji liberalnej, jak: wolność słowa, wolny rynek medialny, pluralizm polityczny, oznaczający możliwość zakładania partii politycznych niepodlegających wpływom władz, istnienie niezależnego sektora organizacji pozarządowych itd. Z powodu braku tych elementów albo ich ścisłego nadzoru w reżimach autorytarnych rządy państw demokratycznych mają znacznie ograniczone możliwości podejmowania wobec nich analogicznych działań *sharp power*. Dodatkowym czynnikiem powstrzymującym demokracje liberalne przed stosowaniem tej strategii jest obawa przed wybuchem poważnego kryzysu politycznego. Ujawnienie, np. przez mass media, prowadzenia tego rodzaju działań przez rząd demokratycznego państwa mogłoby wywołać silną krytykę władz ze strony opinii publicznej, a w skrajnym przypadku spowodować nawet konieczność przeprowadzenia wcześniejszych wyborów.

Podsumowując, s*harp power* można zdefiniować jako **agresywne działania państwa prowadzone przy wykorzystaniu metod imitujących elementy *soft power* w celu manipulacji wizerunkiem danego kraju (lub innego podmiotu stosunków międzynarodowych) bądź destabilizacji jego systemu społeczno-politycznego, bądź wymuszenia określonego postępowania jego władz**[18].

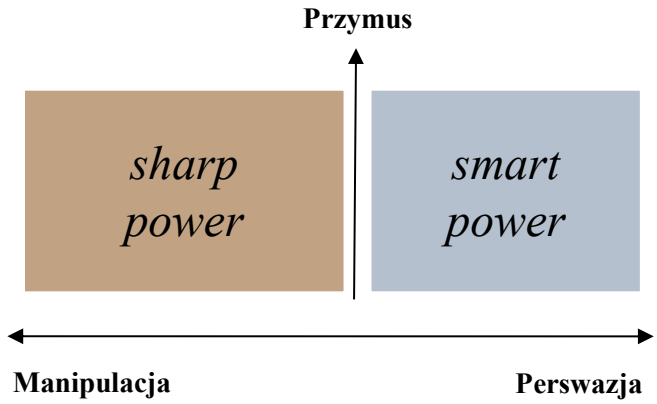
[17] Xin Liu, *What Sharp power? It's nothing but „unsmart" power*, USC Center on Public Diplomacy, 15 XI 2018 r., uscpublicdiplomacy.org/blog/what-sharp-power-it's-nothing-"unsmart"-power [dostęp: 10 V 2021].

[18] Wyróżnienia w tekście pochodzą od autorów (przyp. red.).



Rys. 1. Usytuowanie *sharp power* względem *soft power* i *hard power*.

Źródło: Opracowanie własne.



Rys. 2. Usytuowanie *sharp power* względem *smart power*.

Źródło: Opracowanie własne.

Metody realizacji *sharp power*

W ramach realizacji strategii *sharp power* państwa wykorzystują różne instrumenty ekonomiczne, polityczne, militarne i dyplomatyczne charakterystyczne dla *soft power* i *hard power*. Zaprezentowane poniżej zestawienie nie stanowi ich zamkniętego katalogu. Są to natomiast metody aktualnie najczęściej wybierane przez kraje decydujące się na podjęcie tego typu działań.

Wojna informacyjna

Podstawowym narzędziem wykorzystywanym w ramach *sharp power* jest wojna informacyjna. Jej szczególne znaczenie jest związane z globalną rewolucją teleinformatyczną oraz rozwojem społeczeństw sieciowych. Efektem tych procesów jest gwałtowny wzrost roli Internetu w zdobywaniu informacji i w komunikacji międzyludzkiej. Wojna informacyjna umożliwia dotarcie z określonym przekazem do dużej liczby odbiorców (np. za pomocą mediów społecznościowych, internetowych telewizji i forów dyskusyjnych). Zapewnia przy tym agresorowi anonimowość (ze względu na wielość podmiotów działających w przestrzeni informacyjnej trudno jest wskazać prawdziwego autora danej narracji), a także pozwala na ukrycie, pod pozorem dostarczenia wiarygodnych danych lub innego punktu widzenia na określony temat, rzeczywistych intencji nadawcy. Ważną cechą wojny informacyjnej jest również relatywnie niski koszt jej prowadzenia (związane jest to m.in. z tym, że obecnie głównym obszarem walki informacyjnej jest sieć internetowa). Stanowi ona ponadto główny element wsparcia dla pozostałych działań stosowanych w ramach *sharp power*, znacznie zwiększając ich efektywność.

Na potrzeby niniejszego artykułu wojna informacyjna jest definiowana, za Robertem Rajczykiem[19], jako długotrwały, wieloaspektowy proces komunikowania, którego celem jest uzyskanie przewagi informacyjnej nad przeciwnikiem, m.in. przez oddziaływanie na krajową i zagraniczną opinię społeczną, obniżanie morale oraz kreowanie postaw konformistycznych wśród wrogiego społeczeństwa, a także wykorzystanie dyplomacji publicznej.

Pojęcie „wojna informacyjna" należy rozumieć szeroko. Nie oznacza ono prowadzenia propagandy i dezinformacji wyłącznie w trakcie trwania konfliktu zbrojnego[20], lecz może obejmować również agresywne przedsięwzięcia informacyjne realizowane w czasie pokoju. Działania podejmowane w ramach wojny informacyjnej mogą polegać na:

- upublicznianiu (np. przez portale internetowe typu WikiLeaks) informacji wrażliwych, przechwyconych z prywatnego sprzętu komputerowego oraz telefonów komórkowych należących do polityków, urzędników państwowych, wojskowych lub funkcjonariuszy służb mundurowych;
- aktywności fikcyjnych grup użytkowników (tzw. trolli) prowadzących działalność dezinformacyjną w Internecie, np. na portalach społecznościowych;
- wykorzystaniu agentury wpływu do manipulowania poglądami decydentów politycznych, grup nacisku i środowisk opiniotwórczych;
- tworzeniu przychylnych państwu-manipulatorowi mediów w danym kraju (radio, telewizja, gazety, portale internetowe);

[19] Zob. R. Rajczyk, *Nowoczesne wojny informacyjne*, Warszawa 2016, s. 29.

[20] Szerzej na temat różnic w definiowaniu wojny informacyjnej przez NATO i przez stronę rosyjską zob. K. Giles, *Handbook of Russia information warfare*, Rome 2016, s. 3–13.

– kształtowaniu negatywnego wizerunku danego kraju przez mass media państwa-manipulatora (w tym także w środkach masowego przekazu państw sąsiadujących z celem wrogich działań informacyjnych);
– blokadzie państwowych witryn internetowych lub podmianie publikowanych na nich treści;
– dezawuowaniu ideologii, wartości społecznych czy rozwiązań ustrojowych funkcjonujących w danym państwie;
– niszczeniu sieci światłowodowych lub telekomunikacyjnych w celu uniemożliwienia przekazywania informacji.

Od czasu kryzysu ukraińskiego, który rozpoczął się w 2014 r., systematycznie nasila się wojna informacyjna prowadzona przez Federację Rosyjską (FR) w stosunku do państw Europy Środkowo-Wschodniej, w tym Polski. Głównymi celami Rosji jest m.in. kreowanie negatywnego obrazu regionu oraz podsycanie napięć w jego relacjach z partnerami z Unii Europejskie i Sojuszu Północnoatlantyckiego. Polska, jako bliski sojusznik USA oraz istotny członek UE i NATO, jest postrzegana przez Kreml jako jeden z głównych organizatorów inicjatyw międzynarodowych wymierzonych w interesy FR. Moskwa może angażować przychylnych sobie polskich dziennikarzy, naukowców, polityków oraz działaczy społecznych w działania informacyjne skierowane przeciw RP. Ponadto korzysta ze wsparcia podmiotów odpowiedzialnych za promowanie interesów Rosji poza granicami kraju, a także skupiających mniejszość rosyjską.

Udzielanie wsparcia podmiotom politycznym i organizacjom społecznym wpisującym się w strategię *sharp power* państwa-manipulatora

Kolejnym ważnym narzędziem *sharp power* jest wspieranie aktywności organizacji politycznych oraz środowisk społecznych prowadzących działalność lobbingową na rzecz państwa-manipulatora lub mogących destabilizować sytuację w danym kraju. Wśród najczęściej wykorzystywanych metod należy wskazać:

– **wielokierunkową presję** – polegającą na wywieraniu nacisków politycznych, ekonomicznych, militarnych czy dyplomatycznych na władze danego kraju w celu wymuszenia na nich ustępstw wobec podmiotów działających w interesie państwa-manipulatora (może tu chodzić m.in. o wprowadzanie rozwiązań prawnych korzystnych dla aktywności takich organizacji, np. wpis do rejestru partii politycznych);
– **pomoc ekonomiczną** – obejmującą zarówno legalne, prawnie przewidziane możliwości wspierania tego typu podmiotów (np. darowizny, granty badawcze, wynajem nieruchomości), jak i nielegalne sposoby stosowane przez państwo-manipulatora. Najczęściej – tak jak w przypadku przestępstwa prania pieniędzy – polegają one na wykorzystaniu tzw. słupów, czyli osób fizycznych bądź prawnych, które mają ukryć rzeczywiste pochodzenie środków finansowych. W celu uniemożliwienia wytropienia źródeł finansowania niejednokrotnie są tworzone również konta w bankach działających na terytorium państwa-

-manipulatora, na które są przelewane pieniądze dla danego podmiotu, wypłacane następnie przez jego przedstawicieli;
– **aktywność propagandową i dezinformacyjną** – czyli wszelkie działania informacyjne prowadzone przez państwo-manipulatora w celu kreowania pozytywnych opinii na temat wspieranego podmiotu lub dyskredytowania wizerunku władz kraju, w którym on funkcjonuje (np. kampanie informacyjne w Internecie, czarny PR, utrzymywanie oficjalnych kontaktów przez przedstawicieli dyplomatycznych państwa-manipulatora z danym podmiotem).

Jako przykład omawianego przejawu *sharp power* mogą posłużyć informacje wskazujące na możliwość wspierania katalońskich separatystów przez Rosję i Chiny. Zgodnie z medialnymi doniesieniami hiszpańska policja miała prowadzić śledztwo dotyczące udziału rosyjskiego wywiadu w inspirowaniu katalońskich nacjonalistów do protestów i oporu przeciwko rządowi centralnemu w Madrycie. Oficer rosyjskiego GRU miał kontaktować się w 2017 r. z Victorem Terradellasem, który jako doradca ówczesnego premiera Katalonii Carlesa Puigdemonta wywierał na niego presję w sprawie ogłoszenia niepodległości przez ten region. Na podstawie cyfrowej korespondencji hiszpańskie organy ścigania miały ustalić, że Terradellas zapewniał katalońskiego polityka o poparciu Władimira Putina i możliwości udzielania pomocy finansowej obiecywanej rzekomo przez Chiny[21]. Celem rosyjskich działań mogła być próba destabilizacji sytuacji wewnątrz UE, co pośrednio przełożyłoby się na osłabienie jej pozycji w relacjach z FR.

Polityka historyczna

Narzędziem coraz częściej wykorzystywanym w ramach *sharp power* jest polityka historyczna. Przy czym nie chodzi tu o samo promowanie pewnej wizji historii przez władze danego kraju, gdyż kwestie historyczne od zawsze były wykorzystywane do rozgrywek politycznych na arenie międzynarodowej. W przypadku *sharp power* polityka historyczna polega nie na popularyzowaniu określonej interpretacji historii, ale na jej celowym zakłamywaniu i negowaniu faktów powszechnie przyjętych w historiografii.

Przykładem tego typu działań jest obecna polityka historyczna FR dotycząca wybuchu oraz przebiegu II wojny światowej. Jednym z jej elementów jest tzw. wojna pomnikowa prowadzona przeciwko Polsce. Pretekstem do jej rozpoczęcia przez Moskwę było uchwalenie przez polski parlament 1 kwietnia 2016 r. tzw. ustawy dekomunizacyjnej, a zwłaszcza jej nowelizacji z czerwca 2017 r. W następstwie tych działań Rosja oskarża Polskę o niszczenie cmentarzy żołnierzy radzieckich, którzy walczyli z hitlerowskimi Niemcami w trakcie II wojny światowej. Celem Kremla jest szkalowanie wizerunku RP w oczach opinii międzynarodowej, skutkujące utratą wiarygodności władz w Warszawie oraz osłabieniem jedności NATO i UE. Chodzi także o zwiększenie wrogości do Polski w społeczeństwie rosyjskim. Przyczyną niechęci ma być rzekomy brak wdzięczności

[21] M. Kucharczyk, *Czy Rosja wspierała katalońskich niepodległościowców?*, Euractiv, 28 XI 2019 r., euractiv.pl/section/demokracja/news/czy-rosja-wspierala-katalonskich-niepodleglosciowcow [dostęp: 15 V 2021].

narodu polskiego za ofiary poniesione przez Rosjan podczas wyzwalania naszego kraju spod okupacji niemieckiej.

Kolejnym priorytetem rosyjskiej polityki historycznej jest próba przerzucenia na Polskę odpowiedzialności za wybuch II wojny światowej. W tym kontekście strona rosyjska wskazuje na rzekomo awanturniczą politykę II RP i brak jej zgody na współpracę z ZSRR, a jednocześnie umniejsza rolę paktu Ribbentrop-Mołotow w podziale strefy wpływów w Europie Środkowo-Wschodniej między III Rzeszę a Związek Sowiecki. Ponadto Kreml obarcza stronę polską odpowiedzialnością za Holocaust. Argumentem, którym posługuje się strona rosyjska, jest m.in. wybudowanie przez III Rzeszę niemieckich obozów zagłady na okupowanym terytorium II RP. Wszystkie te działania służą wybielaniu historii ZSRR i jednocześnie kreowaniu negatywnego wizerunku Polski jako państwa nazistowskiego i antysemickiego[22].

Manipulowanie przebiegiem i wynikami procesów wyborczych w danym kraju

Ważnym narzędziem strategii *sharp power* jest przekonanie obywateli danego kraju, że reżim polityczny sprawujący władzę jest pozbawiony odpowiedniej legitymizacji społecznej. Najskuteczniejszą metodą realizacji tego celu jest podważenie wiarygodności samego procesu wyborczego i wywołanie przeświadczenia, że jego wynik został sfabrykowany. Takie działania mogą polegać m.in. na masowym rozpowszechnianiu fake newsów dotyczących ingerencji obcego kraju w proces wyborczy czy nieprawidłowości przy przeliczaniu głosów. Państwo-manipulator może także np. inspirować protesty społeczne negujące rezultat wyborów prezydenckich czy parlamentarnych.

Możliwe jest również bezpośrednie wpływanie na wynik wyborów np. za pomocą działań wymierzonych w określonych kandydatów bądź partie polityczne. Mogą one polegać m.in. na:

- cyberatakach ukierunkowanych na infrastrukturę wyborczą w celu fałszowania liczby oddanych głosów;
- korzystaniu z tzw. *proxies* (np. organizacji pozarządowych) rozpowszechniających krytyczną narrację na temat określonych kandydatów bądź partii politycznych;
- dystrybuowaniu fake newsów w sieci internetowej (media społecznościowe, fora dyskusyjne, portale informacyjne);
- atakach medialnych prowadzonych przez środki masowego przekazu państwa-manipulatora.

Przykładem ingerencji w proces wyborczy, stanowiącej element strategii *sharp power*, może być kampania prezydencka w USA w 2016 r. Istnieją przesłanki wskazujące na to, że Rosja dążyła wtedy do wykreowania negatywnego przekazu medialnego na temat amerykańskiego systemu politycznego, podważenia wiarygodności Hillary

[22] Szerzej na temat rosyjskiej polityki historycznej zob. J. Darczewska, *„Wojny pamięci": historia, polityka i służby specjalne Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 11, s. 13–41.

Clinton – kandydatki Partii Demokratycznej na urząd prezydenta, a także do wsparcia Donalda Trumpa w osiągnięciu zwycięstwa[23].

Współpraca naukowa

Jednym z narzędzi stosowanych przez państwa w ramach realizowanej strategii *sharp power* jest również kooperacja naukowa. Najczęściej będzie ona wykorzystywana do prowadzenia operacji wpływu w środowisku akademickim danego kraju. Celem strategicznym jest stworzenie eksperckiego lobby promującego interesy państwa-manipulatora, np. wśród przedstawicieli elit politycznych, bądź krytykującego publicznie działania podejmowane przez władze państwowe. Realizacja tego planu może polegać na organizacji wyjazdów studyjnych do państwa-manipulatora czy przyznawaniu stypendiów dla młodzieży i pracowników uczelni wyższych. W ten sposób mogą być typowane osoby, które w przyszłości staną się agentami wpływu. Ze względu na osiągniętą pozycję społeczną lub zajmowane stanowisko mogą one być wykorzystywane m.in. do manipulowania poglądami środowisk opiniotwórczych.

Kolejnym elementem omawianych działań może być propozycja udziału przedstawicieli środowisk akademickich w imprezach kulturalno-naukowych o wydźwięku propagandowym. Są one organizowane – w tym przez państwo-manipulatora – zarówno na terytorium kraju będącego celem obcego *sharp power*, jak i za granicą. Wśród zapraszanych gości mogą znajdować się m.in. politycy, uczeni oraz działacze społeczni wygłaszający prowokacyjne wystąpienia. Tego typu imprezy są następnie wykorzystywane jako element walki informacyjnej. Należy zaznaczyć, że niejednokrotnie reprezentanci społeczności naukowej zapraszani na takie wydarzenia nie mają świadomości, jaki jest ich rzeczywisty cel.

Państwo-manipulator może również zaproponować uczonym z danego kraju uczestnictwo w realizacji kontrowersyjnych projektów naukowych, dotyczących np. historii, sytuacji politycznej na świecie, członkostwa w organizacjach międzynarodowych. Za udział w tych przedsięwzięciach może być oferowane m.in. atrakcyjne wynagrodzenie lub pomoc w prowadzeniu badań (w tym dostęp do archiwów dokumentów znajdujących się na terytorium państwa-manipulatora). Celem tego typu inicjatyw jest m.in. kwestionowanie polityki zagranicznej oraz wewnętrznej wybranego kraju albo doprowadzenie do wzrostu napięcia w jego relacjach z państwami ościennymi.

Jednym z narzędzi strategii *sharp power* może być także system grantów naukowych. Podmioty (np. państwowe fundacje i przedsiębiorstwa, prywatni darczyńcy) powiązane z państwem-manipulatorem mogą uzyskać, w zamian za finansowe wsparcie, możliwość lokowania swoich przedstawicieli m.in. w radach nadzorczych oraz zarządach uczelni wyższych czy instytutów badawczych w danym kraju. Zyskują dzięki temu sposobność decydowania np. o realizowanych przez nie projektach badawczych.

[23] Zob. szerzej: R.S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, t. 1–2, Washington 2019.

Dotowane w ten sposób placówki naukowe w obawie przed utratą finansowania same mogą unikać podejmowania inicjatyw niezgodnych z interesami państwa-manipulatora bądź angażowania się w niekorzystne dla niego przedsięwzięcia[24].

Przedsięwzięcia ekonomiczno-gospodarcze o charakterze międzynarodowym

Do elementów *sharp power* można ponadto zaliczyć międzynarodowe inicjatywy, które – pod pozorem zapewnienia korzyści gospodarczych uczestniczącym w nich krajom – służą destabilizacji sytuacji politycznej w danym regionie i jego ekonomicznemu uzależnieniu od państwa-manipulatora. Jako przykład tego rodzaju działań należy wskazać rosyjski Nord Stream 2 oraz chiński Nowy Jedwabny Szlak.

Inwestycja gazowa realizowana przez Kreml ma na celu, poza ominięciem terytorium państw tranzytowych (m.in. Polski, Ukrainy, państw bałtyckich), doprowadzenie do podważenia polityki energetycznej UE w zakresie solidarności i współpracy pomiędzy państwami unijnymi, a także spowodowanie wzrostu napięcia w relacjach pomiędzy Republiką Federalną Niemiec a krajami Europy Środkowo-Wschodniej. Należy przy tym zaznaczyć, że w ocenie wielu ekonomistów budowa kolejnego połączenia gazowego do Niemiec jest nieopłacalna dla Gazpromu i jego akcjonariuszy[25].

Podobny charakter ma promowany przez Pekin projekt Nowego Jedwabnego Szlaku, czyli sieci infrastruktury transportowej umożliwiającej relatywnie szybką wymianę handlową między Chinami a Europą. Celem tej inicjatywy jest doprowadzenie do wzmocnienia pozycji geopolitycznej Chin na świecie, a także stworzenie prochińskiego lobby wśród członków UE, które będzie miało za zadanie wpływać na politykę Brukseli zgodnie z oczekiwaniami Pekinu w zamian za ewentualne benefity płynące z tego przedsięwzięcia. Chiny już w 2012 r. podjęły pierwszą próbę utworzenia w regionie Europy Środkowej kręgu sprzyjających im państw pod postacią „Inicjatywy 16+1" (obecnie „17+1", gdyż w 2019 r. dołączyła Grecja). Próba okazała się jednak nieskuteczna ze względu m.in. na brak poważnych propozycji gospodarczych ze strony Pekinu dla jej uczestników[26].

---

[24] Szerzej o przykładach wykorzystania kooperacji naukowej jako narzędzia *sharp power* zob. A. Foxall, *Russian Sharp Power In European Academia*, w: *The Art Of Deceit: How China And Russia Use Sharp Power To Subvert The West*, A. Foxall, J. Hemmings (red.), London 2019, s. 31–35.

[25] Zob. A. Becker, *Nord Stream 2 w oczach niemieckich ekspertów: „Zbędny, szkodliwy, nierentowny"*, Deutsche Welle, 10 IX 2020 r., dw.com/pl/nord-stream-2-w-oczach-niemieckich-ekspertów-zbędny-szkodliwy-nierentowny/a-54870406 [dostęp: 23 VI 2021]; J. Rutkowski, *Nord Stream 2 – wszystko przemawia przeciw temu projektowi*, Forsal, 27 II 2021 r., forsal.pl/gospodarka/artykuly/8106480,-nord-stream-2-wszystko-przemawia-przeciw-temu-projektowi.html [dostęp: 23 VI 2021].

[26] Zob. M. Przychodniak, *Chiny wobec kryzysu inicjatywy 17+1*, Polski Instytut Spraw Międzynarodowych, pism.pl/publikacje/Chiny_wobec_kryzysu_inicjatywy_171_ [dostęp: 8 VI 2021].

Konflikt hybrydowy

Ostatnią, i zarazem najbardziej agresywną, metodą, na której użycie może zdecydować się państwo w ramach działań *sharp power*, jest konflikt hybrydowy. Pojęcie to oznacza sytuację kryzysową, w której jedna ze stron (państwo lub podmioty niepaństwowe) powstrzymuje się od bezpośredniego użycia sił zbrojnych na rzecz innych sposobów oddziaływania na przeciwnika, tj. o charakterze ekonomicznym, politycznym, dyplomatycznym i militarnym. Ponadto cechą charakterystyczną konfliktu hybrydowego jest brak możliwości precyzyjnego wskazania agresora, a tym samym stwierdzenia formalnego stanu wojny (tzw. agresja poniżej progu wojny)[27].

Możliwość efektywnego prowadzenia konfliktu hybrydowego jest najwyższą formą emanacji *sharp power*, oznaczającą osiągnięcie przez dany kraj maksymalnego potencjału w tym obszarze. Konflikt hybrydowy jest bowiem wynikiem efektu synergii, uzyskanym przez umiejętne zastosowanie poszczególnych metod realizacji *sharp power*, odpowiedniej koordynacji działań instytucji państwowych, a także zdolności adaptacji do dynamicznie zmieniającego się otoczenia międzynarodowego. Przykładem tego typu zagrożenia jest polityka Rosji wobec Ukrainy prowadzona od 2014 r. Ma ona na celu – m.in. przez destabilizację i dezintegrację terytorialną – utrzymanie tego kraju w strefie rosyjskich wpływów oraz uniemożliwienie jego integracji z NATO i UE.

Jak przeciwdziałać *sharp power*?

Ważną kwestią związaną z problematyką *sharp power* jest wypracowanie przez władze państwowe odpowiedniej strategii, która skutecznie zapobiegałaby negatywnym efektom takich działań. Jest to istotne zwłaszcza w przypadku demokracji liberalnych, w tym Polski, które – jak wcześniej wspomniano – są szczególnie podatne na ten rodzaj aktywności ze strony państw autorytarnych.

Priorytetowym celem przyjętej strategii ochronnej powinno być zwiększanie świadomości społecznej na temat zagrożeń związanych z manipulacją informacjami w sieci internetowej. Pozytywnie należy ocenić wysiłki osób prywatnych bądź organizacji pożytku publicznego podejmowane w celu upowszechniania wiedzy na temat dezinformacji oraz demaskowania nieprawdziwych informacji (w kontekście Polski warto wspomnieć o inicjatywie „Rosyjska V kolumna w Polsce”[28] czy aktywności Centrum Analiz Propagandy i Dezinformacji). Są to jednak działania niewystarczające, a skala problemu wymaga zaangażowania ze strony państwa. Na gruncie polskim oznacza to potrzebę powołania podmiotu odpowiedzialnego za programowanie, nadzorowanie, analizowanie, a także koordynowanie aktywności instytucji państwowych w zakresie przeciwdziałania

[27] Zob. Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, wydanie specjalne, s. 39–50.

[28] „Rosyjska V kolumna w Polsce” to facebookowy profil administrowany przez blogera Marcina Reya, na którym jest przedstawiana działalność środowisk prorosyjskich w Polsce (przyp. red.).

wrogim działaniom informacyjnym wymierzonym w wizerunek i pozycję międzynarodową RP. Obecnie te zadania są rozproszone między różnymi organami państwowymi, co negatywnie przekłada się na efektywność ich realizacji. Stwarza to również możliwość powstawania sporów kompetencyjnych, a także dublowania podejmowanych działań.

Należałoby także rozważyć możliwość wprowadzenia rozwiązań legislacyjnych wzorowanych na amerykańskiej ustawie z 1938 r. o rejestrze zagranicznych agentów (Foreign Agents Registration Act, dalej: FARA). Reguluje ona aktywność podmiotów działających na rzecz zagranicznego mocodawcy, która może polegać m.in. na:

- uczestnictwie w różnorodnych inicjatywach o charakterze politycznym;
- pełnieniu funkcji doradcy politycznego, konsultanta PR, pracownika służb informacyjnych;
- udzielaniu pożyczek finansowych lub udostępnianiu innego rodzaju środków materialnych;
- reprezentowaniu zagranicznego mocodawcy przed instytucjami rządowymi USA.

Podstawowym celem FARA jest identyfikacja obcych wpływów w Stanach Zjednoczonych i wynikających z tego zagrożeń bezpieczeństwa narodowego tego kraju. Ustawa ma również zapewnić amerykańskim władzom możliwość ustalenia, czy dana informacja nie stanowi próby oddziaływania na amerykańską opinię publiczną przez inne państwa. Warto wspomnieć, że na podstawie zapisów tego aktu prawnego w listopadzie 2017 r. do rejestru agentów zagranicznych zostały wpisane rosyjska telewizja RT oraz agencja informacyjna Sputnik. Podmioty te zostały zobowiązane m.in. do informowania odbiorców o tym, że funkcjonują jako agenci zagraniczni oraz do przekazywania do Departamentu Sprawiedliwości USA danych dotyczących źródeł ich finansowania.

Ważną kwestią pozostaje także podjęcie przez państwa demokratyczne aktywnych działań wobec reżimów autorytarnych stosujących *sharp power*. Z jednej strony demokracje liberalne muszą zintensyfikować swoje oddziaływanie na społeczeństwa tych krajów za pomocą miękkiej siły (np. przez organizowanie masowych programów wymiany naukowej i kulturowej, ułatwienia w podróżowaniu bądź promowanie wartości demokratycznych). Z drugiej strony powinny one ograniczyć możliwości szerzenia fake newsów i podkopywania zaufania do demokratycznego państwa prawa. W tym kontekście być może warto rozważyć rozwiązanie zastosowane przez władze Łotwy, które w lutym 2021 r. podjęły decyzję o rocznym zakazie transmitowania telewizji Rosja RTR ze względu na podżeganie do nienawiści. Uczestnicy programu publicystycznego wyświetlanego na antenie tej stacji określali Ukrainę jako państwo terrorystyczne i nawoływali do wprowadzenia wojsk rosyjskich na jej terytorium[29].

Reasumując, problem skutecznego przeciwdziałania *sharp power* będzie nabierał coraz większego znaczenia, zwłaszcza w dobie globalizującego się świata. Oznacza to, jak wskazano powyżej, konieczność podjęcia przez władze państwowe przede wszystkim

[29] Zob. *Łotwa zakazała na rok emisji rosyjskiej telewizji państwowej „Rosja RTR"*, Studium Europy Wschodniej UW, 9 II 2021 r., studium.uw.edu.pl/lotwa-zakazala-na-rok-emisji-rosyjskiej-telewizji-panstwowej-rosja-rtr/ [dostęp: 11 VI 2021].

odpowiednich działań edukacyjnych oraz legislacyjnych. Jednocześnie rządy krajów demokratycznych nie mogą biernie przyglądać się próbom destabilizacji ich systemów społeczno-politycznych, lecz muszą podejmować inicjatywy, których celem będzie przeciwdziałanie tego typu agresji.

Bibliografia

Brzeziński Z., *The Grand Chessboard: American Primacy And Its Geostrategic Imperatives*, New York 1997, Basic Books.

CSIS Commision on Smart Power: A Smarter, More Secure America, R.L. Armitage, J.S. Nye Jr. (red.), Washington 2007, Center for Strategic & International Studies.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, Ośrodek Studiów Wschodnich.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, Ośrodek Studiów Wschodnich.

Darczewska J., *„Wojny pamięci": historia, polityka i służby specjalne Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20, s. 13–41.

Gallarotti G., *Soft Power: What it is, Why it's Important, and the Conditions Under Which it Can Be Effectively Used*, „Journal of Political Power" 2011, nr 1, s. 25–47.

Giles K., *Handbook of Russia information warfare*, Rome 2016, NATO Defense College.

Krzak A., *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 11–39.

Kuźniar R., *Polityka i siła. Studia strategiczne – zarys problematyki*, Warszawa 2005, Scholar.

Materski W., *Polityka historyczna Federacji Rosyjskiej po 2000 r.*, „Dzieje Najnowsze" 2014, nr 4, s. 93–115.

Mueller R.S., III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, t. 1–2, Washington 2019, U.S. Department of Justice.

Nye J.S. Jr., *Bound to Lead. The Changing Nature of American Power*, New York 1991, Basic Books.

Nye J.S. Jr., *Przyszłość siły*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Nye J.S. Jr., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007, Wydawnictwa Akademickie i Profesjonalne.

Rajczyk R., *Nowoczesne wojny informacyjne*, Warszawa 2016, Difin.

Sadłocha J., *Pomiędzy miękką a twardą siłą: smart power*, „Wrocławskie Studia Politologiczne" 2012, t. 13, s. 37–46.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne, s. 39–50.

Stoessinger J.G., *The Might of Nation. World Politics in Our Times*, New York 1969, Random House.

The Art Of Deceit: How China And Russia Use Sharp Power To Subvert The West, A. Foxall, J. Hemmings (red.), London 2019, The Henry Jackson Society.

Tomaszewska P., Pohl A., *Dylematy związane z uczestnictwem Polski w chińskiej inicjatywie Belt and Road*, „Przegląd Strategiczny" 2019, nr 12.

Tromblay D.E., *Political Influence Operations: How Foreign Actors Seek to Shape US Policy Making*, Lanham–Boulder–London–New York 2018, Rowman and Littlefield.

Walker Ch., *What Is "Sharp Power"?*, „Journal of Democracy" 2018, nr 3, s. 9–23.

Źródła internetowe

Becker A., *Nord Stream 2 w oczach niemieckich ekspertów: „Zbędny, szkodliwy, nierentowny"*, Deutsche Welle, 10 IX 2020 r., dw.com/pl/nord-stream-2-w-oczach-niemieckich-ekspertów-zbędny-szkodliwy-nierentowny/a-54870406 [dostęp: 23 VI 2021].

Kucharczyk M., *Czy Rosja wspierała katalońskich niepodległościowców?*, Euractiv, 28 XI 2011 r., euractiv.pl/section/demokracja/news/czy-rosja-wspierala-katalonskich-niepodlegloscowcow [dostęp: 15 V 2021].

Liu Xin, *What Sharp power? It's nothing but „unsmart" power*, USC Center on Public Diplomacy, 15 XI 2018 r., uscpublicdiplomacy.org/blog/what-sharp-power-it's-nothing-"unsmart"-power [dostęp: 10 V 2021].

Łotwa zakazała na rok emisji rosyjskiej telewizji państwowej „Rosja RTR", Studium Europy Wschodniej UW, 9 II 2021 r., studium.uw.edu.pl/lotwa-zakazala-na-rok-emisji-rosyjskiej-telewizji-panstwowej-rosja-rtr/ [dostęp: 11 VI 2021].

Nye J.S. Jr., *How Sharp Power Threatens Soft Power. The Right and Wrong Ways to Respond to Authoritarian Influence*, „Foreign Affairs", 24 I 2018 r., foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power [dostęp: 14 VI 2021].

Przychodniak M., *Chiny wobec kryzysu inicjatywy 17+1*, Polski Instytut Spraw Międzynarodowych, pism.pl/publikacje/Chiny_wobec_kryzysu_inicjatywy_171_ [dostęp: 8 VI 2021].

Rutkowski J., *Nord Stream 2 – wszystko przemawia przeciw temu projektowi*, Forsal, 27 II 2021 r., forsal.pl/gospodarka/artykuly/8106480,nord-stream-2-wszystko-przemawia-przeciw--temu-projektowi.html [dostęp: 23 VI 2021].

Sharp power. Rising Authoritarian Influence: New Forum Report, National Endowment for Democracy, 5 XII 2017 r., https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

Walker Ch., *The Point of Sharp Power*, Project Syndicate, 1 II 2018 r., https://www.project-syndicate.org/commentary/soft-power-shortcomings-by-christopher-walker-2018-02 [dostęp: 14 VI 2021]

Walker Ch., Ludwig J., *The Meaning of Sharp Power. How Authoritarian States Project Influence*, „Foreign Affairs", 16 XI 2017 r., foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power [dostęp: 14 VI 2021].

Abstrakt

Celem artykułu jest próba zdefiniowania strategii *sharp power*, przedstawienie charakterystycznych sposobów jej zastosowania oraz zaproponowanie metod minimalizowania jej negatywnych skutków dla bezpieczeństwa Rzeczpospolitej Polskiej. Po przeanalizowaniu problematyki związanej z rodzajami potęgi państwa (*soft power*, *hard power*, *smart power*) autorzy publikacji sformułowali koherentną definicję *sharp power*. W dalszej części artykułu opisano przykładowe metody realizacji wspomnianej strategii oddziaływania na uczestników stosunków międzynarodowych. Na koniec autorzy przedstawili propozycje rozwiązań instytucjonalno-prawnych, których zadaniem jest przeciwdziałanie potencjalnym posunięciom z zakresu *sharp power* ukierunkowanym na zachwianie bezpieczeństwem i pozycją międzynarodową RP.

Słowa kluczowe: potęga państwa, *sharp power*, *soft power*, *hard power*, *smart power*, wojna informacyjna, konflikt hybrydowy.

Sharp power – introduction to the issue

Abstract

The aim of the article is an attempt to define the sharp power strategy, present characteristic ways of its employment and propose methods of minimizing its negative

consequences for the security of the Republic of Poland. The analysis of the issues related to the types of state power (soft power, hard power, smart power) is followed by a coherent definition of sharp power formulated by the authors of the publication. The consecutive section of the article describes examples of methods of implementing the aforementioned strategy of influencing participants of international relations. Finally, the authors presented proposals for institutional and legal solutions, which are to counteract potential sharp power moves aimed at undermining the security and international position of the Republic of Poland.

Keywords: state power, sharp power, soft power, hard power, smart power, information warfare, hybrid conflict.

RAFAŁ JERZY KRUSZYŃSKI
ORCID: 0000-0003-1690-3813

DOI: 10.4467/20801335PBW.21.024.14301

Czerwone morze, czyli dominacja komunizmu we współczesnym świecie

Zbrodnicze, totalitarne systemy XX w. próbowały kreować „nowego człowieka". Narodowy socjalizm w Niemczech opierał się na pogańskim kulcie krwi (wyższości rasy nordyckiej)[1], faszyzm we Włoszech odwoływał się do statolatrii (bałwochwalczej gloryfikacji państwa)[2], komunizm zaś, w różnych jego odmianach i w różnych państwach, w których był i jest zaprowadzany, adorował i adoruje materializm, czyli materialistycznie pojmowaną historię, człowieka, społeczeństwo, związki międzyludzkie, a w końcu – cały świat i rzeczywistość. Kult materializmu powoduje epistemologiczną (poznawczą) redukcję rzeczywistości[3]. Wszystko przecież jawi się jako wytwór człowieka. Nawet duchowe elementy kultury[4], jak religia, są postrzegane jako twory człowieka. Nie widzi się już metafizyki. Nie dostrzega się możliwości wyjścia człowieka poza siebie (ani potrzeby takiego wyjścia) ku Osobie, która jest, niezależnie od człowieka i jego aktywności fizycznej i psychicznej – ku Bogu. Uwielbienie dla materializmu rozprzestrzenia się po świecie, szczególnie zachodnim, wraz z nową odmianą marksizmu.

Zasadniczym celem artykułu jest ukazanie przyczyn powstania oraz głównych założeń nowego wymiaru marksizmu (zwanego marksizmem kulturowym lub

---

1 G. Kucharczyk, *Chrystofobia. 500 lat nienawiści do Chrystusa i Kościoła*, Warszawa 2020, s. 278 i nast.

2 Tamże, s. 295.

3 Wskazuje się, że: „Jedną z podstawowych tez marksistowskiego materializmu filozoficznego jest twierdzenie, że jedynym bytem samoistnym i obiektywnym, przekształcanym w procesie społeczno-historycznej praktyki przedmiotowej, manifestującym się w doświadczeniu, jest materia. (…) Materia jest bytem, do którego sprowadzają się w ostatecznej instancji wszystkie postacie istniejącej rzeczywistości". Zob. szerzej: *Filozofia marksistowska*, J. Grudzień i in. (red.), Warszawa 1975, s. 204.

4 Na temat podziału na kulturę duchową i materialną zob. szerzej: R. Tokarczyk, *Współczesne kultury prawne*, Warszawa 2012, s. 30 i nast.

neomarksizmem). W artykule autor poświęcił również uwagę rozwojowi neomarksizmu i skutkom jego implementacji. Omawiając te zagadnienia, warto przyjrzeć się dominacji we współczesnym świecie kraju komunistycznego, jakim jest Chińska Republika Ludowa. Zastanowienia wymagają przyczyny takiej sytuacji oraz to, czy można ją łączyć z neomarksistowską rewolucją kulturową. Nie sposób nie postawić także pytania o fundamenty materializmu i hedonizmu w Stanach Zjednoczonych. Czy źródłem jest tu (jak w przypadku Europy) marksizm kulturowy, czy też podłoża trzeba poszukiwać gdzie indziej?

Rozważania należy zacząć od wydarzenia, do którego doszło na początku XX w. na polskiej ziemi. Wygrana Polski w wojnie polsko-bolszewickiej postawiła tamę militarnemu eksportowi rewolucji komunistycznej na Zachód. Nowo odrodzone państwo polskie odparło atak pomimo osamotnienia na arenie międzynarodowej oraz postawy niektórych krajów (jak choćby Anglii), które wręcz układały się z bolszewikami[5]. W opinii autora wsparcie udzielone Polsce przez Francję było co najwyżej symboliczne. Notabene, czy zarówno te, jak i wydarzenia z 1939 r. nauczą kiedyś Polaków ograniczonego zaufania do „gwarancji ochrony" udzielanych przez sojuszników? Polska w 1920 r. obroniła w istocie nie tylko siebie, lecz także tych, którzy nie zamierzali bronić Polski. Nie byłoby jednak zwycięstwa w wojnie polsko-bolszewickiej bez Cudu nad Wisłą 15 sierpnia 1920 r. Dlaczego cudu? Nie dlatego, że skuteczną realizację śmiałego planu gen. Tadeusza Rozwadowskiego (a nie – jak dość powszechnie się przyjmuje – marszałka Józefa Piłsudskiego), ujętego w ramy rozkazu operacyjnego nr 10 000, można uważać niemalże za cud[6], lecz dlatego, że podczas walk pod Ossowem i Wólką Radzymińską miał miejsce cud *par excellence*. Wówczas to – co jest zdarzeniem udokumentowanym – zjawiła się Najświętsza Maryja Panna, co wprawiło bolszewików w przerażenie i doprowadziło do (…) *przemiany ofensywy Armii Czerwonej w defensywę*[7]. Bolszewicy uciekali, jak sami zresztą mówili, przed (…) *Carycą – Matier Bożju*[8].

Gdyby stwierdzić, że to wydarzenie nie mogło zaistnieć (mimo że zostało ono potwierdzone przez setki naocznych świadków) lub że nie wypada o nim pisać w artykule naukowym, lub też w ogóle nie powinno się o nim wspominać w przestrzeni publicznej (jak przez ostatnie 100 lat), a co najwyżej „rozważać we własnym wnętrzu", mogłoby to oznaczać, że pomimo militarnego zwycięstwa Polski w wojnie polsko-bolszewickiej, w dłuższym okresie bolszewicy odnieśli jednak zwycięstwo w starciu kulturowym, gdyż zapanowawali nad ludzkimi umysłami. Nie chodzi tu o zwykłą walkę poglądów, a o postrzeganie istoty człowieka i jego roli oraz miejsca w świecie, o postrzeganie

---

[5] Zob. szerzej: W. Roszkowski, *Najnowsza historia Polski 1914–1945*, Warszawa 2003, s. 75 i nast.; http://www.bitwawarszawska.pl/112-sytuacja_polityczna_przed_bitwa [dostęp: 5 VI 2021]; http://www.bitwawarszawska.pl/118-przypisy [dostęp: 5 VI 2021].

[6] Zob. szerzej: https://historia.org.pl/2018/08/19/bolszewicy-znali-nasze-plany-to-rozkaz-operacyjny-nr-10-000-je-ostatecznie-zmienial-i-ich-zaskoczyl/ [dostęp: 5 VI 2021].

[7] Zob. szerzej: J.M. Bartnik, E.J.P. Storożyńska, *Matka Boża Łaskawa a Cud nad Wisłą*, Warszawa 2011, s. 216 i nast.

[8] Tamże, s. 223.

świata. Wszystko to zaś jest tylko pochodną afirmacji albo negacji Boga i roli Boga w świecie. Negacja będzie oznaczać ostatecznie – jak uczy historia – wyłonienie się totalitarnej dyktatury[9].

Marksizm: reedukacja

Strzeż się człowieku, jeżeli nie chcesz przyjąć „wolności", „oświecenia" czy „nowego ładu", który niesie rewolucja. W przypadku takiego oporu mogą cię czekać dwie drogi: anihilacja albo reedukacja. Anihilacja stała się udziałem chociażby ludności prowincji Wandea, która odrzuciła „dobrodziejstwa" rewolucji francuskiej[10]. Anihilacja dotykała i dotyka rzesz ludzkich w krajach rządzonych przez komunistów[11]. Na początku XX w. w obozie komunistycznym zrodziła się jednak idea drugiej ze wspomnianych dróg. Po kolejnych gospodarczych klęskach komunistów odrodzona Polska zadała ostateczny cios siłowemu rozpowszechnianiu „myśli" marksistowskiej na zachodzie Europy. Okazało się, że polscy (tak samo jak i rosyjscy) robotnicy i chłopi w zasadzie byli odporni na bełkotliwe hasła bolszewików[12]. Jak wskazuje Dariusz Rozwadowski, (…) *proletariat, który według koncepcji Karola Marska miał dokonać rewolucji, całkowicie zawiódł*[13]. Dostrzeżono potrzebę reedukacji społeczeństwa. Zgodnie z założeniami „pierwotnego" marksizmu[14] zmiana bazy (czyli stosunków ekonomicznych) powinna doprowadzić do zmiany w nadbudowie (szerzej: w kulturze)[15]. Rzeczywistość okazała się jednak niezbyt łagodna dla hipotez Karola Marksa i Fryderyka Engelsa.

Antonio Gramsci

Na scenę wkroczył Antonio Gramsci, włoski komunista, który zrewolucjonizował rewolucję. Dokonał przewrotu w postrzeganiu kierunku niezbędnych zmian. Stwierdził bowiem, że to kultura jest pierwotna wobec warunków ekonomicznych, co oznacza, że dla zdobycia władzy politycznej konieczne jest w pierwszej kolejności zdobycie hegemonii kulturowej[16]. Zdaniem Marksa decydujące w rozwoju społeczeństw są elementy

---

[9] Por. Jan Paweł II, *Pamięć i tożsamość*, Kraków 2005, s. 13; W. Roszkowski, *Bunt barbarzyńców. 105 pytań o przyszłość naszej cywilizacji*, Kraków 2020, s. 211 i nast.

[10] Zob. szerzej: G. Kucharczyk, *Chrystofobia. 500 lat nienawiści*…, s. 103 i nast.

[11] R.J. Kruszyński, *USA-ChRL: konflikt konieczny?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 23, s. 55 i przywołana tam literatura.

[12] D. Rozwadowski, *Marksizm kulturowy*, Warszawa 2018, s. 14–21.

[13] Tamże, s. 16.

[14] Mowa tu o dojrzałej formie w ujęciu Karola Marksa. Na temat wielości nurtów w obrębie marksizmu zob. szerzej: L. Kołakowski, *Główne nurty marksizmu. Powstanie – rozwój – rozkład*, Londyn 1988, s. 9 i nast.; R. Tokarczyk, *Współczesne doktryny polityczne*, Warszawa 2010, s. 190 i nast.

[15] Por. G.A. Bagaturijai in., *Karol Marks. Biografia*, Warszawa 1979, s. 586 i nast.

[16] D. Rozwadowski, *Marksizm kulturowy*…, s. 23.

ekonomiczne, tj. stosunki produkcji (ujmowane jako baza)[17]. Na takiej bazie wznosi się nadbudowa[18], do której Marks zaliczył m.in. państwo, prawo, a także kulturę. Gramsci natomiast „nową bazę" dostrzegł w kulturze. To kultura ma potencjał, aby zmienić pozostałe elementy rzeczywistości, zarówno to, co było przez Marksa i Engelsa uznawane za nadbudowę (m.in. władzę polityczną, państwo, prawo), jak i element, który dotychczas był przez marksistów postrzegany jako baza, tj. stosunki produkcji (stosunki ekonomiczne). Jak bowiem wskazywał Gramsci, (…) *hegemonia etyczno-polityczna, nie może nie być zarazem hegemonią ekonomiczną*[19]. Gramsci nauczył się na błędach twórców marksizmu i swą ideologię wyłożył w sposób mglisty, niepoddający się historycznej weryfikacji. Leszek Kołakowski, przytaczając wytyczne Gramsciego, podkreśla, że jego plan kulturowy ma charakter negatywny: przeszłość ma podlegać krytyce i zostać skazana na całkowitą destrukcję, z kolei zagadnienie nowej kultury i jej kształtu ma być odłożone (…) *w nieokreśloną przyszłość*[20]. Jaka przeszłość ma podlegać krytyce aż do destrukcji? Jak wskazywał Gramsci, (…) *cywilizowany świat został dokładnie nasączony chrześcijaństwem przez 2000 lat i reżim ugruntowany w wierze i w wartościach judeochrześcijańskich nie może zostać odrzucony, zanim korzenie te nie zostaną odcięte*[21]. Okazuje się więc, że w planie kulturowym Gramsciego podstawową sprawą była destrukcja chrześcijaństwa. Chrześcijaństwo bowiem postrzegał jako największą siłę antyrewolucyjną[22], a Kościół, według niego, był spoiwem łączącym rolników, robotników, kapitalistów, arystokrację, duchowieństwo i inne klasy oraz stany społeczne w jedną kulturę[23].

Sposobem realizacji nowej rewolucji (czy też rewolucji „po nowemu") nie miała być już siła zbrojna. Konieczny stał się komunistyczny rząd dusz. Jak do niego dojść? Otóż przez wprowadzanie „ducha rozłamu", czyli, jak wskazuje Tadeusz Rynkiewicz, przez (…) *stopniowe fabrykowanie „demokratycznej zgody", „przyzwolenia", „consensusu" w społeczeństwie na dominację idei socjalistycznych*[24]. Fabrykowanie zgody, o którym mówi Rynkiewicz, następuje w procesie „naturalizacji" idei komunistycznych[25]. To zaś powoduje, że ostatecznie te idee są przez społeczeństwo postrzegane jako poglądy „zdroworozsądkowe" i „przeźroczyste"[26], czyli bez konotacji komunistycznych. Istotna wydaje

---

[17] M. Cichoracki, *Marksowski materializm historyczny – koncepcja związku między bazą a nadbudową oraz prymatu czynników ekonomicznych*, „Filozofia Publiczna i Edukacja Demokratyczna" 2012, nr 1, s. 134 i nast.

[18] Tamże.

[19] A. Gramsci, *Nowoczesny Książę*, Warszawa 2006, s. 24, http://marksizm.edu.pl/wydawnictwa/klasyka-mysli-marksistowskiej/antonio-gramsci/nowoczesny-ksiaze/ [dostęp: 5 VI 2021].

[20] L. Kołakowski, *Główne nurty marksizmu*…, s. 984.

[21] Por. D. Rozwadowski, *Marksizm kulturowy*…, s. 21.

[22] P.J. Buchanan, *Samobójstwo supermocarstwa*, Wrocław 2013, s. 66–67.

[23] Por. D. Rozwadowski, *Marksizm kulturowy*…, s. 21.

[24] T. Rynkiewicz, *Od „proletariatu" do „człowieka masowego"*, „Człowiek w Kulturze" 2008, nr 20, s. 280.

[25] Tamże.

[26] Tamże.

się tu owa „stopniowość" (nie wyklucza ona jednak rewolucyjności). Sączenie trucizny zostaje powierzone nie masom, a „intelektualistom organicznym", czyli tym, którzy nie opisują rzeczywistości z zewnątrz, ale, jak wskazuje Kołakowski, (…) *w języku wysokiej kultury „wyrażają" realne doświadczenie i uczucia mas*[27]. Innymi słowy – zawodowi rewolucjoniści. Mają to być: (…) *dyrektorzy różnego typu szkół, rektorzy, nauczyciele, przedstawiciele instytucji religijnych, prezesi fundacji, przedstawiciele mediów, kierownicy domów kultury, właściciele dyskotek, prezesi wspólnot mieszkaniowych, a nawet, tak – wydawałoby się – marginalnych „odcinków frontu ideologicznego", jak związków wędkarskich, miejskich bibliotek czy punktów skupu buraków*[28]. Forpoczta rewolucji. Jak widać, chodzi o oddolne oddziaływanie. Zdobycie szkolnictwa, mediów, wydawnictw, instytucji kulturalnych (jak teatr, kino), a także pozyskanie przedstawicieli zawodów cieszących się pewnym autorytetem w społeczeństwie ma gwarantować możliwość „drążenia skały"[29]. Ludzie instynktownie odrzucili marksizm (jako niemoralny i niepatriotyczny) oraz komunizm (jako bezprawny, bezbożny i zły), zatem – według Gramsciego – konieczny stał się (…) *„długi marsz przez instytucje" religijne, kulturalne i oświatowe Zachodu* w celu wykorzenienia chrześcijaństwa i jego nauk dotyczących Boga, człowieka i moralności[30]. Wszystko zaś po to, aby (…) *stworzyć nowych ludzi, którzy nie będą odruchowo odrzucali marksizmu*[31]. Zdaniem Gramsciego, aby zrealizować cel, komuniści powinni podejmować współpracę z niekomunistycznymi organizacjami lewicowymi, do których zaliczał m.in.: (…) *ruchy feministyczne, ekstremistyczne organizacje ochrony środowiska, tzw. ruchy obrony praw obywatelskich, stowarzyszenia anty-policyjne*, a także propagatorów internacjonalizmu i zwolenników Kościoła tzw. otwartego[32].

Zwycięstwo na polu wojny kulturowej spowodowałoby, że władza polityczna sama, niczym dojrzały owoc, wpadłaby w ręce komunistów[33]. Mimo że wybrana droga nie była postrzegana przez innych zwolenników Marksa jako zgodna z marksistowską ortodoksją, to jednak nie *dóxa*, a *praxis*[34] jest jedną z głównych kategorii marksizmu[35].

---

[27] L. Kołakowski, *Główne nurty marksizmu*…, s. 981.

[28] T. Rynkiewicz, *Od „proletariatu" do*…, s. 280.

[29] P.J. Buchanan, *Śmierć Zachodu*, Wrocław 2006, s. 92–93.

[30] P.J. Buchanan, *Samobójstwo supermocarstwa*…, s. 66–67.

[31] Tamże.

[32] T. Rynkiewicz, *Od „proletariatu" do*…, s. 284.

[33] W. Kulbat, *Wobec zagrożeń wiary*, Łódź 2017, s. 19.

[34] Rozróżnienie tych dwóch kategorii jest związane z marksistowskim podejściem do filozofii jako takiej. Marksiści uważali, w przeciwieństwie do starożytnych Greków – twórców filozofii, że filozofia powinna zmieniać rzeczywistość, a nie ją kontemplować. Filozofia, zdaniem marksistów, nie może być więc refleksją czysto teoretyczną (nie wystarcza poszukiwanie prawdy dla samej tylko prawdy), ale musi zostać podporządkowana praktycznemu jej zastosowaniu. Dlatego też marksiści przypisywali pierwszeństwo działaniu i praktyce (*praxis*), a nie myśli lub niezmiennej idei jako takiej (*dóxa*). Zob. szerzej: G. Reale, *Historia filozofii starożytnej*, t. 1, *Od początków do Sokratesa*, Lublin 2000, s. 54–56.

[35] Por. L. Witkowski, *Antonio Gramsci: marksizm jako filozofia rewolucyjnej praktyki*, „Acta Universitatis Nicolai Copernici. Filozofia" 1987, nr 10, s. 89.

Ponadto nie tylko Gramsci dostrzegał wielkie możliwości tkwiące w wywoływaniu przez komunistów zmian ideowych.

Szkoła frankfurcka

W 1922 r. w Instytucie Marksa-Engelsa w Moskwie z inicjatywy Włodzimierza Lenina odbyło się spotkanie poświęcone marksistowskiej rewolucji „na niwie kulturowej"[36]. Głównymi środkami rewolucji miały być wzbudzanie nienawiści do Boga i wierzących w Boga[37] oraz planowa demoralizacja, zwłaszcza ludzi młodych[38]. Zamiast „kapitalistycznego" małżeństwa monogamicznego wprowadzono w ZSRR całkowitą swobodę seksualną, będącą elementem ustroju komunistycznego[39]. Pojawiły się również, respektowane przez prawo, bigamia i poligamia[40]. Ustanowiono model seksualnej dowolności niegodny człowieka (hedonizm bez odpowiedzialności). ZSRR był pierwszym na świecie państwem, w którym zalegalizowano aborcję (w 1920 r.)[41]. Czerwona Międzynarodówka Kobiet głosiła hasła (…) *wyzwolenia kobiety z jarzma rodziny, macierzyństwa, religii oraz moralności burżuazyjnej*[42]. Taki kierunek zmian okazał się zgubny zarówno ze względu na skutki społeczne, jak i gospodarcze[43]. Józef Stalin, który przejął władzę w ZSRR po śmierci Lenina, rozpoczął odejście od marksistowskiej rewolucji seksualnej[44]. Programowa nienawiść do Boga i ludzi wierzących oczywiście nie została zniesiona. Komuniści nie porzucili jednak próby implementowania rewolucji seksualnej na Zachodzie. Cel został dobitnie wyrażony w stwierdzeniu Williego Münzenberga: *Zachód zrobimy tak zepsutym, że będzie śmierdział*[45]. W 1924 r. przy Uniwersytecie we Frankfurcie nad Menem rozpoczął działalność Instytut Badań Społecznych (wzorowany na Instytucie Marksa-Engelsa), szerzej znany pod nazwą „szkoła frankfurcka"[46].

W 1930 r. kierownictwo Instytutu objął Max Horkheimer – wielbiciel markiza de Sade, od którego nazwiska pochodzi termin „sadyzm"[47]. Rozpoczęło się kulturowe przekuwanie marksizmu w neomarksizm: wrogiem był już nie tyle kapitalizm, ile zachodnia kultura; nie chodziło już o zbrojny przewrót, a o zawładnięcie umysłami i duszami. Zwycięstwo miało przyjść wraz z upadkiem wiary chrześcijańskiej, a do tego

[36] D. Rozwadowski, *Marksizm kulturowy*…, s. 33.

[37] Zob. szerzej: G. Kucharczyk, *Chrystofobia. 500 lat nienawiści*…, s. 230 i nast.

[38] Tamże, s. 229.

[39] P.A. Sorokin, *Amerykańska rewolucja seksualna*, Wrocław 2020, s. 104.

[40] Tamże.

[41] G. Kucharczyk, *Chrystofobia. 500 lat nienawiści*…, s. 229.

[42] Tamże.

[43] P.A. Sorokin, *Amerykańska rewolucja*…, s. 104.

[44] D. Rozwadowski, *Marksizm kulturowy*…, s. 33.

[45] Tamże.

[46] Tamże.

[47] P.J. Buchanan, *Śmierć Zachodu*…, s. 92–93.

konieczny był upadek chrześcijańskiej moralności[48]. Można więc tu dostrzec zbieżność z założeniami Gramsciego. Głównymi przedstawicielami szkoły frankfurckiej byli: Theodor Adorno, Wilhelm Reich oraz Erich Fromm. Ich prace były poświęcone przede wszystkim promowaniu rewolucji seksualnej (jako podstawowego środka ukierunkowanego na upadek chrześcijaństwa) i podważaniu tradycyjnego modelu rodziny[49]. Autor artykułu określa rewolucję seksualną mianem „podstawowego środka w walce z chrześcijaństwem", gdyż zrewolucjonizowanie tej sfery życia człowieka (podatnej na hedonizm) ustanawia przyczółek dalszych wyjątków. Skoro – jak może postrzegać świadomy czy nieświadomy adept rewolucji – jest możliwe uczynienie wyłomu w moralności chrześcijańskiej w sferze życia seksualnego, to jest możliwe czynienie kolejnych wyłomów w innych sferach moralności chrześcijańskiej (relatywizm moralny). To z kolei oznacza, zgodnie z dalszymi wywodami takiego adepta, możliwość (a być może nawet konieczność) podważania chrześcijaństwa, nie tylko w sferze moralności, lecz także w sferze metafizyki, wiary. Skoro wiara chrześcijańska może być usunięta, to czym ją zastąpić[50]? Na to pytanie odpowiadają zawodowi rewolucjoniści (Kołakowski wskazuje, że komunizm w każdym przypadku dąży do sprawowania władzy „wszechobejmującej"[51]).

Po dojściu do władzy Adolfa Hitlera przedstawiciele szkoły frankfurckiej, z których większość była Żydami, wyemigrowali z Niemiec do Stanów Zjednoczonych, gdzie założyli ośrodki w Nowym Jorku i w Kalifornii[52]. Kierunek prac szkoły frankfurckiej na emigracji nie uległ zmianie. Horkheimer wraz z Adorno przygotowali ich ideologiczne ujęcie, tworząc „teorię krytyczną" (zgodnie z postulatami Gramsciego). Była ona definiowana jako (…) *zasadniczo niszczycielski krytycyzm wobec wszystkich głównych elementów zachodniej kultury, łącznie z chrześcijaństwem, kapitalizmem, władzą, rodziną, patriarchatem, hierarchią, moralnością, tradycją, ograniczeniami w sferze seksualności, lojalnością, patriotyzmem, nacjonalizmem, dziedzicznością, etnocentryzmem, konwenansami i konserwatyzmem*[53] (o powodach stworzenia ideologicznego ujęcia jest mowa w dalszej części artykułu). Stwierdzono, że do hegemonii kulturowej należy dojść nie przez prowadzenie dyskusji filozoficznych (zapewne neomarksiści wiedzieli, że taka dyskusja jest dla nich przegrana), a przez psychologiczne formowanie młodych ludzi czy wręcz dzieci[54]. W ten sposób było możliwe ukształtowanie nowego człowieka,

[48] Por. tamże, s. 94.

[49] Zob. szerzej: tamże, s. 94 i nast.; D. Rozwadowski, *Marksizm kulturowy*…, s. 35 i nast.

[50] Na temat zastępowania religii w systemie komunistycznym zob. szerzej: M. Krajski, *Okultystyczne korzenie światowej rewolucji. Ezoteryka w służbie postępu*, Warszawa 2020, s. 205 i nast.

[51] L. Kołakowski, *Cywilizacja na ławie oskarżonych*, Warszawa 1990, s. 297 (szczególnie zob. rozdział: *Komunizm jako formacja kulturalna*).

[52] Zob. szerzej: D. Rozwadowski, *Marksizm kulturowy*…, s. 36.

[53] Tamże, s. 37 i przywołana tam literatura.

[54] Zob. szerzej: E.M. Jones, *Rebelia. Kościół Katolicki i kulturowa rewolucja*, Wrocław 2019, s. 77 i nast.; P.J. Buchanan, *Śmierć Zachodu*…, s. 99.

nasiąkniętego od najmłodszych lat ideami neomarksistowskimi. Dotychczasowy proletariat (robotnicy) stał się siłą reakcyjną, tak więc konieczne było znalezienie nowego proletariatu i nowego modelu „wyzwalania z ucisku". Nowym proletariatem stała się młodzież, nowym uciskiem tradycyjne wychowanie w modelu etyki chrześcijańskiej czy wprost – rzymskokatolickiej, która ogranicza ekspresję seksualną młodych[55]. Trzeba dodać, w odniesieniu do deprawacji młodzieży, że szkolnictwo w Stanach Zjednoczonych już w latach 40. XX w. było zdominowane przez poglądy szkoły frankfurckiej[56]. Dokładne przedstawianie tez szkoły frankfurckiej nie jest przedmiotem niniejszego artykułu, można je jednak sprowadzić do ciągłej walki z chrześcijaństwem i tradycyjnym modelem rodziny oraz do realizacji postulatów rewolucji seksualnej, w tym wczesnej edukacji seksualnej, którą Reich ujmował jako jeden ze sposobów – oprócz rewolucyjnej polityki seksualnej – zniszczenia rodziny[57]. Dla neomarksistów ze szkoły frankfurckiej to właśnie rodzina jest zasadniczym elementem opresyjnego systemu, który niewoli nowy proletariat. Niewoli, tłumiąc instynkt seksualny[58]. Wychowanie zostało więc przez neomarksistów ujęte jako opresja. Nadszedł czas reedukacji młodzieży. Oczywiście nie trzeba dodawać, że chodziło o młodzież świata zachodniego.

USA – kraj antykomunistyczny?

Zimna wojna spowodowała postrzeganie świata jako dychotomicznego, z żelazną kurtyną pośrodku. Walka miała się toczyć między „wolnym światem" (na czele z USA) a komunistami. Zdaniem autora w zimnej wojnie Stany Zjednoczone nie walczyły jednak z komunizmem, a z ZSRR (gdyby walczyły z komunizmem, nie wspomagałyby ChRL, o czym będzie mowa dalej).

Wywód warto rozpocząć od odnotowania roli, jaką mający wpływy i znaczenie finansiści i przedsiębiorcy z USA odegrali w sponsorowaniu rewolucji komunistycznej w Rosji oraz w jej propagowaniu na arenie międzynarodowej[59]. Świadczy o tym chociażby zmiana kierunku rządu brytyjskiego na bardziej przychylny bolszewikom, co nastąpiło po bezpośredniej interwencji[60] Williama Boyce'a Thompsona (dyrektora Banku Rezerwy Federalnej w Nowym Jorku, najważniejszego banku w Systemie

[55] D. Rozwadowski, *Marksizm kulturowy*…, s. 66–67 i przywołana tam literatura.

[56] P.J. Buchanan, *Śmierć Zachodu*…, s. 99.

[57] Tamże, s. 104.

[58] D. Rozwadowski, *Marksizm kulturowy*…, s. 56–57 i przywołana tam literatura.

[59] Zob. szerzej: A.C. Sutton, *Wall Street a rewolucja bolszewicka*, Wrocław 2017, s. 169 i nast.

[60] Thompson wraz z Thomasem Williamem Lamontem, wspólnikiem w J.P. Morgan & Company, przekonali Lloyda George'a i innych – wówczas jeszcze antybolszewickich – członków rządu, że bolszewicy w Rosji przetrwają, więc alianci powinni zmienić swą dotychczasową politykę i wesprzeć Lenina i Trockiego, ponieważ mają do wyboru: Rosję wrogą, neutralną lub sojuszniczą (w tle występowała możliwość realizacji handlu międzynarodowego). Zob. szerzej: tamże, s. 85–90.

Rezerwy Federalnej, specjalistę od inwestycji wysokiego ryzyka[61]) u ówczesnego premiera Wielkiej Brytanii Lloyda George'a w grudniu 1917 r.[62] (Wielka Brytania miała wówczas jeszcze pewne znaczenie jako imperium[63]). Nie sposób również nie zauważyć współpracy USA i ZSRR w czasie II wojny światowej. Za godną uwagi należy uznać wypowiedź Belli V. Dodd, działaczki Komunistycznej Partii USA (dalej: KP USA) w tamtym okresie, wskazującą, że po konferencji w Teheranie w KP USA panowało przeświadczenie o nadchodzącym nowym światowym ładzie, końcu imperializmu i powstaniu radziecko-amerykańskiej jedności, która będzie trwała po wojnie[64]. Gil Green (wysoko postawiony funkcjonariusz partyjny, m.in. przewodniczący KP USA w stanie Nowy Jork) miał stwierdzić: *Stany Zjednoczone i Związek Sowiecki wspólnie rozwiążą problemy kolonialne świata i w ogóle wszystkie inne jego problemy*[65]. Nie jest istotne ślepe przekonanie komunistycznego lidera o możliwości rozwiązania problemów świata przez komunistów. Istotna jest jednak atmosfera panująca wśród działaczy i liderów KP USA, atmosfera przyjaźni amerykańsko-radzieckiej. Co ciekawe, komuniści w USA (oczywiście za przyzwoleniem centrali w Moskwie – jak to w ówczesnym komunizmie bywało) otwarcie popierali m.in. akcję „zero strajków"[66], co było postępowaniem wbrew robotnikom. Dodd stwierdza, że (…) *partia komunistyczna wzięła klasę pracującą w sztywne cugle. Żaden pracodawca nie był bardziej skuteczny czy też bardziej bezlitosny w tłumieniu strajków albo w bagatelizowaniu robotniczych skarg odnośnie* [do] *nierówności zarobków i warunków pracy*[67]. KP USA wyciszała sprawy, które powinna była wykorzystać w walce z „imperialistami", a jednocześnie organizowała kampanie przeciw osobom stojącym na czele niepokornych ruchów społecznych[68]. Wszystko to czyniła w celu ochrony gospodarki Stanów Zjednoczonych (czyli w istocie pracodawców, bez uwzględnienia interesu pracowników). Komuniści z KP USA nie tylko nie dbali o dobro robotników, ale nawet nie udawali przed samymi robotnikami, że o nich dbają. *Praxis*, nie *dóxa*. Proletariat może być definiowany różnie. Niezależnie jednak od tego, jak jest definiowany, zawsze i wszędzie – w zależności od potrzeb komunistów – jest on tylko środkiem do uzyskania celu, a to z kolei wskazuje na wręcz „pasożytniczy" charakter komunizmu[69]. Celem jest uzyskanie totalitarnej władzy nad całym społeczeństwem.

---

[61] Tamże, s. 67, 85–86.

[62] Tamże, s. 171.

[63] https://historia.org.pl/2019/04/01/jak-bledy-polityczne-zatopily-imperium-brytyjskie/ [dostęp: 5 VI 2021].

[64] B.V. Dodd, *Szkoła ciemności*, Kraków 2020, s. 202.

[65] Tamże, s. 202.

[66] Tamże, s. 213.

[67] Tamże, s. 183.

[68] Tamże.

[69] L. Kołakowski, *Cywilizacja na ławie*…, s. 304.

Mimo etapu przyjaźni USA z ZSRR coś jednak poszło nie tak, skoro niedługo potem nastąpiły zmagania znane powszechnie jako zimna wojna, które trwały kilka dekad. Zdumiewające, jak często tzw. mądrość ludowa przychodzi z prostymi (i jakże trafnymi) odpowiedziami na skomplikowane pytania (lub na pytania dotyczące skomplikowanego stanu faktycznego). Według autora podstawą konfliktu, jaki miał wybuchnąć pomiędzy USA i ZSRR, nie były wcale różnice ideologiczne ani polityczne. O tym, że nie były to różnice ideologiczne świadczy to, że szkoła frankfurcka, promująca przecież marksizm kulturowy, dobrze sobie radziła w Stanach Zjednoczonych. Co więcej, między oboma systemami kapitalistycznym i komunistycznym występowała istotna łączność, która objawiała się w materializmie[70].

W kontekście braku różnic politycznych należy natomiast wskazać, że decydenci w Stanach Zjednoczonych musieli wiedzieć od dawna, kim jest Józef Stalin i co zapewne zrobi z państwami, jak chociażby z Polską, oddanymi mu na konferencjach tzw. wielkiej trójki. Wypowiedź Winstona Churchilla z marca 1946 r. o żelaznej kurtynie[71] nie padła w związku z uzyskanymi nowymi informacjami na temat charakteru czy działań Stalina. Co zatem legło u podstaw konfliktu na linii USA–ZSRR? Według autora były to pieniądze.

Od 1 do 22 lipca 1944 r. w miejscowości Bretton Woods odbywała się (…) *międzynarodowa konferencja walutowo-finansowa Narodów Zjednoczonych zwołana z inicjatywy Stanów Zjednoczonych*[72]. Była ona przełomowa dla sprawy utworzenia międzynarodowego, powojennego porządku finansowego[73]. To na podstawie ustaleń z Bretton Woods powołano m.in. Międzynarodowy Fundusz Walutowy (MFW) oraz Międzynarodowy Bank Odbudowy i Rozwoju[74]. Na nowym porządku finansowym świata nie skorzystał natomiast ZSRR[75]. Warto też zwrócić uwagę na zbieżność dat. W tym samym roku (1944 r.) na zjeździe KP USA wysłannicy Komunistycznej Partii Włoch sprzeciwili się kierunkom działania amerykańskich komunistów polegającym na próbach

---

[70] Ciekawe są zbieżności komunizmu (w ujęciu Marksa) i kapitalizmu. Obydwa systemy prezentują przecież skrajnie materialistyczny pogląd na świat. Co więcej, centralną kategorią obydwu systemów jest „kapitał". Różnica wydaje się sprowadzać do kwestii, kto powinien dysponować kapitałem i innymi czynnikami produkcji. Warto również mieć na uwadze, że zgodnie z poglądami Marksa komunizm może się rozwinąć wyłącznie w społeczeństwie kapitalistycznym (konieczny jest więc pewien determinizm historyczny i cykl rozwoju dziejowego). Tym samym marksizm mógłby być postrzegany jako swoisty, konkurencyjny wobec kapitalizmu, system zasad gospodarowania kapitałem i transferu kapitału (gdyby nie to, że nie poprzestaje on na zmianach ekonomicznych, tylko zmierza do rewolucyjnego przejęcia władzy i zaprowadzenia dyktatury).

[71] https://www.polskieradio.pl/39/156/Artykul/1066814,Przemowienie-Winstona-Churchilla-w-Fulton [dostęp: 5 VI 2021].

[72] W. Materski, *Konferencja Narodów Zjednoczonych w Bretton Woods i Związek Radziecki*, „Dzieje Najnowsze" 1981, nr 4, s. 29.

[73] Ł. Gruszczyński, M. Menkes, Ł. Nowak, *Prawo międzynarodowe gospodarcze*, Warszawa 2016, s. 156 i nast.

[74] Tamże.

[75] Na ten temat zob. m.in.: J. Bartosiak, *Przeszłość jest prologiem*, Warszawa 2019, s. 362; S. Hongbing, *Wojna o pieniądz. Prawdziwe źródła kryzysów finansowych*, Wrocław 2010, s. 140 i nast.

włączania obcokrajowców do amerykańskiego ruchu robotniczego. Jasne było, że nie mówią tego od siebie, tylko dostali polecenie z samej góry (i nie chodzi tu o kierownictwo partii we Włoszech)[76]. W 1945 r. nastąpiło kolejne uderzenie w KP USA (zgodnie z zasadami komunistycznymi znów zapewne inspirowane odgórnie). Było nim opublikowanie w komunistycznej gazecie listu wpływowego działacza Komunistycznej Partii Francji, w którym zarzucał on KP USA zdradę ideałów marksizmu i piętnował prowadzoną przez KP USA politykę zgody i przyjaźni pomiędzy USA i ZSRR[77]. Ataki innych partii komunistycznych na KP USA w dziwny sposób zbiegały się więc w czasie z konferencją w Bretton Woods, co do której prac ZSRR zgłosił liczne uwagi[78]. Konferencje w Jałcie i Poczdamie odbyły się w 1945 r., skąd w takim razie pierwsze oznaki pęknięcia, którego przejawem było wystąpienie członków KP Włoch już na zjeździe w 1944 r.[79] Nie sposób uznać, że było to „tylko zdanie odrębne w ruchu robotniczym", ponieważ komunizm nie przewiduje zdań odrębnych. Zdaniem autora przyczyną tego konfliktu i kolejnych tarć (aż po konflikt zimnowojenny) pomiędzy USA i ZSRR była właśnie konferencja w Bretton Woods i ustanowiony w jej trakcie nowy, światowy ład finansowy. ZSRR nie mógł się na niego zgodzić, ponieważ przyjęcie go promowało Stany Zjednoczone (czy też – jak czasami się wskazuje – Wall Street[80]) i wzmacniało ich pozycję[81]. Na skutek ataków na KP USA ZSRR zadbał o zakwestionowanie, żywej jeszcze wówczas w KP USA, koncepcji przyjaźni radziecko-amerykańskiej (która to idea powstała przecież za wcześniejszym przyzwoleniem ZSRR), w momencie gdy ta koncepcja stała się nieaktualna z uwagi na brak porozumienia pomiędzy USA a ZSRR co do ustaleń z Bretton Woods. *Praxis* nie *dóxa*. Przyczyną zimnej wojny nie był więc domniemany „antykomunizm" czy antymarksizm Stanów Zjednoczonych, a konflikt, który powstał pomiędzy USA a ZSRR na gruncie finansowym. Ciekawe, że często za datę graniczną pierwszych przejawów zimnej wojny przyjmuje się rok 1947[82]. Zważywszy na negatywne stanowisko ZSRR wobec ustaleń konferencji z Bretton Woods Rada Gubernatorów MFW, wbrew literalnemu brzmieniu postanowień *Umowy o utworzeniu Międzynarodowego Funduszu Walutowego*[83], przesunęła termin przyjęcia członkostwa w MFW (co było warunkiem uzyskania statusu członka założyciela) na… 31 grudnia

[76] B.V. Dodd, *Szkoła ciemności*…, s. 215.

[77] Tamże, s. 216.

[78] W. Materski, *Konferencja Narodów Zjednoczonych*…, s. 35 i nast.

[79] Wskazuje się niekiedy na jałtańskie oznaki zbliżającego się konfliktu. Należy zadać jednak pytanie, co było przyczyną, a co skutkiem. W opinii autora ewentualne problemy polityczne widoczne podczas konferencji w Jałcie nie były czynnikiem napędowym, a objawem. Przyczyną starcia zaś był brak porozumienia w zakresie nowego międzynarodowego ładu finansowego.

[80] S. Hongbing, *Wojna o pieniądz*..., s. 140 i nast.

[81] J. Bartosiak, *Przeszłość jest*…, s. 362.

[82] A. Czubiński, W. Olszewski, *Historia powszechna 1939–1997*, Poznań 2003, s. 211 i nast.

[83] *Umowa o utworzeniu Międzynarodowego Funduszu Walutowego, zawarta w Bretton Woods dnia 22 lipca 1944 r.* (DzU z 1948 r. nr 40 poz. 290) – przyp. red.

1946 r., przy czym udogodnienie to dotyczyło praktycznie ZSRR[84]. Związek Radziecki nie przystąpił wówczas do MFW ani nie przyjął ustaleń konferencji w Bretton Woods.

Rewolucja na Zachodzie

Pomimo uznania ZSRR za wroga ideologia marksizmu (a dokładnie: neomarksizmu) święciła na Zachodzie triumf. W latach 60. nastąpiła pokoleniowa zmiana kadrowa w szkole frankfurckiej w Stanach Zjednoczonych. Wcześniej, bo już w 1951 r., Instytut Badań Społecznych wznowił działalność w swojej dawnej siedzibie w Niemczech (RFN). W USA głównym ideologiem szkoły frankfurckiej został Herbert Marcuse, były oficer Office of Strategic Services (OSS), instytucji będącej poprzedniczką CIA. Marcuse był jednym z przedstawicieli szkoły frankfurckiej, który wyemigrował wraz z nią w latach 30. z Niemiec do USA.

Herbert Marcuse

Już w tezach Gramsciego słychać było echo zawodu skierowane pod adresem robotników. Konieczny był nowy proletariat, ponieważ dotychczasowy (zdefiniowany jeszcze przez Marksa) zawiódł. Jak już wspomniano, nowym proletariatem została okrzyknięta zachodnia młodzież, wychowywana przez swych rodziców w duchu chrześcijańskim. Marcuse poszerzył spektrum potencjalnych adeptów rewolucji. Do struktur rozbudowanego, nowego proletariatu oprócz radykalnej młodzieży mieli być włączeni wojujący członkowie mniejszości rasowych czy seksualnych, feministki, (…) *ludzie wyobcowani, aspołeczni, rewolucjoniści Trzeciego Świata, wszystkie prześladowane „ofiary" Zachodu*[85]. Marcuse dostrzegł potencjał także w nowej broni – obok seksu pojawiły się narkotyki; oczywiście nie w sensie fizycznego pojawienia się, lecz w sensie zaadoptowania ideologicznego[86]. Zmieniały się środki (nikt nie powinien mieć wątpliwości co do tego, że nowy proletariat był – i jest – jedynie środkiem do osiągnięcia celu), lecz idea pozostawała ta sama: przejęcie władzy i ustanowienie totalitarnej dyktatury materialistycznej. Być może niektórzy chcieliby próbować polemizować z tezą o zamiarze ustanowienia współczesnej dyktatury. Przecież – mogliby twierdzić – pokolenia nowej lewicy z lat 60. odrzucały terror i totalitaryzm, wskazując na konieczność zastąpienia tych ostatnich przez (…) *idee wolności, praw człowieka, tolerancji, pacyfizmu, ekologii czy równości*[87]. Warto mieć jednak pełny obraz sytuacji. W 1965 r. ukazała się praca Marcuse'a o znamiennym tytule *Tolerancja represywna*[88]. Już na wstępie swojego eseju Marcuse

[84] W. Materski, *Konferencja Narodów Zjednoczonych*…, s. 40.

[85] P.J. Buchanan, *Śmierć Zachodu*…, s. 101.

[86] Tamże.

[87] D. Rozwadowski, *Marksizm kulturowy*…, s. 106.

[88] https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021].

wskazuje wprost, że (…) *realizacja celu, jakim jest tolerancja, wymagałaby nietolerancji względem dominujących polityk, postaw, opinii i rozszerzenia tolerancji na polityki, postawy i opinie, które są zakazane lub stłumione*[89]. W innym miejscu swojej pracy stwierdza wprost: (…) *tolerancja wyzwalająca oznaczałaby zatem nietolerancję wobec ruchów Prawicy i tolerancję wobec ruchów Lewicy. Jeśli chodzi o zakres tej tolerancji i nietolerancji* (…) *rozciągałby się on na etap działania, dyskusji i propagandy, czynu i słowa*[90]. Zgodnie z poglądami Marcuse'a i powyższymi aksjomatami nietolerancja powinna dotyczyć nawet badań naukowych[91]. Konieczna jest więc dyktatura ludzi właściwie wyedukowanych (tj. reedukowanych). Zdaniem Marcuse'a ta dyktatura miałaby być sprawowana przez nielicznych i niekoniecznie wybranych demokratycznie[92]. Wyraźnie można więc dostrzec tu prymitywny odgłos komunistycznej dyktatury (pomimo całej otoczki pseudonaukowości). Należy też wspomnieć, że podczas studenckich rozruchów w Paryżu w 1968 r.[93] na transparentach widniało m.in. hasło: *Marks, Mao, Marcuse*[94]. Marcuse, wzywający do ustanowienia dyktatury ludzi właściwie wyedukowanych, był więc jednym z głównych ideologów marksizmu (czy też – neomarksizmu). Tym samym nie sposób obronić tezy, że nowe ujęcie marksizmu zrywa z korzeniami terroru i totalitaryzmu. Jak słusznie podsumowuje Rozwadowski, (…) *esej „Tolerancja represywna" został napisany dla marksistowskiej elity i warto to jeszcze raz podkreślić. Marcuse wyznaczył nowy kierunek rewolucji i przypomniał koncepcję kadrowej partii rewolucyjnej.* (…) *mniejszość miała określać także zasady życia społecznego*[95]. W tym

[89] W oryginale: „(…) the realization of the objective of tolerance would call for intolerance toward prevailing policies, attitudes, opinions, and the extension of tolerance to policies, attitudes, and opinions which are outlawed or suppressed", https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021]. Tłumaczenia w tekście pochodzą od autora artykułu (przyp. red.).

[90] W oryginale: „Liberating tolerance, then, would mean intolerance against movements from the Right and toleration of movements from the Left. As to the scope of this tolerance and intolerance: (...) it would extend to the stage of action as well as of discussion and propaganda, of deed as well as of word", https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021].

[91] https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021].

[92] W oryginale: „(…) this would be a small number indeed, and not necessarily that of the elected representatives of the people", https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021].

[93] Jak wskazuje Wojciech Roszkowski, „Akcją [studencką] kierowała Krajowa Unia Studentów Francuskich (…), ale głównymi jej motorami były organizacje trockistowskie i maoistyczne. Przywódcy ruchu studenckiego w rodzaju Cohn-Bendita głosili hasła lewackie i anarchistyczne". Zob. szerzej: W. Roszkowski, *Roztrzaskane lustro. Upadek cywilizacji zachodniej*, Kraków 2019, s. 227.

[94] P.J. Buchanan, *Śmierć Zachodu*…, s. 102.

[95] D. Rozwadowski, *Marksizm kulturowy*…, s. 114 i przywołana tam literatura. Komuniści podkreślają, że „(…) bez kierowniczej roli partii marksistowsko-leninowskiej utrzymanie władzy ludowej i zbudowanie socjalizmu nie jest możliwe". Zob. szerzej: A. Łopatka, *Kierownicza rola partii komunistycznej w systemie demokracji socjalistycznej (krytyka koncepcji antykomunistycznych)*,

kontekście warto przywołać myśl wyrażoną przez Gillian Tett w filmie z 2012 r. *Four Horsemen* (pol. *Czterech jeźdźców Apokalipsy*), że sprawowanie władzy odbywa się aktualnie przez manipulowanie mapą poznawczą, tj. sposobem, w jaki myślimy[96]. Neomarksiści postanowili wykorzystać ten sposób sprawowania władzy w dzisiejszych społeczeństwach „demokratycznych" (nie można bowiem uznać, że władza, która manipuluje swymi obywatelami, jest władzą demokratyczną[97]) do jej przejęcia.

W latach 60. (zwłaszcza w latach 1967–1968) nie tylko w USA, lecz także na szerzej rozumianym Zachodzie zaistniała rewolucja młodzieży. Ze względu na ograniczoną objętość artykułu autor nie analizuje tutaj jej przebiegu w poszczególnych krajach[98]. Wspomniana rewolucja unaoczniła wiele zmian społecznych, politycznych i kulturowych, jakie zaszły dzięki realizacji postulatów Gramsciego i szkoły frankfurckiej[99]. Należy jednak mieć na uwadze istotne różnice pomiędzy Europą a USA w przyczynach zmian kulturowych.

Dzisiejsze skutki rewolucji

Na polu ideowym i kulturowym marksiści odnieśli niewątpliwy sukces, co można dostrzec również w dzisiejszym czasach, na Zachodzie bowiem dominują idee marksistowskie (czy też – neomarksistowskie). W dużym stopniu nastąpiła już, ukazywana przez Rynkiewicza, „naturalizacja" poglądów neomarksistowskich, które obecnie są często postrzegane w społeczeństwie jako „zdroworozsądkowe" i „przeźroczyste"[100].

Co natomiast wydarzyło się na niwie gospodarczej? Uczestnicy rewolucji z lat 60. to głównie ludzie młodzi, przyzwyczajeni do dobrobytu, żyjący z pracy swych rodziców. Program krytyczny szkoły frankfurckiej, negujący wszelkie zasady społeczne, uniemożliwiał zaś tworzenie hierarchicznego, uporządkowanego społeczeństwa zdolnego do produkcji dóbr[101]. Dobrobyt musiał zatem być podtrzymywany przez produkcję realizowaną przez kogoś innego, a nie przez rewolucyjnych członków neomarksistowskiego społeczeństwa Zachodu (hołdujących przecież hedonistycznej zasadzie przyjemności Marcuse'a). Jak należało rozwiązać ten problem? Dzięki importowi taniej siły roboczej (czyli imigracji)[102] i… Chińskiej Republice Ludowej. W tym przypadku znów zadziwia zbieżność dat. W 1971 r. (niedługo po szczycie wydarzeń rewolucyjnych z lat 60.) ChRL zajęła miejsce Tajwanu w Radzie Bezpieczeństwa ONZ. Zbliżenie USA

w: *Marksizm-leninizm w walce z antykomunizmem: konferencja teoretyczna. Moskwa styczeń 1970 – referaty delegacji polskiej*, T. Bujanowska, P. Rogalski (red.), Warszawa 1970, s. 157.

96 *Four Horsemen* (film), R. Ashcroft (reż.), https://www.youtube.com/watch?v=PbudoTJJmM8 [dostęp: 5 VI 2021].

97 T. Snyder, *O tyranii. Dwadzieścia lekcji z dwudziestego wieku*, Kraków 2017, s. 103 i nast.

98 Zob. szerzej: W. Roszkowski, *Roztrzaskane lustro. Upadek…*, s. 213 i nast.

99 D. Rozwadowski, *Marksizm kulturowy…*, s. 116 i nast.

100 T. Rynkiewicz, *Od „proletariatu" do…*, s. 280.

101 D. Rozwadowski, *Marksizm kulturowy…*, s. 133.

102 Tamże, s. 134.

i ChRL mogło więc mieć – poza politycznymi[103] – także silne przesłanki ekonomiczne. W przypadku ChRL tania siła robocza nie miała być importowana. Zachodził proces odwrotny, który z biegiem czasu – co dziś dobitnie widać – doprowadził do niemal zupełnego uzależnienia Zachodu od ChRL[104]. Mowa o procesie przenoszenia produkcji z Zachodu do Chin. Analizując skalę zjawiska, nie sposób oprzeć się wrażeniu, że była to wręcz skoordynowana akcja. Jej beneficjentem miały być Stany Zjednoczone (czy też wprost – Wall Street), choć uczestniczyły w niej także inne państwa Zachodu. W latach 70. powstał system, w którym (…) *USA były największym generatorem popytu na dobra produkowane na całym świecie a w zamian reszta świata lokowała swój kapitał na nowojorskich rynkach i kupowała amerykańskie obligacje*[105]. Ten system został nazwany przez byłego ministra finansów Grecji Yanisa Varoufakisa systemem Globalnego minotaura[106]. Czy jednak w tym systemie minotaurem były rzeczywiście USA, czy raczej ChRL? Stany Zjednoczone, zgodnie z założeniami systemu, miały otrzymywać kapitał, Chińska Republika Ludowa otrzymywała natomiast nie tylko strumień inwestycyjny kapitału (związanego z przenoszeniem produkcji), lecz także strumień pieniędzy wynikający z popytu na produkowane tam dobra. ChRL – USA: dwa do jednego. Taki układ doprowadził do sytuacji, w której Stany Zjednoczone przegrywają wyścig z komunistycznymi Chinami[107]. Według danych Międzynarodowego Funduszu Walutowego PKB ChRL (mierzony przy wykorzystaniu parytetu siły nabywczej) już w 2014 r. przewyższył mierzony w ten sam sposób PKB USA[108]. Parytet siły nabywczej (PSN; ang. *purchasing power parity*) jest uznawany za adekwatny miernik m.in. przez MFW, CIA zaś uznaje PSN wręcz za (…) *najlepsze dostępne narzędzie do porównywania siły gospodarczej i dobrobytu krajów*[109]. Mimo takiego znaczenia PSN, jak wskazuje Graham Allison, niekorzystne dla Stanów Zjednoczonych dane MFW (…) *skłoniły osoby traktujące pozycję Ameryki w świecie jako dogmat do gorączkowego poszukiwania mierników, dzięki którym można by wykazać, że Stany Zjednoczone nadal utrzymują pozycję lidera*[110]. Ekonomiczna przegrana gospodarki USA w konkurencji z gospodarką ChRL jest zatem faktem. Dodatkowo Leslie Howard Gelb, honorowy przewodniczący Rady Stosunków Zagranicznych (ang. Council on Foreign Relations), wprost stwierdził, że

[103] Zob. szerzej: R.J. Kruszyński, *USA-ChRL: konflikt*…, s. 49 i nast.

[104] Zob. szerzej: tamże, s. 61 i przywołana tam literatura.

[105] https://www.rp.pl/Spiskowa-Teoria-Wszystkiego/301029946-Kissinger-i-Wielki-Minotaur.html [dostęp: 5 VI 2021].

[106] V. Yanis, *Globalny minotaur. Europa, Ameryka i przyszłość światowej gospodarki,* Warszawa 2021, s. 111 i nast.

[107] P.J. Buchanan, *Samobójstwo…*, s. 25

[108] G. Allison, *Skazani na wojnę? Czy Ameryka i Chiny unikną Pułapki Tukidydesa?*, Bielsko-Biała 2018, s. 33; https://www.businessinsider.com/china-overtakes-us-as-worlds-largest-economy-2014-10?IR=T [dostęp: 5 VI 2021].

[109] Tamże.

[110] Tamże.

(…) *żadne państwo o ogromnym długu publicznym nie utrzymało statusu mocarstwa*[111]. W styczniu 2021 r. dług publiczny USA pobił kolejny rekord i wynosi już ponad 27 bln dolarów[112].

Ciąg wydarzeń doprowadził więc do sytuacji, w której Zachód jest zdominowany przez marksizm w wymiarze kulturowym (neomarksizm), Wschód zaś (a właściwie komunistyczna ChRL) dominuje gospodarczo nad Zachodem, a także rozprzestrzenia na cały świat totalitarne koncepcje (i środki, w tym techniczne) rodem z najczarniejszych wizji George'a Orwella. Przykładem może tu być chociażby wprowadzanie w ostatnim okresie tzw. koronapaszportów, których zastosowanie w jakiejkolwiek postaci, w opinii autora, doprowadzi do nowej formy apartheidu[113].

USA a Europa – zmiany kulturowe i (neo)marksizm

Zmiany kulturowe zaszły zarówno w Europie, jak i w Stanach Zjednoczonych. W tym miejscu warto omówić źródła wspomnianych zmian. John Glubb wskazał, że (…) *powstanie i upadek wielkiego narodu wydaje się przebiegać* przez następujące fazy: (…) *Faza Pionierów (lub Zrywu), Faza Zdobywców (lub Podboju), Faza Rozwoju*

[111] P.J. Buchanan, *Samobójstwo…*, s. 16.

[112] https://www.bankier.pl/wiadomosc/Stany-Zadluzone-Ameryki-Dlug-publiczny-USA-rownie-wielki-co-wyjatkowy-8039764.html [dostęp: 5 VI 2021].

[113] Istotą apartheidu, totalitarnego systemu panującego w Republice Południowej Afryki, był segregacjonizm. Jakikolwiek system oparty na segregacjonizmie stanowi więc nową formę apartheidu, w której istota systemu pozostaje ciągle ta sama: podział ludzi na lepszych i gorszych. Może się jedynie zmieniać *criterium divisionis*: w RPA była to rasa człowieka; aktualnie jest to cecha związana ze zdrowiem człowieka, np. określone szczepienie. Następuje zróżnicowanie sytuacji, w tym niejednokrotnie prawnej, ludzi (grup) uznanych za gorszych. Dla ukazania możliwego stopnia absurdu i jednocześnie barbarzyństwa, do jakiego taki stan może doprowadzić, wystarczy przytoczyć słowa Hansa Joachima Rehsego (członka składu orzekającego Trybunału Narodowego III Rzeszy, który uczestniczył w skazaniu na karę śmierci 231 osób), gdy na zadane mu pytanie, co zrobiłby jako sędzia, „(…) jeśliby ustanowione zostało prawo, według którego wszyscy noszący okulary byliby surowo karani?", odpowiedział – „Zupełnie nic nie mógłbym zrobić. Musielibyśmy być posłuszni". Zob. szerzej: W. Kulesza, *Crimien laesae iustitiae. Odpowiedzialność karna sędziów i prokuratorów za zbrodnie sądowe według prawa norymberskiego, niemieckiego, austriackiego i polskiego*, Łódź 2013, s. 16. System oparty na segregacjonizmie jest więc nie tylko systemem antyludzkim, lecz także antyspołecznym, niszczy bowiem społeczeństwo jako wspólnotę. W perspektywie potencjalnej dychotomii „zaszczepiony przeciw COVID-19 – niezaszczepiony przeciw COVID-19" nie sposób pominąć milczeniem wyników analiz, według których nie ma istotnej różnicy między zdolnością do zakażania innych przez osoby zaszczepione i niezaszczepione przeciw COVID-19. Zob. szerzej: https://www.cdc.gov/mmwr/volumes/70/wr/mm7031e2.htm [dostęp: 4 VIII 2021]. W takim więc razie próba różnicowania sytuacji faktycznej lub prawnej osób zaszczepionych i niezaszczepionych przeciw COVID-19 musiałaby być, zdaniem autora, uznana nie tylko za niespełniającą wymogów demokratycznego państwa prawnego, lecz także za sprzeczną z wymogami rozumu.

Gospodarki, Faza Obfitości, Faza Intelektu, Faza Schyłku (lub Upadku)[114]. Faza Schyłku charakteryzuje się m.in.: (…) *materializmem, rozwiązłością, napływem cudzoziemców, opiekuńczością państwa* czy (…) *osłabieniem religii*, a jest spowodowana (…) *zbyt długim okresem bogactwa i sprawowania władzy, egoizmem, pociągiem do pieniędzy* oraz (…) *utratą poczucia obowiązku*[115]. Można dostrzec, że elementy Fazy Schyłku pokrywają się z konsekwencjami neomarksistowskiej rewolucji kulturowej. Czy zatem za obecny stan świata zachodniego można obwiniać neomarksizm, czy może mamy tu do czynienia z prawami historii?

Przedstawiane przez Glubba fazy odnoszą się do wielkiego narodu, imperium (okres świetności takiego imperium określa on na przeciętnie 250 lat, czyli 10 pokoleń[116]). W swojej analizie Glubb niejednokrotnie wprost wspomina o USA: *Stany Zjednoczone obudziły się nagle jako wielki naród, a okres pionierski, zamiast w podboju ludów ościennych, znalazł ujście w podboju wielkiego kontynentu. Kolejne fazy historii USA podążały jednak wedle schematu, który próbujemy tu nakreślić: Faza Pionierska, Faza Rozwoju Gospodarki, Faza Obfitości, Faza Intelektu i Faza Schyłku (lub Dekadencji)*[117]. W USA do rewolucji seksualnej (pierwszej) doszło już w latach 20. XX w., czyli jeszcze przed rozprzestrzenieniem nauk szkoły frankfurckiej[118]. Wydaje się, że miało to wpływ na dość łatwe zaakceptowanie w USA neomarksistowskich koncepcji szkoły frankfurckiej, w tym koncepcji człowieka zredukowanego jedynie do wymiaru ciała i seksu. To, że pierwsza rewolucja seksualna zaistniała w USA jeszcze przed rozpropagowaniem nauk szkoły frankfurckiej, zaowocowało przygotowaniem przez tę szkołę wspomnianej „teorii krytycznej". Przedstawiciele szkoły dostrzegli bowiem, że w Stanach Zjednoczonych kapitalizm nie upada jedynie przez rewolucję seksualną[119]. Dlaczego nie upada? Poniżej zostanie przedstawiony pogląd autora na ten temat. Rewolucja seksualna narzucana przez szkołę frankfurcką była nowością w Europie, ale nie w USA. Stany Zjednoczone już wtedy weszły w Fazę Upadku, o której mówi Glubb. Innym przejawem tej fazy, poza rozwiązłością seksualną, jest m.in. wspomniany materializm (występujący zarówno w kapitalizmie, jak i w marksizmie, a w USA wynikający właśnie z kapitalizmu). Materializm ugruntowuje konsumpcjonistyczne postrzeganie świata, a to z kolei umacnia system kapitalistyczny. Konsumpcjonizm powoduje, że jako towar są postrzegane nie tylko rzeczy, lecz także ludzie. Chodzi tylko o zaspokojenie egoistycznych potrzeb. Egoizm związany z kapitalizmem i materializmem[120] jest więc, oprócz innych

[114] J. Glubb, *Cykl życia imperium. W poszukiwaniu środków zaradczych*, Warszawa 2017, s. 78.

[115] Tamże, s. 78–79.

[116] Tamże, s. 30 i 78.

[117] Tamże, s. 37.

[118] Zob. szerzej: P.A. Sorokin, *Amerykańska rewolucja*…, s. 22 i nast.; D. Rozwadowski, *Marksizm kulturowy*…, s. 37 i nast.

[119] D. Rozwadowski, *Marksizm kulturowy*…, s. 37.

[120] Zob. szerzej: J.K. Galbraith, *Ekonomia w perspektywie. Krytyka historyczna*, Warszawa 1992, s. 77; R. Cooter, T. Ulen, *Ekonomiczna analiza prawa*, Warszawa 2009, s. 5 i nast.

symptomów, objawem upadku cywilizacji – ludzie przestają myśleć o dobru wspólnym, a myślą jedynie o dobru własnym, sprowadzonym przede wszystkim do posiadania dóbr materialnych i pieniędzy[121]. Wszystkie wymienione elementy składają się (choć nie wyczerpują) na swego rodzaju zaklęte koło, które tocząc się, nie upada (jeszcze), lecz niechybnie dąży, zgodnie z wywodami Glubba, ku upadkowi. Idee szkoły frankfurckiej doskonale wpisują się w taki krajobraz. Zdaniem autora można zatem skłaniać się ku tezie, że zmiany kulturowe, jakie zaszły w USA, były związane z wejściem w Fazę Upadku, jednak nie bez znaczenia dla tempa i ostatecznego ich kierunku wydaje się również „teoria krytyczna". W USA nastąpiła bowiem implementacja neomarksizmu. Gdy mowa o upadku, należy mieć na względzie to, że niekoniecznie musi chodzić o rozkład organizacji państwowej, jak chociażby w Cesarstwie zachodniorzymskim. Dla mocarstwa upadkiem jest także utrata pozycji międzynarodowej, podobnie jak było w przypadku imperium brytyjskiego. Zdaniem autora właśnie taka przyszłość (istotna utrata pozycji, a nie tylko przegrana w konkurencji z Chinami, o czym mowa była powyżej) czeka Stany Zjednoczone. Przebieg Fazy Schyłku, jak uważa Glubb, zależy nie tyle od czynników wewnętrznych (one jedynie zapoczątkowują proces), ile od zewnętrznych, które (…) *pojawiają się podczas upadku i powodują przejęcie władzy*[122]. Dla Stanów Zjednoczonych tym czynnikiem zewnętrznym może być Chińska Republika Ludowa, która jawi się jako nowy dominant w stosunkach światowych[123].

Ideologię neomarskistowską (a nie prawa historii, jak w przypadku USA) można uznać za przyczynę zmian kulturowych (rewolucji kulturowej) w Europie. W kontekście europejskim (a dokładniej – integracji europejskiej) warto mieć także na uwadze,

[121] „Ludzie zdobywają pieniądze dla siebie samych, a nie dla swojego kraju", J. Glubb, *Cykl życia imperium*…, s. 64.

[122] Tamże, s. 72.

[123] R.J. Kruszyński, *USA-ChRL: konflikt*…, s. 61 i przywołana tam literatura. ChRL dodatkowo przejmuje inicjatywę międzynarodową, co uwidoczniło się chociażby w podpisaniu będącego największą na świecie umową handlową porozumienia RCEP (ang. *Regional Comprehensive Economic Partnership*), które bywa także ujmowane jako odnoszące się nie tyle do wolnego handlu, ile do ustanowienia „imperialnego systemu preferencji: Pax Sinica". ChRL nie oddziela spraw gospodarczych od politycznych czy militarnych, dlatego też RCEP może w przyszłości istotnie zmienić układ sił (nie tylko ekonomicznych) w regionie oraz na świecie. Na ten temat zob. szerzej: https://biznes.gazetaprawna.pl/artykuly/1496193,asean-podpisanie-umowy-o-wolnym-handlu-chiny-gospodarka.html [dostęp: 5 VI 2021]; https://forsal.pl/swiat/usa/artykuly/8012779,umowa-rcep-to-nowy-pax-sinica-bardziej-niz-wolny-handel-przypomina-imperialny-system-preferencji-opinia.html [dostęp: 5 VI 2021]. Zakończyły się też rozmowy dotyczące umowy inwestycyjnej pomiędzy UE i ChRL (ang. *Comprehensive Agreement on Investment*, CAI), która wymaga ratyfikacji. Zob. m.in.: https://www.pism.pl/publikacje/Zakonczenie_negocjacji_porozumienia_inwestycyjnego_UEChiny [dostęp: 5 VI 2021]. Znamienne wydaje się również wystąpienie przewodniczącego ChRL Xi Jinpinga podczas Światowego Forum Ekonomicznego w 2021 r. Wezwał on wówczas do globalnej koordynacji polityki makroekonomicznej, https://www.rp.pl/Forum-w-Davos/210129588-Forum-w-Davos-Prezydent-Chin-apeluje-o-wspolprace.html [dostęp: 5 VI 2021]. Europa Zachodnia (w tym również, niestety, Polska) wydaje się podatna na posunięcia ChRL, o czym może świadczyć nie tylko treść CAI.

poza tzw. marksizmem kulturowym, komunistyczny *Manifest z Ventotene*[124]. Na oficjalnym portalu Unii Europejskiej włoski komunista Altiero Spinelli, będący współautorem manifestu, jest określany jako jeden z ojców-założycieli Unii Europejskiej. Wskazuje się również na rolę tego dokumentu w europejskiej integracji[125]. W istocie jednak manifest jawi się jako program zaprowadzenia komunizmu w Europie. Można w nim przeczytać m.in.: (…) *prawdziwy ruch rewolucyjny musi powstać spośród tych, którzy potrafili krytykować stare deklaracje polityczne. Musi być zdolny do współpracy z siłami demokratycznymi i komunistycznymi, a także z tymi wszystkimi, którzy przeciwdziałają totalitaryzmowi. Jednocześnie nie dać się uwikłać w polityczne praktyki jakiejkolwiek z tych grup.* Dalej zaś: (…) *aby odpowiedzieć na nasze potrzeby, europejska rewolucja musi być socjalistyczna. To znaczy, mieć za cel wyzwolenie klasy robotniczej i stworzenie dla niej bardziej humanitarnych warunków życia*[126].

Optymiści mogą myśleć, że to jeszcze nie komunizm. W takim razie trzeba zacytować kolejne fragmenty tekstu: (…) *prywatna własność ma być likwidowana, ograniczana, korygowana albo rozszerzana w zależności od sytuacji, nie zaś dogmatycznie, dla zasady.* Następnie: (…) *dzięki dyktaturze partii rewolucyjnej, tworzy się nowe państwo a wraz z nim nowa prawdziwa demokracja.* O jakie państwo chodzi? Na to pytanie można znaleźć odpowiedź w następującym fragmencie[127]:

> (…) kwestia, która musi być rozwiązana jako pierwsza, to zniesienie podziału Europy na suwerenne państwa narodowe. W przeciwnym razie postęp osiągnięty w innych dziedzinach będzie jedynie pozorny. (…) Propaganda i działania winny służyć do ustanowienia, w każdy możliwy sposób, porozumień i więzi między pojedynczymi ruchami, które z pewnością będą formowane w różnych krajach. Już teraz należy budować fundamenty ruchu będącego w stanie zmobilizować wszystkie siły do stworzenia nowego organizmu – wielkiego dzieła całkowicie nowego w dziejach Europy. Będzie nim ustanowienie stabilnego państwa federalnego z europejskimi siłami zbrojnymi zamiast armii narodowych, bez autarkii gospodarczych będących podstawą reżimów totalitarnych.

Warto też zacytować wypowiedź Glubba: (…) *wydaje się, że Wspólnota Europejska powinna zostać zorganizowana właśnie w kontekście możliwego odrodzenia potęgi i dobrobytu Europy Zachodniej*[128]. Integracja europejska może być więc odebrana jako

[124] Polska wersja tekstu Manifestu z Ventotene jest dostępna na stronie: https://www.poloniainstitute.net/battle-of-ideas/manifest-z-ventotene-1941/ [dostęp: 5 VI 2021], angielska zaś na stronie: https://www.cvce.eu/en/obj/the_manifesto_of_ventotene_1941-en-316aa96c-e7ff-4b9e-b43a-958e96afbecc.html [dostęp: 5 VI 2021].

[125] https://europa.eu/european-union/sites/europaeu/files/docs/body/altiero_spinelli_pl.pdf [dostęp: 5 VI 2021].

[126] https://www.poloniainstitute.net/battle-of-ideas/manifest-z-ventotene-1941/ [dostęp: 5 VI 2021], brak numeracji stron (przyp. red.).

[127] Tamże.

[128] J. Glubb, *Cykl życia imperium*…, s. 92.

element pozytywny. Istotne jednak jest to, co jest podłożem integracji. Komunizm nigdy nie przyniósł i nie przyniesie niczego dobrego poza niewoleniem ludzi (w tym kontekście niepokojąca jest m.in. wyrażona w manifeście dążność do ustanowienia armii europejskiej zamiast armii narodowych).

Manifest z Ventotene ma charakter komunistyczny. Od czasu jego powstania do głosu w Europie doszedł również marksizm kulturowy. Jego dominacja jest wzmagana przez amerykanizowanie europejskiej (choć nie tylko) kultury[129] (kultura amerykańska jest neomarksistowska, więc amerykanizowanie kultury w istocie potęguje jedynie nasycenie ideami nowego marskizmu). Warto pamiętać o celu przeprowadzenia rewolucji seksualnej wyrażonym przez Münzenberga: *Zachód zrobimy tak zepsutym, że będzie śmierdział* oraz o tym, że ten cel miał być realizowany w Europie (przeniesienie szkoły frankfurckiej do USA nastąpiło przecież z powodu konieczności ewakuacji z Niemiec, a nie w ramach planowego rozwoju).

Stany Zjednoczone, wchodząc w Fazę Schyłkową, stały się jednocześnie gruntem, na którym szybko przyjęły się idee i „wartości" marksizmu kulturowego (zbieżne, zdaniem Glubba, z tymi propagowanymi w ostatniej fazie życia imperium).

Europa zaś jest aktualnie poddana oddziaływaniu komunistycznego *Manifestu z Ventotene*, neomarksizmu i wpływom dwóch mocarstw: znajdującego się w fazie schyłkowej, tj. Stanów Zjednoczonych (gdzie jednocześnie „zadomowił się" neomarksizm), i ugruntowującego swą pozycję hegemona, tj. Chińskiej Republiki Ludowej, będącej jednocześnie krajem stricte komunistycznym[130].

Zakończenie

Nie sposób nie dostrzec dominacji komunizmu we współczesnym świecie. Różnice, jakie zachodzą między marksizmem w ujęciu Karola Marksa (nazwanym w pewnym uproszczeniu pierwotnym) a tzw. marksizmem kulturowym (czy inaczej: neomarksizmem) są drugorzędne, jeżeli chodzi o istotę światopoglądu. Różnice bowiem dotyczą jedynie kierunków i środków walki, kierunków i środków rewolucji. Istota pozostaje ta sama: dążenie do ustanowienia władzy totalitarnej, materialistycznej dyktatury. Marksizm (czy neomarksizm) i komunizm nie są dwoma odrębnymi bytami. Marksizm zlewa się z komunizmem, a komunizm z marksizmem. Chodzi przecież o wywołanie rewolucji; o przejęcie władzy i totalitarne jej sprawowanie. Leszek Kołakowski słusznie wskazuje,

[129] Zob. m.in.: P. Siuda, *Homogenizacja i amerykanizacja globalnej popkultury*, „Kultura – Historia – Globalizacja" 2011, nr 10, s. 185 i nast., http://www.khg.uni.wroc.pl/files/15khg10_siuda_t.pdf [dostęp: 5 VI 2021]. Co ciekawe, autor cytowanego artykułu zaznacza, że ujmuje kulturę (a właściwie popkulturę) w perspektywie szkoły frankfurckiej.

[130] R.J. Kruszyński, *USA-ChRL: konflikt*…, s. 53 i nast.

że nie można mówić o marksizmie przed Marksem[131]. Marks, twórca komunizmu, komunizmem nazywał (…) *rzeczywisty ruch, który znosi stan obecny*[132].

Marksizm, w tej czy innej postaci, jest tylko (i aż) kolejnym wcieleniem totalitarnych sił działających w historii[133]. Współcześnie nie jest to jedyny przejaw tego rodzaju sił[134]. Jest to jednak wcielenie istotne, dlatego zasługuje na odrębne omówienie. W niniejszym artykule to omówienie przyjęło raczej formę zasygnalizowania tematu, ukazania coraz większego (jednak czy dostrzegalnego?) pogrążania się świata w okowach niewoli. Marek Orzechowski wspomina o nieprzystającej do rzeczywistości „nieznośnej narracji", zgodnie z którą (…) *żyjemy w najbardziej stabilnym, pokojowym okresie* [w dziejach świata][135]. Podobnie można wskazać na nieprzystającą do rzeczywistości „nieznośną narrację" o wolności w świecie, w którym wykuwa się totalitaryzm[136].

Bibliografia

Allison G., *Skazani na wojnę? Czy Ameryka i Chiny unikną Pułapki Tukidydesa?*, Bielsko-Biała 2018, Pascal.

Bagaturija G.A. i in., *Karol Marks. Biografia*, Warszawa 1979, Książka i Wiedza.

Bartnik J.M., Storożyńska E.J.P., *Matka Boża Łaskawa a Cud nad Wisłą*, Warszawa 2011, Wydawnictwo AA.

Bartosiak J., *Przeszłość jest prologiem*, Warszawa 2019, Wydawnictwo Zona Zero.

Buchanan P.J., *Samobójstwo supermocarstwa*, Wrocław 2013, Wektory.

Buchanan P.J., *Śmierć Zachodu*, Wrocław 2006, Wektory.

Cichoracki M., *Marksowski materializm historyczny – koncepcja związku między bazą a nadbudową oraz prymatu czynników ekonomicznych*, „Filozofia Publiczna i Edukacja Demokratyczna" 2012, nr 1, s. 133–138.

Cooter R., Ulen T., *Ekonomiczna analiza prawa*, Warszawa 2009, C.H. Beck.

Czubiński A., Olszewski W., *Historia powszechna 1939–1997*, Poznań 2003, Wydawnictwo Naukowe UAM.

131 L. Kołakowski, *Główne nurty marksizmu…*, s. 15.

132 Tamże, s. 145 i przywołana tam literatura.

133 Zob. szerzej: M. Krajski, *Okultystyczne korzenie…*, s. 7 i nast.

134 Zob. m.in.: G. Kucharczyk, *Chrystofobia. 500 lat nienawiści…*, s. 166–177, 241–245, 347 i nast.

135 M. Orzechowski, *Chaos. Nowy porządek świata*, Warszawa 2018, s. 9.

136 Por. Jan Paweł II, *Pamięć i tożsamość…*, s. 20.

Dodd B.V., *Szkoła ciemności. Wstrząsające świadectwo działaczki Komunistycznej Partii USA*, Kraków 2020, Wydawnictwo AA.

Filozofia marksistowska, Grudzień J. i in. (red.), Warszawa 1975, PWN.

Galbraith J.K., *Ekonomia w perspektywie. Krytyka historyczna*, Warszawa 1992, Państwowe Wydawnictwo Ekonomiczne.

Glubb J., *Cykl życia imperium. W poszukiwaniu środków zaradczych*, tłum. P. Słowiński, J. Kubań, N. Popielewicz, Warszawa 2017, Polsko-Amerykańska Fundacja Edukacji i Rozwoju Ekonomicznego PAFERE : QBS-Jan Kubań.

Gramsci A., *Nowoczesny Książę*, Warszawa 2006, Studenckie Koło Filozofii Marksistowskiej, Uniwersytet Warszawski.

Gruszczyński Ł., Menkes M., Nowak Ł., *Prawo międzynarodowe gospodarcze*, Warszawa 2016, C.H. Beck.

Hongbing S., *Wojna o pieniądz. Prawdziwe źródła kryzysów finansowych*, Wrocław 2010, Wektory

Jan Paweł II, *Pamięć i tożsamość*, Kraków 2005, Znak.

Jones E.M., *Rebelia. Kościół Katolicki i kulturowa rewolucja*, Wrocław 2019, Wektory.

Kołakowski L., *Cywilizacja na ławie oskarżonych*, Warszawa 1990, Res Publica.

Kołakowski L., *Główne nurty marksizmu. Powstanie – rozwój – rozkład*, Londyn 1988, Wydawnictwo Aneks.

Krajski M., *Okultystyczne korzenie światowej rewolucji. Ezoteryka w służbie postępu*, Warszawa 2020, Fronda.

Kruszyński R.J., *USA-ChRL: konflikt konieczny?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 23, s. 48–68.

Kucharczyk G., *Chrystofobia. 500 lat nienawiści do Chrystusa i Kościoła*, Warszawa 2020, Fronda.

Kulbat W., *Wobec zagrożeń wiary*, Łódź 2017, Archidiecezjalne Wydawnictwo Łódzkie.

Kulesza W., *Crimien laesae iustitiae. Odpowiedzialność karna sędziów i prokuratorów za zbrodnie sądowe według prawa norymberskiego, niemieckiego, austriackiego i polskiego*, Łódź 2013, Wydawnictwo Uniwersytetu Łódzkiego.

Łopatka A., *Kierownicza rola partii komunistycznej w systemie demokracji socjalistycznej (krytyka koncepcji antykomunistycznych)*, w: *Marksizm-leninizm w walce z antykomunizmem. Konferencja teoretyczna. Moskwa styczeń 1970 – referaty delegacji polskiej*, T. Bujnowska, P. Rogalski (red.), Warszawa 1970, Książka i Wiedza, s. 151–171.

Materski W., *Konferencja Narodów Zjednoczonych w Bretton Woods i Związek Radziecki*, „Dzieje Najnowsze" 1981, nr 4, s. 159–177.

Reale G., *Historia filozofii starożytnej*, t. 1. *Od początków do Sokratesa*, Lublin 2000, Redakcja Wydawnictw Katolickiego Uniwersytetu Lubelskiego.

Roszkowski W., *Bunt barbarzyńców. 105 pytań o przyszłość naszej cywilizacji*, Kraków 2020, Biały Kruk.

Roszkowski W., *Najnowsza historia Polski 1914–1945*, Warszawa 2003, Świat Książki.

Roszkowski W., *Roztrzaskane lustro. Upadek cywilizacji zachodniej*, Kraków 2019, Biały Kruk.

Rozwadowski D., *Marksizm kulturowy*, Warszawa 2018, Prohibita.

Rynkiewicz T., *Od „proletariatu" do „człowieka masowego"*, „Człowiek w Kulturze" 2008, nr 20, s. 277–288.

Siuda P., *Homogenizacja i amerykanizacja globalnej popkultury*, „Kultura – Historia – Globalizacja" 2011, nr 10, s. 185–197.

Snyder T., *O tyranii. Dwadzieścia lekcji z dwudziestego wieku*, Kraków 2017, Znak.

Sorokin P.A., *Amerykańska rewolucja seksualna*, Wrocław 2020, Wektory.

Sutton A.C., *Wall Street a rewolucja bolszewicka*, tłum. M. Kotowski, Wrocław 2017, Wektory.

Tokarczyk R., *Współczesne doktryny polityczne*, Warszawa 2010, Wolters Kluwer.

Tokarczyk R., *Współczesne kultury prawne*, Warszawa 2012, Wolters Kluwer.

Witkowski L., *Antonio Gramsci: marksizm jako filozofia rewolucyjnej praktyki,* „Acta Universitatis Nicolai Copernici. Filozofia" 1987, nr 10, s. 86–92.

Yanis V., *Globalny minotaur. Europa, Ameryka i przyszłość światowej gospodarki,* Warszawa 2021, Wydawnictwo Naukowe PWN.

Źródła internetowe

15 krajów podpisało największą na świecie umowę o wolnym handlu, „Dziennik Gazeta Prawna", 15 XI 2020 r., https://biznes.gazetaprawna.pl/artykuly/1496193,asean-podpisanie-umowy-o-wolnym-handlu-chiny-gospodarka.html [dostęp: 5 VI 2021].

Altiero Spinelli: niestrudzony federalista, https://europa.eu/european-union/sites/europaeu/files/docs/body/altiero_spinelli_pl.pdf [dostęp: 5 VI 2021].

Bird M., *China Just Overtook The US As The World's Largest Economy*, Business Insider, 8 X 2014 r., https://www.businessinsider.com/china-overtakes-us-as-worlds-largest-economy-2014-10?IR=T [dostęp: 5VI 2021].

Bitwa Warszawska 1920. Sytuacja polityczna przed bitwą, http://www.bitwawarszawska.pl/112-sytuacja_polityczna_przed_bitwa [dostęp: 5 VI 2021].

Brown C.M i in., *Outbreak of SARS-CoV-2 Infections, Including COVID-19 Vaccine Breakthrough Infections, Associated with Large Public Gatherings — Barnstable County, Massachusetts, July 2021*, https://www.cdc.gov/mmwr/volumes/70/wr/mm7031e2.htm [dostęp: 4 VIII 2021].

Duch W., *Bolszewicy w 1920 znali nasze plany, to rozkaz operacyjny nr 10 000 je ostatecznie zmieniał i ich zaskoczył*, Historia.org.pl, 19 VIII 2018 r., https://historia.org.pl/2018/08/19/bolszewicy-znali-nasze-plany-to-rozkaz-operacyjny-nr-10-000 -je-ostatecznie-zmieniał--i-ich-zaskoczył/ [dostęp: 5 VI 2021].

Four Horseman (film), Ashroft R. (reż.) https://www.youtube.com/watch?v=PbudoTJJmM8 [dostęp: 5 VI 2021].

http://www.bitwawarszawska.pl/118-przypisy [dostęp: 5 VI 2021].

KN, Fickling D., *Umowa RCEP to nowy Pax Sinica. Bardziej niż wolny handel przypomina imperialny system preferencji*, Forsal, 19 XI 2020 r., https://forsal.pl/swiat/usa/artykuly/8012779,umowa-rcep-to-nowy-pax-sinica-bardziej-niz-wolny-handel-przypomina--imperialny-system-preferencji-opinia.html [dostęp: 5 VI 2021].

Kozieł H., *Kissinger i Wielki Minotaur*, „Rzeczpospolita", 2 I 2017 r., https://www.rp.pl/Spiskowa--Teoria-Wszystkiego/301029946-Kissinger-i-Wielki-Minotaur.html [dostęp: 5 VI 2021].

Marcuse H., *Repressive Tolerance*, 1960 r., https://www.marcuse.org/herbert/publications/1960s/1965-repressive-tolerance-fulltext.html [dostęp: 5 VI 2021].

Nogal A., *Jak błędy polityczne zatopiły Imperium Brytyjskie*, Historia.org.pl, 1 IV 2019 r., https://historia.org.pl/2019/04/01/jak-bledy-polityczne-zatopily-imperium-brytyjskie/ [dostęp: 5 VI 2021].

Przemówienie Winstona Churchilla w Fulton, Polskie Radio.pl, 5 III 2021 r., https://www.polskieradio.pl/39/156/Artykul/1066814,Przemowienie-Winstona-Churchilla-w-Fulton [dostęp: 5 VI 2021].

Przychodniak M., *Zakończenie negocjacji porozumienia inwestycyjnego UE–Chiny*, 31 XII 2020 r., PISM, https://www.pism.pl/publikacje/Zakonczenie_negocjacji_porozumienia_inwestycyjnego_UEChiny [dostęp: 5 VI 2021].

The Manifesto of Ventotene, CVCE.edu, https://www.cvce.eu/en/obj/the_manifesto_of_ventotene_1941-en-316aa96c-e7ff-4b9e-b43a-958e96afbecc.html [dostęp: 5 VI 2021]; wersja polska *Manifestu z Ventotene* pod adresem: https://www.poloniainstitute.net/battle-of-ideas/manifest-z-ventotene-1941/ [dostęp: 5 VI 2021].

Walewska D., *Forum w Davos. Prezydent Chin apeluje o współpracę*, „Rzeczpospolita", 25 I 2021 r., https://www.rp.pl/Forum-w-Davos/210129588-Forum-w-Davos-Prezydent-Chin-apeluje-o-wspolprace.html [dostęp: 5 VI 2021].

Żuławiński M., *Stany Zadłużone Ameryki. Dług publiczny USA równie wielki, co wyjątkowy*, Bankier.pl, 20 I 2021 r., https://www.bankier.pl/wiadomosc/Stany-Zadluzone-Ameryki--Dlug-publiczny-USA-rownie-wielki-co-wyjatkowy-8039764.html [dostęp: 5 VI 2021].

Abstrakt

Celem artykułu jest ukazanie przyczyn powstania oraz głównych założeń nowego wymiaru marksizmu (zwanego marksizmem kulturowym lub neomarksizmem). Pomimo pewnej przemiany istota tej ideologii pozostaje niezmienna, a jest nią dążenie do ustanowienia materialistycznej i totalitarnej dyktatury. Dzisiejszy świat jawi się jako zdominowany przez komunizm, w tej czy innej formie. Zastanawiające jest, że tezy będące w istocie marksistowskimi są dziś postrzegane jako niemające z marksizmem żadnego związku. Z kolei społeczność międzynarodowa podejmuje szeroką współpracę z Chińską Republiką Ludową. Skoro komunizm dąży do ustanowienia totalitarnej dyktatury, a świat współczesny jest przez komunizm zdominowany, to czy zmierzamy ku niewolniczej przyszłości?

Słowa kluczowe: marksizm kulturowy, neomarksizm, komunizm, dyktatura, totalitaryzm.

The sea of red, that is the domination of communism in the world today

Abstract

The object of this article is to show the reasons for the emergence and the basic assumptions of the new dimension of Marxism (referred to as the cultural Marxism or neo-Marxism). Despite its certain transformation, the essence of the ideology remains unchanged, namely its pursuit to establish a materialistic and totalitarian dictatorship.

The world today appears to be dominated by communism, in one form or another. It is thought-provoking that the theses, which are in fact Marxist, are seen today as having no connection with Marxism. Likewise, the international community undertakes extensive cooperation with China (the People's Republic of China). Since communism moves towards the establishment of a totalitarian dictatorship, and the modern world is dominated by communism, are we heading towards a servile future?

Keywords: cultural Marxism, neo-Marxism, communism, dictatorship, totalitarianism.

RAFAŁ WĄDOŁOWSKI
ORCID: 0000-0003-0601-1213

DOI: 10.4467/20801335PBW.21.025.14302

Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne

Bieżące kierunki polskiej polityki międzynarodowej świadczą o dążeniu do zacieśniania gospodarczej i militarnej współpracy Rzeczpospolitej Polskiej ze Stanami Zjednoczonymi Ameryki. Wiedza o przyjętych w USA aktualnych regulacjach prawnych dotyczących bezpieczeństwa tajemnic publicznoprawnych może być jednym z wielu elementów wspierających kształtowanie optymalnego systemu ich ochrony w RP. Jest to szczególnie ważne w kontekście współdziałania Sił Zbrojnych RP z komponentami US Army rozlokowanymi na terytorium naszego kraju. Rzeczpospolita Polska jest związana wieloma umowami bilateralnymi z USA[1]. W 2020 r. zawarto niezwykle ważną umowę dotyczącą wzmocnionej współpracy obronnej, która konstytuuje i szczegółowo określa uwarunkowania prawne, gospodarcze i militarne pobytu Sił Zbrojnych USA na terytorium RP[2]. Strony umowy zdefiniowały rozumienie informacji niejawnych we wzajemnych stosunkach, wskazując między innymi na to, że są to informacje, które

[1] *Ustawa z dnia 20 marca 2015 r. o ratyfikacji Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie* (DzU z 2015 r. poz. 686); *Memorandum o porozumieniu między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzajemności w ramach zamówień obronnych, podpisane w Waszyngtonie dnia 27 sierpnia 2011 r. oraz w Warszawie dnia 8 września 2011 r.* (DzU z 2012 r. poz. 975); *Umowa o zabezpieczeniu społecznym między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisana w Warszawie dnia 2 kwietnia 2008 r.* (DzU z 2009 r. nr 46 poz. 374); *Protokół dodatkowy między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisany w Brukseli dnia 12 stycznia 2004 r., do Traktatu o stosunkach handlowych i gospodarczych między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, sporządzonego w Waszyngtonie dnia 21 marca 1990 r.* (DzU z 2005 r. nr 3 poz. 14).

[2] Zob. szerzej: *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzmocnionej współpracy obronnej, podpisana w Warszawie dnia 15 sierpnia 2020 r.* (DzU z 2020 r. poz. 2153).

wymagają ochrony zgodnie z prawem i regulacjami wewnętrznymi stron[3]. W kontekście ochrony tajemnic nie można pominąć umownego ustanowienia jurysdykcji umawiających się państw dotyczącej ścigania sprawców przestępstw, które potencjalnie mogą popełnić obywatele każdej ze stron na szkodę drugiego państwa[4]. W celu budowania sojuszniczej interoperacyjności warto poddać analizie amerykańskie przepisy karne i administracyjne, które regulują ochronę informacji niejawnych (*classified information*[5]). Jest to istotne z powodu deficytu aktualnych opracowań w przedmiotowym zakresie. Relewantność przedmiotowego zagadnienia wynika także z historycznych uwarunkowań, tj. kształtowania systemu ochrony tajemnic państwowych w Polsce podczas kilkudziesięcioletniego wpływu na nasz kraj wschodniego modelu zarządzania państwem. Polski system ochrony publicznoprawnych informacji był determinowany zmianami systemu politycznego, które następowały w ubiegłym stuleciu z woli narodu, a niekiedy wbrew niej. Po odzyskaniu niepodległości niebagatelne znaczenie miała recepcja do polskiego porządku prawnego kodeksu karnego feudalnej Rosji z 1903 r.[6] Rosyjskie prawodawstwo wywarło wpływ na kształtowanie polskich instytucji prawa karnego, w tym dotyczących ochrony tajemnic. Proces „sowietyzacji" przepisów karnych nasilił się w okresie socjalistycznego ustroju Polski, tj. od zakończenia II wojny światowej do 1990 r., i pomimo wprowadzenia licznych zmian i nowelizacji aktów prawnych nie można pominąć wpływu rosyjskiego prawodastwa na ukształtowanie aktualnej treści polskich przepisów prawnych.

Przyjmując powyższą argumentację za trafną, można sformułować następującą hipotezę badawczą: procedura weryfikacji osób przed udostępnieniem im informacji niejawnych oraz przesłanki odpowiedzialności karnej za ujawnienie lub wykorzystanie tajemnic publicznoprawnych w USA są krańcowo odmienne od obowiązujących w RP. W celu weryfikacji przyjętej hipotezy należy podjąć próbę sformułowania, uzasadnionych

---

[3] Tamże, art. 2 lit. j: „Wyrażenie »informacje niejawne« oznacza informacje wytworzone przez lub dla Ministerstwa Obrony Narodowej Rzeczypospolitej Polskiej lub Departament Obrony Stanów Zjednoczonych Ameryki (w Stanach Zjednoczonych jako »wojskowe informacje niejawne«), lub informacje, którymi one prawnie dysponują lub które znajdują się pod ich kontrolą, i które wymagają ochrony zgodnie z prawem i regulacjami wewnętrznymi Stron oraz postanowieniami niniejszej Umowy. Informacje niejawne mogą mieć formę ustną, wizualną, elektroniczną, formę dokumentu, lub dowolną inną formę, w tym także formę sprzętu lub technologii".

[4] Tamże, art. 14 ust. 1: „Rzeczypospolita Polska uznaje szczególne znaczenie nadzoru dyscyplinarnego władz sił zbrojnych USA nad członkami sił zbrojnych USA oraz skutki, jakie taki nadzór ma dla gotowości operacyjnej. Tym samym, Rzeczpospolita Polska, na wniosek Stanów Zjednoczonych w celu realizacji zobowiązania o wzajemnej obronie, niniejszym korzysta ze swojego suwerennego prawa i zrzeka się pierwszeństwa Rzeczypospolitej Polskiej w sprawowaniu jurysdykcji karnej".

[5] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski. Prawie wszystkie tłumaczenia w artykule pochodzą od autora (przyp. red.).

[6] *Уголовное уложение от 1903 г.* (Собрание узаконений и распоряжений правительства от 16 Апреля 1903 г. номер 88) [*Kodeks karny z 1903 r.* (Zbiór ustaw i rozporządzeń rządowych z 16 kwietnia 1903 r., numer 88)].

materiałem badawczym, odpowiedzi na następujące pytania: 1. Czy w USA weryfikacja osób przed udostępnieniem niejawnych informacji jest określona prawem, a jeżeli tak, to jaki jest zakres tych regulacji oraz charakter podmiotów wykonujących to prawo? 2. Czy w USA ujawnienie lub bezprawne wykorzystanie informacji niejawnych jest sankcjonowane, a jeżeli tak, to jakie są podstawy odpowiedzialności depozytariusza tajemnicy?

Relewantne regulacje prawne tworzące system ochrony tajemnic USA

W przeciwieństwie do konstytucyjnych regulacji w RP[7] oraz Federacji Rosyjskiej[8] Konstytucja USA[9] nie precyzuje *expressis verbis* prawa obywateli USA do informacji. Nie jest ono również wskazane wśród innych praw i swobód obywatelskich w treści późniejszych poprawek do przywołanej konstytucji. Na uwagę zasługuje pierwsza poprawka, która została przyjęta w 1791 r. Jej wprowadzenie skutkowało pojawieniem się w amerykańskim systemie prawa przepisów dotyczących między innymi wolności prasy i słowa[10].

Z uwagi na omawianą problematykę nie można pominąć również dziewiątej poprawki, zgodnie z którą wyszczególnienie w Konstytucji USA określonych praw nie wyklucza istnienia oraz nie ogranicza innych praw, które nie są w niej wskazane. Tak więc ustanowienie prawa do informacji może nastąpić w akcie niższej rangi, tj. ustawie federalnej[11].

---

[7] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.* (DzU z 1997 r. nr 78 poz. 483, ze zm.), art. 61 ust. 1: „Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa".

[8] *Конституция Российской Федерации от 12 декабря 1993 г.*, статья 29.4: „Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом" (*Konstytucja Federacji Rosyjskiej z 12 grudnia 1993 r.*, art. 29.4: „Każdy ma prawo do swobodnego poszukiwania, uzyskiwania, przekazywania, tworzenia i rozpowszechniania informacji w dowolny, zgodny z prawem, sposób. Wykaz informacji stanowiących tajemnicę państwową określa ustawa federalna").

[9] *Constitution of the United States of America*, House of Representatives, dok. No 110 – 50, 110th Congress, https://www.govinfo.gov/content/pkg/CDOC-110hdoc50/pdf/CDOC-110hdoc50.pdf [dostęp: 4 VI 2021].

[10] Pierwsza poprawka: „Żadna ustawa Kongresu nie może wprowadzić religii ani zabronić swobodnego praktykowania jej, ograniczać wolności słowa lub prasy ani prawa ludu do spokojnych zgromadzeń lub do składania naczelnym władzom petycji o naprawienie krzywd" (tłum. A. Pułło, *Konstytucja Stanów Zjednoczonych Ameryki*, Warszawa 2002).

[11] *Konstytucja Stanów Zjednoczonych Ameryki* w artykule 1 ust. 8 zawiera enumeratywne wyliczenie dziedzin, w odniesieniu do których Kongres Stanów Zjednoczonych ma prawo wydawać ustawy regulujące. Są one skodyfikowane w *United States Code* (dalej: USC) (*Kodeksie Stanów Zjednoczonych*).

Najistotniejszą regulacją uprawniającą obywateli USA do uzyskiwania informacji o funkcjonowaniu administracji rządowej jest federalna *Ustawa o wolności informacji* z 1966 r.[12] Amerykański prawodawca ustanowił w niej prawa osoby zainteresowanej uzyskaniem informacji oraz obowiązki podmiotów zobligowanych do jej udzielenia. W § 522 ust. b pkt 1–9 oraz § 522b ust. c pkt 1–10 określono przypadki wyłączające prawo do informacji, które mogą zostać zastosowane, jeżeli dany organ zdecyduje, że dane informacje spełniają kryteria ustanowione ww. przepisami.

Pierwszą przesłanką umożliwiającą odmowę udzielenia informacji jest jej zaliczenie do informacji niejawnych z uwagi na interes obrony narodowej albo polityki zagranicznej[13]. Przedmiotowa regulacja jest co do istoty zbieżna z polskimi przepisami ustawy o dostępie do informacji publicznej[14], w tym z jej art. 5. W USA istnieje też wiele odrębnych regulacji wyłączających dostęp do informacji publicznej o działalności podmiotów państwowych, czego przykładem może być § 3507 *Kodeksu Stanów Zjednoczonych*[15], w którym amerykański prawodawca między innymi zwalnia dyrektora Wywiadu Narodowego (Director of National Intelligence, DNI)[16] z obowiązku stosowania się do jakichkolwiek przepisów nakazujących ujawnienie: organizacji, funkcji, nazwisk, oficjalnych tytułów, wynagrodzeń lub liczby pracowników zatrudnionych we Wspólnocie Wywiadów (Intelligence Community, IC)[17].

Kodeks składa się z 54 tytułów podzielonych co do zasady kolejno na: rozdziały, części, sekcje, paragrafy, ustępy, punkty i litery. Ustawodawstwo federalne w USC obejmuje m.in. takie działy, jak: *Organizacja rządu i jego pracownicy* (tytuł 5), *Bezpieczeństwo wewnętrzne* (tytuł 6), *Siły zbrojne* (tytuł 10), *Przestępstwa i postępowanie karne* (tytuł 18), *Sądownictwo i procedura sądowa* (tytuł 28), *Wojna i obrona narodowa* (tytuł 50), https://uscode.house.gov/browse.xhtml [dostęp: 4 VI 2021].

[12] *Freedom of Information Act* of 1966, USC, Title 5, § 552 (*Ustawa o wolności informacji* z 1966 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 522.)

[13] Tamże, § 522 ust. b pkt 1 lit. A i lit. B: „This section does not apply to matters that are: (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order" („Niniejszy paragraf nie ma zastosowania do spraw, które są: (1)(A) specjalnie zatwierdzonymi zgodnie z kryteriami ustanowionymi w zarządzeniu wykonawczym, które mają być utrzymywane w tajemnicy w interesie obrony narodowej lub polityki zagranicznej oraz (B) są rzeczywiście właściwie sklasyfikowane zgodnie z takim zarządzeniem wykonawczym").

[14] *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej* (t.j.: DzU z 2020 r. poz. 2176).

[15] USC, Title 50, Chapter 46, § 3507 (*Kodeks Stanów Zjednoczonych,* tytuł 50, rozdział 46, § 3507), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section3507&num=0&edition=prelim [dostęp: 21 I 2021].

[16] Director of National Intelligence, urząd utworzony ustawą Kongresu USA o zapobieganiu terroryzmowi i reformie służb specjalnych z 2004 r. – *Intelligence Reform and Terrorism Prevention Act* of 2004, USC, Title 50, § 401, Public Law 108 – 458 (*Ustawa o zapobieganiu terroryzmowi i reformie służb specjalnych* z 2004 r., *Kodeks Stanów Zjednoczonych*), https://www.govinfo.gov/content/pkg/STATUTE-118/pdf/STATUTE-118-Pg3638.pdf [dostęp: 4 VI 2021].

[17] Nazwa *Intelligence Community* została użyta w *The President Executive Order 12333* of 1981, *United States Intelligence Activities* (*Zarządzeniu Wykonawczym Prezydenta 12333* z 1981 r., *Działania Wywiadowcze Stanów Zjednoczonych*), które w 2008 r. zostało znowelizowane *The President Executive Order 13470* of 2008, *United States Intelligence Activities* (*Zarządzeniem Wykonawczym 13470*

Ważnym judykatem w kontekście tych dwóch wartości, tj. prawa do informacji i prawa do odmowy jej udzielenia, jest wyrok wydany w procesie: magazyn „Hustler" versus Falwell[18]. Nie zagłębiając się w szczegóły sporu, należy odnotować, że był on spowodowany parodią reklamy napojów alkoholowych zamieszczoną w miesięczniku „Hustler", w której wykorzystano wizerunek duchownego Jerry'ego Falwella bez jego zgody. Po długotrwałym procesie sądowym w kilku instancjach Sąd Najwyższy USA w uzasadnieniu rozstrzygnięcia oparł się na pierwszej poprawce, którą zinterpretował bardzo szeroko. Podniósł między innymi, że wolność wyrażania swoich myśli nie jest wyłącznie prawem indywidualnym, a więc dobrem samym w sobie. Dodatkowo wskazał, że wolność słowa jako prawo jest podstawą wspólnego poszukiwania prawdy i siłą całego społeczeństwa[19]. Wspomniany sąd dostrzegł na tle rozpoznawanego konfliktu dotyczącego wolności prasy, że niebagatelną rolą środków masowego przekazu jest poszukiwanie prawdy, czyli zdobywanie obiektywnych informacji.

Prawo żądania udzielenia informacji jest ograniczone obowiązkiem ochrony informacji niejawnych przez ich depozytariusza. W amerykańskim piśmiennictwie prawniczym moc wiążąca imperatywu zakazu ujawniania informacji niejawnych jest szeroko

---

z 2008 r., *Działania Wywiadowcze Stanów Zjednoczonych*). Zarządzenie definiuje służby tworzące wspólnotę: „Office of the Director of National Intelligence, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs, the intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, intelligence elements of the Federal Bureau of Investigation, Office of National Security Intelligence of the Drug Enforcement Administration, Office of Intelligence and Counterintelligence of the Department of Energy, Bureau of Intelligence and Research of the Department of State, Office of Intelligence and Analysis of the Department of the Treasury, Office of Intelligence and Analysis of the Department of Homeland Security, intelligence and counterintelligence elements of the Coast Guard, and such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community" („Biuro Dyrektora Wywiadu Narodowego, Centralna Agencja Wywiadowcza, Agencja Bezpieczeństwa Narodowego, Agencja Wywiadu Obronnego, Narodowa Agencja Wywiadu Geoprzestrzennego, Krajowe Biuro Rozpoznania, inne biura w Departamencie Obrony zajmujące się gromadzeniem informacji przez krajowe i zagraniczne programy rozpoznawcze; jednostki wywiadowcze i kontrwywiadowcze Wojsk Lądowych, Marynarki Wojennej, Sił Powietrznych i Piechoty Morskiej, elementy wywiadowcze Federalnego Biura Śledczego, Biuro Wywiadu Bezpieczeństwa Narodowego Administracji ds. Walki z Narkotykami, Biuro Wywiadu i Kontrwywiadu Departamentu Energii, Biuro Wywiadu i Badań Departamentu Stanu, Biuro Wywiadu i Analiz Departamentu Skarbu, Biuro Wywiadu i Analiz Departamentu Bezpieczeństwa Wewnętrznego, elementy wywiadu i kontrwywiadu Straży Przybrzeżnej, i inne elementy dowolnego departamentu lub agencji, które mogą być wyznaczone przez prezydenta lub wyznaczone wspólnie przez dyrektora i szefa danego departamentu lub agencji jako element Wspólnoty Wywiadów"). Należy dodać, że DIA oraz FBI prowadzą także działania kontrwywiadowcze. Zob. https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf [dostęp: 4 VI 2021].

[18] Wyrok Sądu Najwyższego USA w sprawie „Hustler" v. Falwell, 485 U.S. 46, 24 II 1988 r.

[19] Tamże, s. 51: „(…) freedom to speak one's mind is not only an aspect of individual liberty – and thus a good unto itself – but also is essential to the common quest for truth and the vitality of society as a whole".

komentowana. Heidi Kitrosser negatywnie ocenia ferowanie przez sądy dotkliwych wyroków za ujawnienie informacji niejawnych. Według niej sąd powinien uzyskać stanowisko rządu w sprawie szkód, jakie wynikły z ujawnienia informacji istotnych dla bezpieczeństwa narodowego, oraz rozważyć, czy dla interesu publicznego korzyści wynikające z ujawnienia informacji przeważają nad przewidywanymi szkodami[20]. Aktem prawnym, w który kompleksowo określono zasady postępowania z informacjami niejawnymi, w tym ich klasyfikowanie, deklasyfikowanie (zmianę lub pozbawienie klauzuli) oraz procedurę udostępniania tajemnic, jest *Zarządzenie Wykonawcze Prezydenta 13526* z 2009 r.[21] Przywołany akt zawiera część wstępną, która może być uznana za uzasadnienie ograniczania przez rząd ustawowego prawa obywateli do informacji. Głównym argumentem przytoczonym przez prezydenta USA jest bezpieczeństwo narodowe postrzegane w wymiarze wewnętrznym i zewnętrznym, w tym ochrona społeczeństwa przed międzynarodowym terroryzmem. W zarządzeniu zdefiniowano podmioty uprawnione do selekcji informacji i ich klasyfikacji jako niejawne. Są to wyłącznie podmioty rządowe, a przede wszystkim administracja, która tworzy rząd pod kierunkiem prezydenta USA, oraz inne agencje i organy państwowe. Podkreślono, że agencja, która nadaje informacji klauzulę tajności, nie ma obowiązku uzasadniać swojej decyzji. Jednocześnie zastrzeżono, że główną przesłanką wyłączenia powszechnego dostępu do określonej informacji jest szkoda dla bezpieczeństwa narodowego, jaką mogłoby spowodować upublicznienie informacji objętej ochroną. Relewantnym elementem omawianej regulacji jest zobowiązanie podmiotu klasyfikującego do pozostawania w gotowości do pisemnego określenia potencjalnej szkody, która była podstawą jej utajnienia, i w konsekwencji odmowy upublicznienia (w przypadku wystąpienia z takim wnioskiem przez osobę zainteresowaną informacją). Kryterium rozstrzygającym o utajnieniu jest więc potencjalna szkoda dla interesu państwa, podobnie jak w systemie ochrony tajemnic RP.

Polski ustawodawca w art. 1 ust. 1 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[22] (dalej: ustawa o.i.n.) wskazuje kryteria, których należy użyć

---

[20] Zob. szerzej: H. Kitrosser, *Leak prosecutions and first amendment: New developments and a closer look at the feasibility of protecting leakers*, „William and Mary Law Review" 2015, nr 4, s. 1262 i nast., https://scholarship.law.wm.edu/wmlr/vol56/iss4/7 [dostęp: 4 VI 2021]. Heidi Kitrosser, profesor Uniwersytetu Minnesota, specjalizuje się w badaniu skutków oddziaływania społeczeństwa na sprawowanie władzy państwowej w USA przez korzystanie z prawa do informacji na podstawie pierwszej poprawki do *Konstytucji Stanów Zjednoczonych Ameryki*, https://www.law.umn.edu/profiles/heidi-kitrosser [dostęp: 7 VI 2021].

[21] *The President Executive Order 13526* of 2009, *Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 13526* z 2009 *r.*, *Informacje Niejawne Bezpieczeństwa Narodowego*), akt jest modyfikacją poprzedniego zarządzenia 13292 z 25 III 2003 r., które zmieniało *The President Executive Order 12958*, *Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 12958* z 17 IV 1995 r.).

[22] Tekst jednolity: DzU z 2019 r. poz. 742, art. 1 ust. 1: „Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej »informacjami niejawnymi«".

w procesie selekcji jawnych informacji w celu wyodrębnienia tylko takich, które z uwagi na konstytucyjne przesłanki ograniczenia prawa do informacji można utajnić albo wytworzyć jako niejawne. Ustanowionymi weryfikatorami są skutki, jakie mogłyby nastąpić w wyniku ujawnienia tego rodzaju informacji, czyli: 1) wystąpienie szkody dla RP, 2) spowodowanie zagrożenia wystąpienia szkody dla RP, 3) wywołanie niekorzystnego stanu interesów RP. Analizując przywołane przesłanki, należy zauważyć, że tworzą one **materialną definicję informacji niejawnych**[23], wskazują bowiem na treść, a nadanie klauzuli jest jedynie formalnym oznaczeniem chronionych informacji (komunikatem dla dysponenta wskazującym charakter informacji). W przypadku ustalenia, że ujawnienie danej informacji doprowadzi do zaistnienia chociażby jednego z wymienionych skutków, należy dokonać jej klasyfikacji i nadać odpowiednią klauzulę ochrony, a więc zastosować się do nakazu ustanowionego w art. 5 ustawy o.i.n. Jak wskazuje Trybunał Konstytucyjny w uzasadnieniu wyroku z 2009 r., *Obowiązek przyznawania właściwej klauzuli tajności istnieje i wynika z materialnoprawnych kryteriów klasyfikacji informacji oraz art. 7 Konstytucji*[24].

W procesie klauzulowania należy więc rozważyć, czy w związku z ujawnieniem danej informacji zostaną zagrożone interesy USA, a jeżeli nastąpi szkoda, to jaka, w jakiej formie i w jakim wymiarze. Przedmiotowa regulacja w części dotyczącej braku konieczności formułowania uzasadnienia decyzji klasyfikacyjnej w procesie jej podejmowania jest zbieżna z polskimi przepisami. Amerykański prawodawca uznał, że nieuprawnione ujawnienie klauzulowanych informacji nie jest przesłanką automatycznego pozbawienia ochrony lub zmiany klauzuli informacji niejawnych, podobnych lub tożsamych z ujawnionymi[25]. Przedmiotowe ujęcie tego ważnego problemu pozostaje więc w opozycji do ugruntowanego w polskiej literaturze poglądu, że upublicznione tajemnice nie podlegają karnoprawnej ochronie[26]. Jonathan Abel wskazuje, że pozostawienie upublicznionych informacji jako niejawnych wydaje się bezprzedmiotowe. Argumentuje, że przecież tajemnice USA rozpowszechnione przez Edwarda Snowdena są znane milionom użytkowników Internetu, a mimo to pozostają nadal niejawne, co wyłącza je z publicznej debaty – ze szkodą dla wolności mass mediów[27].

---

[23] Wyróżnienia w tekście pochodzą od autora (przyp. red.).

[24] Wyrok TK z 15 października 2009 r. sygn. akt K 26/08, uzasadnienie – pkt 183.

[25] *The President Executive Order 13526*…, article 1 section 1 letter c: „Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information" (*Zarządzenie Wykonawcze Prezydenta USA 13526*…, art. 1 ust. 1 lit. c*:* „Informacji niejawnych nie odtajnia się automatycznie w wyniku nieuprawnionego ujawnienia identycznych lub podobnych informacji").

[26] Zob. szerzej: M. Leciak, *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, s. 188–190; K. Lewandowski, *Przestępstwa przeciwko ochronie informacji w świetle rozdziału XXXIII Kodeksu karnego*, *orzecznictwa i doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 63; A. Marek., V. Konarska-Wrzosek, *Prawo karne*, Warszawa 2016, s. 682.

[27] Zob. szerzej: J. Abel, *Do you have to keep the Government's secrets*? *Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record*, „University of Pennsylwania Law Review" 2015, nr 4, s. 1039 i nast.

W zarządzeniu 13526 zdefiniowano pojęcie „informacja”[28] oraz wprowadzono trzy poziomy klauzul ochronnych, które są odpowiednie do szkód, jakie mogłoby spowodować nieuprawnione ujawnienie danego rodzaju informacji. Jak już zasygnalizowano, we wspomnianym zarządzeniu zobowiązano organ przyznający klauzulę do pozostawania w gotowości do zidentyfikowania lub opisania potencjalnych szkód w razie konieczności uzasadnienia podjętej decyzji klasyfikacyjnej w odniesieniu do konkretnej informacji, którą utajnił. I tak:

1) klauzulę „Top Secret” stosuje się w odniesieniu do informacji, której nieuprawnione ujawnienie (przy uwzględnieniu racjonalnych przesłanek oceny) mogłoby spowodować **wyjątkowo poważną** szkodę dla bezpieczeństwa narodowego,
2) klauzulę „Secret” stosuje się do ochrony informacji, której nieuprawnione ujawnienie mogłoby spowodować **poważną** szkodę dla bezpieczeństwa narodowego,
3) klauzula „Confidential” jest stosowana z zachowaniem warunków wskazanych w pkt 1, przy czym szkoda nie jest wartościowana.

Zgodnie z omawianym zarządzeniem 13526 przy klasyfikowaniu informacji należy kierować się ogólną zasadą nadawania informacjom bezpośrednio niższej klauzuli, jeżeli wystąpiły istotne wątpliwości co do przyznania adekwatnego poziomu ochrony[29]. Jeżeli nie można rozstrzygnąć, jakiego rodzaju szkoda wystąpiłaby po ujawnieniu informacji stanowiącej tajemnicę, np. czy byłaby ona wyjątkowo poważna, czy jedynie poważana, taką informację należy objąć niższym poziomem ochrony. Powyższa regulacja „uelastycznia” proces klasyfikacji informacji, a tym samym pozwala na uniknięcie ewentualnych zarzutów celowego zaniżenia albo zawyżenia nadanej klauzuli. Przepisy polskiej ustawy o.i.n. w tym zakresie są znacznie bardziej złożone[30], dlatego wydaje się, że recepcja tego rozwiązania na grunt krajowego prawodawstwa byłaby korzystna.

Ogólna przesłanka utajniania informacji, tj. bezpieczeństwo narodowe, w tym ochrona przed międzynarodowym terroryzmem, została doprecyzowana w części I, art. 1 ust. 4 omawianego zarządzenia, w którym enumeratywnie określono sfery podlegające ochronie. Są to:

1) wojskowe plany, systemy uzbrojenia i operacje militarne,
2) informacje od rządów obcych państw,

---

[28] *The President Executive Order 13526*…, article 6 section 1 subsec. 1 letter t: „»Information« – means any knowledge that can be communicated or dokumentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government” (*Zarządzenie Wykonawcze Prezydenta 13526*…, art. 6 ust. 1 pkt 1 lit. t: „»Informacja« – oznacza wszelką wiedzę, którą można zakomunikować albo mającą postać dokumentu materialnego, bez względu na jego fizyczną formę lub cechy, która jest własnością rządu USA lub jest wytworzona przez [rząd] lub dla tego rządu albo jest nadzorowana przez Rząd Stanów Zjednoczonych”).

[29] *The President Executive Order 13526*…, article 1 section 2 letter. c: „If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level” (*Zarządzenie Wykonawcze Prezydenta USA 13526*…, art. 1 ust. 2 lit. c: „Jeśli istnieją poważne wątpliwości co do odpowiedniego poziomu klauzuli, klasyfikuje się [ją] na niższym poziomie”).

[30] Zob. szerzej: art. 9 ustawy o.i.n.

3) stosunki z innymi państwami oraz działania USA poza granicami kraju, w tym poufne zagraniczne źródła informacji,
4) działania służb specjalnych[31], w tym operacje pod przykryciem, źródła informacji oraz metody ich działania, kryptologia,
5) zagadnienia naukowe, technologiczne i ekonomiczne związane z bezpieczeństwem narodowym,
6) rządowe programy ochrony obiektów i materiałów nuklearnych,
7) potencjał: systemów, instalacji, infrastruktury, projektów i planów, a także służb ochrony związanych z bezpieczeństwem narodowym oraz ich słabe strony,
8) rozwój, produkcja oraz stosowanie broni masowego rażenia.

Regulacje ustanowione w art. 5 ustawy o.i.n. w zakresie kryteriów stosowanych w procesie nadawania klauzuli informacjom niejawnym wykazują co do zasady zbieżność ze stosowanymi w USA. Z tego względu warto poddać analizie adekwatne przepisy polskiej ustawy, należy bowiem zauważyć, że prawodawca po skonstruowaniu ogólnej definicji informacji niejawnych w art. 1, w art. 5 ust. 1–3 określa sfery, z których informacjom można nadać klauzulę „ściśle tajne", „tajne" albo „poufne". Między ogólną (abstrakcyjną) definicją informacji niejawnych a przedmiotowym określeniem obszarów aktywności państwa, które należy chronić przez limitowanie informacji, zachodzi relacja nadrzędności i podrzędności. Dziedziny (obszary) wymienione w art. 5 zawężają możliwość szerokiego ograniczania prawa do informacji w wyniku autonomicznego stosowania art. 1 ustawy.

Za uzasadnione należy uznać wątpliwości interpretacyjne powstające w kontekście nieostrych znaczeniowo pojęć, których ustawodawca użył do konstrukcji formalnoprawnych przesłanek służących do nadawania informacjom niejawnym wymaganego poziomu ochrony. Implikuje to pytanie, czy jakakolwiek osoba ustawowo uprawniona do nadania klauzuli[32] dysponuje dostateczną wiedzą, aby uznać, że ujawnienie określonej informacji niejawnej spowoduje albo mogłoby spowodować wystąpienie wyjątkowo poważnej lub poważnej szkody dla RP. Ustawodawca w art. 5 ust. 1–3 wymienia dziedziny, w których szkoda[33] ma wystąpić, ale nie definiuje, jak należy rozumieć szkodę i jakie są kryteria jej wartościowania. Ustawowe dookreślenie szkody w art. 5 ust.1 i ust. 2 pojęciami: „zagrozi", „pogorszy", „zakłóci", „utrudni" i „osłabi" nie wyznacza jasnych ram interpretacyjnych.

Konfrontacja kryteriów weryfikacyjnych wymienionych w art. 1 oraz art. 5 ustawy o.i.n. ujawnia niekonsekwencję ustawodawcy. Zgodnie z **materialną** definicją informacji niejawnych (art. 1) do uznania informacji za niejawną dostateczną przesłankę stanowi

[31] W tekście źródłowym użyto terminu „*intelligence activities*", który jest definiowany w ust. 6 pkt 1 lit. Y *Zarządzenia Wykonawczego Prezydenta 13526* jako „działania Wspólnoty Wywiadów" (IC).

[32] Art. 6 ustawy o.i.n.: „Osobą uprawnioną do nadania klauzuli jest osoba uprawniona do podpisania dokumentu lub oznaczenia danego materiału".

[33] Kierując się zasadą zakazu homonimiczności pojęć, należy przyjąć, że szkoda wskazana w art. 1 jest tożsama ze szkodą z art. 5.

„niekorzystny wpływ na interesy RP", natomiast w definicji **materialno-formalnej** (art. 5 ust. 1 i 2) kryterium niekorzystnego wpływu na interesy RP nie występuje. Można też rozważyć przypadek przyznania jawnej informacji statusu informacji niejawnej z uwagi na niekorzystny wpływ na interesy RP, który może zaistnieć po jej ujawnieniu. Jednocześnie tego typu informacja może pozostać bez klauzuli, ponieważ jej treść nie będzie związana tematycznie z dziedzinami wymienionymi w art. 5 ust. 1–3. Ustawodawca, wskazując na interesy RP w art. 1, odwoływał się do tych obszarów aktywności państwa, które są wymienione w art. 5 ust. 1–3. Przywołane przepisy należy więc stosować łącznie, ich odrębne stosowanie prowadzi bowiem do interpretacji *ad absurdum*.

Częściowo taką sytuację potwierdza stanowisko Naczelnego Sądu Administracyjnego, który stwierdza, że (…) *informacja jest informacją niejawną, nie w następstwie jej klasyfikacji, a z uwagi na zagrożenie wynikające z jej treści lub sposobu jej uzyskania. Chroniona jest zatem jak informacja niejawna bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą*[34]. Sąd słusznie uznał, że treść informacji jest priorytetową przesłanką objęcia jej ochroną państwa, a jednocześnie pominął formalną klasyfikację (oznaczenie klauzulą) jako element przesądzający o tej ochronie.

W USA informacje, które dotyczą powyżej wymienionych zagadnień, mogą zostać zaliczone do niejawnych tylko wówczas, gdy istnieją racjonalne przesłanki pozwalające przewidywać, że ich bezprawne upublicznienie przyniesie szkodę dla bezpieczeństwa narodowego Stanów Zjednoczonych. Podobnie jak w polskim ustawodawstwie w zarządzeniu nie określono wymiaru czasowego ochrony dla danej klauzuli[35]. Sprecyzowano, że może to być dowolny okres, co do zasady nie dłuższy niż 25 lat, albo określone zdarzenie, po którego zaistnieniu należy przeprowadzić deklasyfikację lub powtórną ocenę danej informacji. Amerykański prawodawca zastrzega jednocześnie, że żadne informacje nie mogą pozostać niejawne na zawsze. Wyjątkiem od zasady ochrony do 25 lat są między innymi dane personalne osobowych źródeł informacji (niejawnych współpracowników IC). Dodatkowo prezydent USA wprowadził przepisy prewencyjne, zakazujące utrzymywania w tajemnicy informacji lub obejmowania ich klauzulą, aby ukryć naruszenie prawa przez administrację albo ograniczyć konkurencję, albo ukryć informacje kłopotliwe dla osoby fizycznej lub prawnej. Przedmiotowa regulacja nie ma odzwierciedlenia w polskich aktach normatywnych, mimo że ma aksjologiczne

[34] Wyrok Naczelnego Sądu Administracyjnego z 6 VII 2017 r., sygn. akt. I OSK 932/16.

[35] Uwzględniając aspekt historyczny, warto zaznaczyć, że w nieobowiązującej *Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* polski ustawodawca w art. 25 ust. 1 i 3 wprowadzał ochronę informacji tajnych i ściśle tajnych przez 50 lat, poufnych przez 5 lat i zastrzeżonych przez 2 lata. Obowiązująca obecnie ustawa o.i.n. nie określa długości okresów ochrony, pozostawiając to ocenie osoby, która podpisała dokument, lub osoby odpowiedzialnej za przechowywanie danego materiału, a w odniesieniu do informacji ściśle tajnych – kierownikowi jednostki organizacyjnej przy uwzględnieniu aktualności przyczyn, które spowodowały objęcie ochroną danej informacji. Wyjątkiem od powyższej zasady są informacje wskazane w art. 7 ustawy o.i.n., które dotyczą pracowników służb prowadzących czynności operacyjno-rozpoznawcze i ich współpracowników, a także informacje pochodzące z wymiany międzynarodowej, o ile taki był warunek ich udostępnienia RP – tego rodzaju informacje są objęte ochroną na zawsze.

podstawy. Należy więc postulować wprowadzenie tej instytucji do polskiego systemu ochrony informacji niejawnych. Omawiane zarządzenie wprowadza ponadto zakaz pozostawienia niejawnymi informacji, które nie są ważne ze względu na bezpieczeństwo państwa.

Przyjęcie przedmiotowych przepisów w amerykańskim systemie prawnym wskazuje, że uprawnienie publicznych organów do utajniania informacji może sprzyjać nadużyciom. Ze względu na podobieństwa zasadniczych norm systemu polskiego i amerykańskiego należy uznać, że tożsame zagrożenia występują w Polsce.

Mimo szczegółowego określenia procedury deklasyfikacji tajemnic pozostających w dyspozycji administracji rządowej i nakazu jej bieżącego prowadzenia, zarządzeniem 13526 powołano odrębny organ państwowy – Narodowe Centrum Odtajniania informacji (National Declassification Center, NDC). Głównym zadaniem tego organu jest prowadzenie szkoleń, doradztwo i działania koordynacyjne w procesie odtajniania niejawnych informacji w rządowych jednostkach organizacyjnych. Innymi istotnymi postanowieniami zawartymi w zarządzeniu są zasady dostępu do tajemnic. Wyszczególniono trzy podstawowe warunki, które przed udostępnieniem informacji muszą zostać spełnione: 1) przyznanie uprawnień do dostępu do informacji niejawnych przez kierownika agencji lub osobę przez niego wyznaczoną, 2) podpisanie przez kandydata umowy poufności (*nondisclosure agreement*)[36], 3) dostęp do informacji jest uzasadniony wykonywanymi obowiązkami lub funkcją (zgodnie z zasadą *need to know*).

Organ wydający zgodę na zapoznanie się z informacjami niejawnymi jest również zobowiązany do zorganizowania szkolenia osoby spełniającej wymienione kryteria. Poznaje ona wówczas metody właściwej ochrony informacji niejawnych oraz zostaje pouczona o grożących sankcjach karnych, administracyjnych i odpowiedzialności cywilnej za bezprawne ujawnienie tajemnicy. Warunki wymienione w pkt 1 i 3 mają odpowiedniki w polskiej ustawie o ochronie informacji niejawnych. Warto przypomnieć, że w polskim porządku prawnym dostęp do tajemnic państwowych nie jest determinowany zawarciem umowy z państwem o zachowaniu uzyskanych informacji w tajemnicy. Osoba po zakończeniu szkolenia składa jedynie oświadczenie potwierdzające znajomość przepisów o ochronie informacji niejawnych.

[36] Pisemna umowa jest zawierana pomiędzy osobą, która otrzymuje dostęp do informacji niejawnych, a Stanami Zjednoczonymi. Dokument został wprowadzony do stosowania na mocy *The President Executive Order 12958*…(*Zarządzenia Wykonawczego Prezydenta 12958*…). Osoba zainteresowana zobowiązuje się do zachowania w tajemnicy oznaczonych i nieoznaczonych informacji niejawnych, w tym przekazanych ustnie. Potwierdza, że została poinformowana o przepisach dotyczących ochrony tajemnic, oraz deklaruje ich przestrzeganie, a ponadto, że zapoznano ją z odpowiedzialnością karną jej grożącą. Dodatkowo w treści umowy oświadcza, że pouczono ją o tym, że w wyniku niewłaściwego postępowania z informacjami niejawnymi uprawniony organ może odebrać poświadczenie bezpieczeństwa, które posiada, co z kolei może być podstawą wypowiedzenia stosunku pracy. Zainteresowany zrzeka się na rzecz USA również wszelkich honorariów, należności i wynagrodzeń otrzymanych w związku z ujawnieniem informacji. Końcowy rozdział umowy zawiera wskazówki dla strony i obejmuje okres po zakończeniu udostępniania jej tajemnic, między innymi zawiera pouczenie o zagrożeniu szpiegostwem.

Ogólnokrajowy nadzór nad przetwarzaniem informacji niejawnych sprawuje w USA Urząd Nadzoru Bezpieczeństwa Informacji (Information Security Oversight Office, ISOO)[37]. W zarządzeniu ustanowiono podległość tego organu Archiwum Państwowemu USA i określono jego zadania, w tym:

1) opracowanie aktów wykonawczych w celu implementacji zarządzenia 13526,
2) nadzorowanie agencji rządowych w celu zapewnienia zgodności ich działalności z zarządzeniem i aktami wykonawczymi,
3) składanie prezydentowi USA, przynajmniej raz w roku, raportu z przebiegu implementacji zarządzenia[38].

W polskim systemie ochrony tajemnic nie ma podmiotów tożsamych z NDC i ISOO, jednak podobne zadania nadzorcze są realizowane przez ABW i SKW, zgodnie z właściwością rzeczową tych służb specjalnych. W tym miejscu warto wskazać na istotną rolę Instytutu Pamięci Narodowej, który w celu realizacji ustawowych zadań gromadzi materiały, w tym niejawne, wytworzone przed 6 maja 1990 r. Prezes IPN w każdym czasie może zażądać nieprzekazanych dotychczas dokumentów od: ministra właściwego do spraw wewnętrznych, ministra obrony narodowej, ministra sprawiedliwości, prezesa sądu powszechnego i wojskowego, prokuratora kierującego powszechną jednostką organizacyjną prokuratury, dyrektora Archiwum Akt Nowych oraz innego archiwum państwowego, szefów Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, a także innych instytucji. Na podstawie art. 27 ustawy o IPN prezes IPN jest uprawniony do uzyskania wglądu w dokumenty, jeżeli istnieje uzasadnione przypuszczenie, że te dokumenty zawierają informacje z zakresu działania Instytutu[39]. W ramach działalności archiwalnej IPN gromadzi, ewidencjonuje, przechowuje, opracowuje, zabezpiecza i udostępnia dokumenty na temat zbrodni dokonanych w latach 1917–1990 oraz dokumenty ukazujące fakty i okoliczności dotyczące losów narodu polskiego w latach 1939–1990 (informujące o poniesionych ofiarach i wyrządzonych szkodach), a także wydaje na ich podstawie uwierzytelnione odpisy, wypisy, wyciągi i reprodukcje przechowywanych dokumentów.

W USA zarządzenie prezydenckie konstytuuje przepisy sankcjonujące świadome, umyślne albo wynikające z niezamierzonych zaniedbań naruszenia zasad postępowania z informacjami niejawnymi. Przewidywanymi konsekwencjami są: upomnienie, zawieszenie w obowiązkach bez wynagrodzenia, odwołanie ze stanowiska, wygaśnięcie upoważnienia do klasyfikacji, utrata lub odmowa dostępu do informacji niejawnych i inne sankcje, przewidziane w obowiązującym prawie i aktach normatywnych danej agencji.

---

[37] Urząd został powołany na mocy *The President Executive Order 12065* of 1978, *National Security Information* (*Zarządzenia Wykonawczego Prezydenta 12065* z 1978 r., *Informacje Bezpieczeństwa Narodowego*). Jego podporządkowanie oraz zadania realizowane przez ten podmiot były wielokrotnie modyfikowane. Zob. szerzej: https://www.archives.gov/isoo/about/history [dostęp: 12 II 2021].

[38] Zob. szerzej: *The President Executive Order 13526*…, section 5 (*Zarządzenie Wykonawcze Prezydenta 13526*…, ust. 5).

[39] Zob. szerzej: *Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu* (t.j.: DzU z 2021 r. poz. 177).

Dla porównania – regulacje mające charakter retorsji nie są wprost wyartykułowane w polskiej ustawie o ochronie informacji niejawnych, ewentualne konsekwencje dyscyplinarne wynikają z prawa pracy (ustaw pragmatycznych służb), karne natomiast – z zasad ogólnych. Ponadto utrata dostępu do tajemnic (poświadczenia bezpieczeństwa) może wynikać z przeprowadzonego kontrolnego postępowania sprawdzającego.

Drugim istotnym aktem prawnym kształtującym system bezpieczeństwa informacji niejawnych w USA jest *Zarządzenie Wykonawcze Prezydenta 12968* z 1995 r., *Dostęp do informacji niejawnych*[40]. Unormowano w nim tryb i zakres postępowania (*security background investigation*) realizowanego przez agencje państwowe wobec osób, którym mają być udostępnione informacje niejawne. W ogólnych zarysach jest to postępowanie odpowiadające postępowaniu sprawdzającemu, które jest przeprowadzane na podstawie polskiej ustawy o ochronie informacji niejawnych. Amerykański prawodawca wprowadza kilkanaście zastrzeżeń natury ogólnej. I tak, dostęp do informacji niejawnych:

1) co do zasady mogą mieć obywatele USA;
2) następuje po pozytywnym zakończeniu dochodzenia bezpieczeństwa (odpowiednio: postępowania sprawdzającego ustanowionego w rozdziale 5 polskiej ustawy o.i.n., którego ogólny zarys przedstawiono po omówieniu procedury obowiązującej w USA);
3) może uzyskać osoba, której osobista oraz zawodowa przeszłość wskazuje, że jest:
   – lojalna wobec USA i ma mocny charakter (rozumie się przez to, że nie jest ona uzależniona od używek, a także że jest asertywna),
   – wiarygodna, uczciwa i rzetelna,
   – dyskretna i roztropna,
   – niepodporządkowana innemu państwu i nieuzależniona od tajnego przymusu,
   – gotowa i zdolna przestrzegać przepisów regulujących korzystanie z informacji niejawnych, postępowanie z nimi i ich ochronę.

[40] *The President Executive Order 12968* of 1995, *Access to Classified Information*. Zarządzenie zostało znowelizowane w 2008 r. przez *The President Executive Order 13467*, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (*Zarządzenie Wykonawcze Prezydenta 13467, Reforma procedury związanej z oceną zdolności pracowników rządowych i uprawnień do uzyskania dostępu do informacji niejawnych bezpieczeństwa narodowego*), które ostatecznie zostało znowelizowane przez *The President Executive Order 13741* of 2016, *Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters* (*Zarządzenie Wykonawcze Prezydenta 13741* z 2016 r. *zmieniające Zarządzenie Wykonawcze 13467 w celu ustanowienia kompetencji i obowiązków Krajowego Biura Postępowań Sprawdzających i spraw z tym związanych*). Zob. https://www.govinfo.gov/content/pkg/DCPD-201600648/pdf/DCPD-201600648.pdf [dostęp: 4 VI 2021].

W myśl zarządzenia wszelkie wątpliwości co do wymienionych okoliczności należy rozstrzygać na korzyść bezpieczeństwa narodowego. Podobna norma generalna została zastosowana w art. 24 ust. 4 polskiej ustawy o.i.n.

Zgodnie z zarządzeniem 12968 uzyskanie poświadczenia bezpieczeństwa (*security clearance*) nie zależy od: rasy, koloru skóry, religii, płci, narodowości, niepełnosprawności lub orientacji seksualnej. Jeśli osoba sprawdzana korzysta z poradnictwa w zakresie zdrowia psychicznego, może to uzasadniać kolejne czynności mające na celu ustalenie, jak jej stan zdrowia wpływa na predyspozycje wymienione w pkt 3.

Interesującym rozwiązaniem jest możliwość zrezygnowania z prowadzenia kolejnego dochodzenia bezpieczeństwa w przypadku upływu ważności poświadczenia bezpieczeństwa. Pominięcie procedury sprawdzeniowej może nastąpić wówczas, gdy zostaną zachowane następujące warunki:

1) osoba sprawdzana będzie u tego samego pracodawcy zajmowała stanowisko z dostępem do tego samego rodzaju informacji niejawnych, jak te, które przetwarzała w okresie ważności ostatniego poświadczenia bezpieczeństwa,
2) brakuje informacji wskazujących na to, że zainteresowana osoba już nie spełnia kryteriów określonych w zarządzeniu 12968,
3) przedłużenie ważności następuje w odniesieniu do tej kategorii informacji niejawnych, do której dana osoba uzyskała dostęp na podstawie poświadczenia bezpieczeństwa wydanego w ostatnich pięciu latach,
4) ewentualna przerwa w zatrudnieniu danej osoby nie może być dłuższa niż dwa lata, a łączny okres od wydania ostatniego poświadczenia nie może przekraczać pięciu lat.

Polskie przepisy są mniej elastyczne, gdyż nie umożliwiają odstąpienia od przeprowadzenia kolejnego postępowania sprawdzającego[41].

W myśl zarządzenia 12968, jeżeli sytuacja osobista osoby uprawnionej albo inne okoliczności mające wpływ na bezpieczeństwo przekazywanych jej informacji uległy zmianie, uprawniony organ może przeprowadzić powtórne dochodzenie bezpieczeństwa. Jest to instytucja zbliżona do kontrolnego postępowania sprawdzającego

[41] Imperatyw wystąpienia z wnioskiem o przeprowadzenie kolejnego postępowania sprawdzającego na co najmniej sześć miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa posiadanego przez pracownika wynika z dyspozycji art. 32 ust. 1 ustawy o.i.n. Ważną przesłanką faktyczną uprawniającą kierownika do skorzystania z tego trybu jest zajmowanie przez osobę, mającą być sprawdzoną, stanowiska związanego z dostępem do informacji niejawnych o określonej klauzuli oraz zbliżający się koniec ważności poświadczenia bezpieczeństwa. Błędną interpretacją tego przepisu jest przyjęcie, że można go zastosować, kierując się jedynie przesłanką upływu terminu ważności posiadanego przez pracownika poświadczenia. Określony przez ustawodawcę termin sześciu miesięcy jest terminem instrukcyjnym, nie ma charakteru prekluzyjnego, złożenie wniosku wraz z ankietą z naruszeniem terminu nie powoduje bezskuteczności tej czynności. Wniosek powinien być złożony z wyprzedzeniem sześciomiesięcznym, aby organ podczas kolejnego postępowania sprawdzającego, prowadzonego w trybie poszerzonego lub zwykłego postępowania, zdążył rozstrzygnąć o utrzymaniu dotychczasowych uprawnień lub o ich zmianie przed końcem ważności poświadczenia, które osoba sprawdzana już posiada. Takie rozwiązanie zapewnia osobie sprawdzanej ciągłość pracy i pewność zatrudnienia, a także efektywne funkcjonowanie instytucji, tj. pracodawcy.

określonego w polskiej ustawie o.i.n. Ponadto prawodawca uprawnia właściwy organ wydający poświadczenia do bieżącej oceny osób, którym udzielono dostępu do tajemnic zgodnie z zasadami określonymi przez dyrektora Wywiadu Narodowego. Zasady, o których mowa w zarządzeniu, nie są publikowane. W przypadku otrzymania odmowy lub cofnięcia prawa dostępu do tajemnic USA osoba sprawdzana jest uprawniona do zapoznania się z dokumentami, na podstawie których podjęto negatywną decyzję. W wyjątkowych przypadkach kierownik agencji może odmówić udostępnienia materiałów z uwagi na naruszenie bezpieczeństwa narodowego USA. W takiej sytuacji organem odwoławczym od tego rodzaju odmowy jest komisja składająca się z co najmniej trzech pracowników (dwóch spoza pionu bezpieczeństwa) agencji, w której podjęto decyzję negatywną. Zarządzenie nie daje możliwości zaskarżenia decyzji komisji odwoławczej – jest ona ostateczna. Procedura odwoławcza i skargowa od negatywnych rozstrzygnięć organu uprawnionego do przyznania dostępu do tajemnic w RP jest diametralnie odmienna od stosowanej w USA. O zgodności z prawem odmowy wydania poświadczenia bezpieczeństwa, po wniesieniu skargi, rozstrzygają sądy administracyjne, w pierwszej instancji wojewódzki sąd administracyjny, w drugiej – Naczelny Sąd Administracyjny.

Prawo przyznawania dostępu do informacji niejawnych USA przysługujące agencjom państwowym jest określone w aktach powołujących te podmioty. Akta te są konsultowane z organami nadzorującymi programy bezpieczeństwa informacji niejawnych. Tego rodzaju agencje są zobowiązane do współpracy z ISOO oraz NDC, a przede wszystkim z dyrektorem Wywiadu Narodowego. Przykładem instytucji o szerokim spectrum oddziaływania na bezpieczeństwo tajemnic w aspekcie osobowym jest Agencja Bezpieczeństwa i Kontrwywiadu Obronnego (Defense Counterintelligence and Security Agency, DCSA)[42]. W październiku 2019 r. DCSA przejęła prowadzenie dochodzeń bezpieczeństwa od Krajowego Biura Postępowań Sprawdzających (National Background Investigations Bureau, NBIB), które utraciło autonomię i zostało podporządkowane DCSA. NBIB przeprowadzało postępowania wobec pracowników administracji rządowej i zapewniało realizację 95 proc. sprawdzeń dla agencji rządowych. Obecnie DCSA prowadzi postępowania nie tylko wobec urzędników lub kontrahentów wykonujących zlecenia rządowe, lecz także wobec żołnierzy i pracowników US Army. NBIB posiadało również specyficzną strukturę organizacyjną, ponieważ piony merytoryczne zajmujące się bezpieczeństwem w ponad 100 agencjach zostały po 2016 r. funkcjonalnie jej podporządkowane[43]. Jako wyspecjalizowany organ NBIB prowadziło wszystkie czynności w ramach dochodzenia bezpieczeństwa i gromadziło materiały (sprawdzenia osoby w bazach danych innych podmiotów, wywiady w miejscach zamieszkania i pracy itp.).

[42] Zob. szerzej: https://www.dcsa.mil/mc/pv/mbi/gicp/ [dostęp: 4 VI 2021].

[43] Zob. szerzej: https://obamawhitehouse.archives.gov/blog/2016/01/22/modernizing-strengthening-security-effectiveness-federal-background-investigations [dostęp: 4 VI 2021].

Po zakończeniu dochodzenia bezpieczeństwa przez DCSA akta są przesyłane do agencji, w której jest zatrudniona osoba sprawdzana. Tam szef danej agencji podejmuje decyzję dotyczącą możliwości udostępnienia tej osobie informacji niejawnych i określa poziom dostępu (najwyższą klauzulę tajemnic, do jakich ma mieć dostęp sprawdzony pracownik). Sprawdzeniu podlega przeszłość danej osoby, tzn. 10 ostatnich lat, jeżeli ubiega się ona o dostęp do informacji ściśle tajnych, albo 5 lat – jeśli do informacji tajnych. Z uwagi na to, że DCSA ma komórki współdziałające w agencjach, od których przyjmuje wnioski o przeprowadzenie postępowania oraz w strukturach podległych Departamentowi Obrony USA, może uzyskać łatwy dostęp do aktualnych i poprzednich miejsc pracy, edukacji i zamieszkania sprawdzanych osób, a także do innych – nawet zagranicznych – źródeł informacji oraz wszelkich krajowych baz danych. Dodatkowo agencja udostępniająca informacje niejawne może wystąpić do DCSA o objęcie danego pracownika programem ciągłego nadzoru (*Rap Back*). W ramach tego programu pracownik jest rejestrowany w bazach danych FBI i jeżeli złamie prawo albo zainteresuje się nim FBI, to dyrektor agencji zostaje poinformowany o potencjalnym zagrożeniu bezpieczeństwa informacji niejawnych przekazywanych temu pracownikowi.

Osoba sprawdzana, podobnie jak w Polsce, jest zobowiązana do wypełnienia kwestionariusza bezpieczeństwa[44]. Podanie w nim nieprawdziwych informacji może skutkować negatywnym rozstrzygnięciem postępowania. Dodatkowo osoba sprawdzana jest zobligowana do umożliwienia pobrania wzorów linii papilarnych. Karta daktyloskopijna lub odwzorowanie elektroniczne są przechowywane w bazach danych FBI oraz w bazach DCSA.

Zgodnie z zarządzeniem 12968 osoby mające dostęp do informacji niejawnych są zobowiązane do:

1) ochrony informacji niejawnych pozostających w ich dyspozycji przed nieuprawnionym ujawnieniem,
2) zgłaszania wszystkich kontaktów z osobami, włącznie z obcokrajowcami, które dążyły w jakikolwiek sposób do nieuprawnionego uzyskania dostępu do informacji niejawnych,
3) informowania urzędników odpowiedzialnych za bezpieczeństwo tajemnic o wszelkich naruszeniach przepisów bezpieczeństwa,
4) przestrzegania wszelkich innych wymogów bezpieczeństwa określonych w zarządzeniu i dyrektywach wykonawczych,
5) zgłaszania wątpliwości co do potrzeby dalszego dostępu do tajemnic przez innych pracowników z uwagi na zachowanie interesu bezpieczeństwa narodowego.

[44] *Questionnaire for National Security Positions*. Formularz nr 86 zatwierdzony przez United States Office of Management and Budget, OMB (nr autoryzacji: 3206 0005), https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf [dostęp: 4 VI 2021]. Dokument zawiera między innymi pouczenie o odpowiedzialności karnej z § 1001 za podanie fałszywych danych, tj. o czyn zagrożony karą pozbawienia wolności do lat 5 (USC, Title 18, Part I, Chapter 47 – *Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 47).

Przedmiotowe dyspozycje prawodawca zabezpieczył sankcjami, które mogą zostać zastosowane, w przypadku gdy pracownik agencji umyślnie przyznaje uprawnienia lub udostępnia informacje niejawne innej osobie, z naruszeniem zarządzenia albo aktów wykonawczych. Konsekwencjami powyższych naruszeń są: upomnienie, zawieszenie w obowiązkach bez wynagrodzenia, odwołanie ze stanowiska, a także inne środki przewidziane w prawie powszechnym i aktach normatywnych danej agencji.

Na podstawie *Kodeksu Stanów Zjednoczonych* organem powołanym do dokonywania interpretacji przepisów omawianego zarządzenia jest Asystent Prokuratora Generalnego USA ds. Bezpieczeństwa Narodowego[45].

W polskim porządku prawnym postępowanie służące weryfikacji osób, którym mają być udostępnione informacje niejawne, ustanowiono w rozdziale 5 ustawy o.i.n. zatytułowanym *Bezpieczeństwo osobowe*.

W okresie międzywojennym oraz w socjalistycznej Polsce organami upoważnionymi do udzielania dostępu do informacji stanowiących tajemnicę państwową byli kierownicy jednostek organizacyjnych w odniesieniu do podległych pracowników. Służby specjalne wyłącznie opiniowały daną osobę na wniosek kierowników jednostek, z tym zastrzeżeniem, że negatywna opinia zobowiązywała wnioskodawcę do odmowy nadania uprawnień. Warto dodać, że upoważnienia wydawane przez kierowników jednostek nie były decyzjami administracyjnymi i w związku z tym nie były wiążące dla innych podmiotów, a ponadto nie podlegały kontroli instancyjnej lub sądowej. Zmiana miejsca zatrudnienia powodowała konieczność powtórnego sprawdzenia danej osoby i wydania nowego upoważnienia albo odmowy, w zależności od opinii służb bezpieczeństwa państwa. Wprowadzenie ustawą o ochronie informacji niejawnych demokratycznych i określonych jawnymi przepisami procedur spowodowało przyznanie uprawnionym służbom i pełnomocnikom do spraw ochrony informacji niejawnych prawa do wydawania poświadczeń bezpieczeństwa, których termin ważności jest uzależniony od poziomu klauzuli informacji dostępnych na ich podstawie[46]. Negatywne rozstrzygnięcia są podejmowane w postaci decyzji administracyjnych z zachowaniem wszelkich konsekwencji prawnych, tj. możliwości wniesienia odwołania do organu II stopnia i ewentualnie skargi do sądów administracyjnych.

---

[45] Zob. szerzej: *Code of Federal Regulations*, Title 18, Chapter I, Part 17, Subpart A, Section 17.13 (*Kodeks przepisów federalnych*, tytuł 18, rozdział I, część 17, podczęść A, sekcja 17.13). Przepisy wydawane przez administrację federalną, tzn. rządową (*Federal Regulations issued by federal administrative agencies*), są skodyfikowane w akcie o nazwie *Code of Federal Regulations* (CFR). Kodeks składa się zazwyczaj z 50 tytułów (zależnie od roku wydania) w znacznej części pokrywających się z zakresem regulowanym przez ustawy federalne skodyfikowane w USC. Jedyną różnicą jest to, że CFR obejmuje wyłącznie przepisy wydawane przez władzę wykonawczą i jest publikowany w edycji rocznej. Zob. https://www.govinfo.gov/app/collection/cfr [dostęp: 4 VI 2021].

[46] Termin ważności poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji ściśle tajnych wynosi 5 lat, tajnych 7 lat i poufnych 10 lat.

Dostęp do informacji poufnych następuje po pozytywnie zakończonym zwykłym postępowaniu sprawdzającym. Do prowadzenia tego rodzaju postępowań ustawodawca upoważnił pełnomocników jednostek organizacyjnych ds. ochrony informacji niejawnych. Z kolei poszerzone postępowania sprawdzające stanowią podstawę do rozstrzygania o dostępie do informacji tajnych i ściśle tajnych. Podmiotami uprawnionymi do ich realizacji są służby państwowe, przede wszystkim ABW i SKW, a dodatkowo podmioty wyszczególnione enumeratywnie w ustawie[47].

Kontrolne postępowania sprawdzające w odniesieniu do prawomocnie zakończonych zwykłych postępowań sprawdzających są prowadzone przez pełnomocników ochrony właściwych ze względu na miejsce zatrudnienia osoby sprawdzanej. W przypadkach uzasadnionych względami bezpieczeństwa państwa mogą być również prowadzone przez ABW albo SKW (art. 33 ust. 3 ustawy o.i.n.). Kontrolne postępowania w odniesieniu do poszerzonych postępowań sprawdzających są realizowane wyłącznie przez ABW albo SKW (wg właściwości rzeczowej), a także przez służby wymienione w art. 23 ust. 5 w stosunku do postępowań przeprowadzonych przez te służby. Postępowania sprawdzające, na podstawie których strona uzyskuje dostęp do informacji niejawnych organizacji międzynarodowych, mogą prowadzić tylko ABW lub SKW w trybie poszerzonego lub tzw. skróconego postępowania sprawdzającego[48]. Mianem „kolejne postępowanie sprawdzające" ustawodawca określa postępowanie prowadzone wobec osoby już posiadającej poświadczenie, którego termin ważności dobiega końca. W celu zapewnienia ciągłości uprawnień prawodawca wydłużył okres jego prowadzenia z trzech do sześciu miesięcy i nakazał złożyć do właściwego organu ankietę i wniosek z wyprzedzeniem sześciu miesięcy. Kolejne postępowanie jest prowadzone w trybie zwykłego lub poszerzonego postępowania sprawdzającego w zależności od stanowiska, jakie zajmuje dana osoba w dniu złożenia wniosku.

Zgodnie z art. 21 ustawy o.i.n. dostęp do informacji niejawnych o klauzuli „poufne", „tajne" albo „ściśle tajne" może nastąpić po uzyskaniu przez określoną osobę odpowiedniego poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony

[47] W art. 23 ust 5 ustawy o.i.n prawodawca uprawnia: Agencję Wywiadu, Centralne Biuro Antykorupcyjne, Służbę Ochrony Państwa, Policję, Służbę Więzienną, Służbę Wywiadu Wojskowego, Straż Graniczną i Żandarmerię Wojskową do prowadzenia poszerzonych postępowań sprawdzających wobec osób zatrudnionych w tych organach i ubiegających się o zatrudnienie, a także wobec osób realizujących zlecenia na ich rzecz.

[48] Podstawą prawną do przeprowadzenia skróconego postępowania sprawdzającego jest art. 32 ust. 4 ustawy o.i.n. Określenie „skrócone postępowanie sprawdzające" pochodzi z terminologii resortowej, ponieważ w tym trybie nie dokonuje się weryfikacji danych zawartych w ankiecie bezpieczeństwa osobowego z tego powodu, że osoba sprawdzana nie ma obowiązku jej składania. Organem prowadzącym postępowanie jest wyłącznie ABW albo SKW, ponieważ tylko te organy są uprawnione do wydawania poświadczeń bezpieczeństwa organizacji międzynarodowych. Aby skorzystać z tego trybu, osoba sprawdzana musi mieć ważne poświadczenie bezpieczeństwa do tajemnic RP, które było wydane przez ABW, SKW, Agencję Wywiadu lub Służbę Wywiadu Wojskowego, na których podstawie jest dopuszczalne ograniczenie czynności sprawdzających i wydanie poświadczenia organizacji międzynarodowej z terminem ważności takim samym, jaki określono w poświadczeniu krajowym.

informacji niejawnych[49]. Wydanie poświadczenia jest możliwe wyłącznie po przeprowadzeniu wobec określonej osoby postępowania sprawdzającego zakończonego pozytywnym wynikiem. Od tej generalnej zasady istnieją odstępstwa. Ustawa w art. 34 ust. 5, 6 oraz 9 upoważnia osoby piastujące określone stanowiska państwowe do wyrażania zgody na jednokrotny lub tymczasowy dostęp do tajemnicy osobom, które nie mają poświadczenia bezpieczeństwa. Ponadto prawodawca w art. 34 ust. 10–13 wymienił podmioty, które są zwolnione od obowiązku posiadania poświadczenia lub ten obowiązek jest ograniczony do określonych typów poświadczeń.

W kontekście bezpieczeństwa państwa oraz konstytucyjnych praw obywatelskich warto odpowiedzieć na pytanie, czym jest postępowanie sprawdzające i według jakiej procedury jest ono prowadzone w demokratycznym państwie. Na podstawie kompetencji organów prowadzących, a także praw i obowiązków osoby sprawdzanej, można stwierdzić, że wspomniane postępowanie jest ciągiem czynności urzędowych podejmowanych przez uprawniony podmiot w celu ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy[50]. Podejmowane czynności są uregulowane w ustawie, a także – w określonej części – są administracyjnym prawem procesowym[51]. Ustawodawca w art. 24 ust. 6 ustawy o.i.n. określa, że postępowanie sprawdzające powinno być zakończone przed upływem trzech miesięcy od otrzymania przez organ dokumentów nakazanych ustawą, tj. wniosku wraz z ankietą bezpieczeństwa osobowego (ABO) lub tylko ankiety w przypadku postępowań zwykłych. Z uwagi na celowy charakter postępowania oraz instrukcyjny termin prowadzenia jego tok winien mieć charakter ciągły, tzn. postępowanie powinno być prowadzone bez przerwy – od wszczęcia do rozstrzygnięcia decyzją administracyjną. Ze względu na precyzyjne określenie przebiegu postępowania w ustawie szczególnej jest ono postępowaniem autonomicznym, z pewnym zakresem stosowania elementów postępowania jurysdykcyjnego określonego Kodeksem

[49] Kierując się wyłącznie treścią art. 21, można błędnie sądzić, że osoba, która spełniła ustanowione w nim warunki, ma dostęp do każdej tajemnicy o określonej klauzuli, a także że jest to uprawnienie obejmujące wszystkie informacje chronione daną klauzulą. Należy jednak wskazać, że ustawodawca w art. 4 ustawy o.i.n. ustanowił normę generalną w zakresie dostępu osób do informacji niejawnych ograniczającą pozornie uniwersalny charakter tego uprawnienia. Wprowadził zasadę wiedzy niezbędnej, która polega na udostępnianiu osobie uprawnionej tylko takich informacji, które są jej niezbędne do wykonywania pracy (służby) na zajmowanym stanowisku albo realizacji czynności zleconych (zasada była już stosowana w okresie II RP).

[50] W art. 2 pkt 2 ustawy o.i.n. zawarto definicję legalną: „(…) rękojmią zachowania tajemnicy jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego".

[51] Zgodnie z art. 3 ustawy o.i.n.: „Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nieuregulowanym w ustawie, mają zastosowanie przepisy: art. 6–8, art. 12, art. 14–16, art. 24 § 1 pkt 1–6 i § 2–4, art. 26 § 1, art. 28, art. 29, art. 30 § 1–3, art. 35 § 1, art. 39, art. 41–47, art. 50, art. 55, art. 57–60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 65, art. 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 103, art. 104, art. 105 § 2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125 § 1, art. 156–158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego".

postępowania administracyjnego[52] oraz ustawą Prawo o postępowaniu przed sądami administracyjnymi[53] (dalej: ustawa p.p.s.a.) (w części rozpatrywania skarg na negatywne rozstrzygnięcia organów II stopnia). Można zatem stwierdzić, że postępowanie sprawdzające jest postępowaniem szczególnym w odniesieniu do ogólnego postępowania administracyjnego określonego w kpa. Trafną, chociaż lapidarną, definicję postępowania jurysdykcyjnego sformułował Adam Bochentyn, stwierdzając, że jest to postępowanie administracyjne rozumiane jako proces stosowania norm prawnych przez wydawanie decyzji administracyjnych[54].

Należy zaznaczyć, że tylko niektórzy kierownicy jednostek organizacyjnych są uprawnieni do wnioskowania lub zlecania przeprowadzenia postępowania sprawdzającego wobec podległych im pracowników. Ustawodawca w art. 1 ust. 2 wymienił podmioty władzy publicznej zobowiązane do stosowania jej przepisów oraz przykładowo je wyliczył. Pomimo zastosowania terminu „w szczególności", który wskazuje na otwarty charakter danego wykazu, w rzeczywistości przyjęty sposób określenia podmiotów związanych przepisami ustawy czyni ten katalog „zewnętrznie" zamkniętym. Decydują o tym przyjęte kryteria selekcji podmiotów, ustawę bowiem mogą stosować wyłącznie organy władzy publicznej oraz podmioty wskazane *expressis verbis* w jej treści. Postępowanie sprawdzające mogą również przeprowadzać jednostki niepubliczne spełniające szczególny warunek, zawarty w art. 1 ust. 2 pkt 6 ustawy o.i.n., lub takie instytucje, którym ustawodawca narzucił obowiązek stosowania tej ustawy, odsyłając do niej w innych aktach normatywnych[55]. Kierownicy jednostek, które nie kwalifikują się do wyżej wymienionych zbiorów, nie mają ani obowiązku, ani legitymacji do występowania o przeprowadzenie wobec pracowników postępowań sprawdzających (np. przedsiębiorcy niespełniający przesłanek określonych w art. 1 ust. 2 pkt 6 ustawy o.i.n.)[56].

Głównymi organami prowadzącymi poszerzone postępowania sprawdzające przed wydaniem poświadczenia bezpieczeństwa upoważniającego do dostępu do

---

[52] *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (t.j.: DzU z 2021 r. poz. 735).

[53] *Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi* (t.j.: DzU z 2019 r. poz. 2325, ze zm.).

[54] A. Bochentyn, *Dopuszczalność dowodu z opinii biegłego na okoliczność treści prawa krajowego i europejskiego w jurysdykcyjnym postępowaniu administracyjnym*, w: *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, t. 2, J. Sługocki (red.), Wrocław 2014, s. 359.

[55] Stosowanie odesłań do ustawy o.i.n. wynika z zakazu powtarzania tych samych regulacji w różnych aktach prawnych. Zob. § 4 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej"* (DzU z 2016 r. poz. 283). Bezpośrednie odesłanie zastosowano w 22 innych ustawach i 12 rozporządzeniach, a pośrednie w blisko 100 ustawach i kilkudziesięciu rozporządzeniach. Zob. szerzej: D. Chromicka, *Struktura regulacji ochrony informacji niejawnych*, w: *Jawność i jej ograniczenia*, t. 4: *Struktura tajemnic*, A. Gruszczyńska (red.), Warszawa 2016, s. 237 i nast.

[56] Por. J. Borowicz, *Przetwarzanie informacji niejawnych w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne" 2011, nr 7, s. 24.

informacji o klauzuli „tajne" i „ściśle tajne" są ABW i SKW. Ustawodawca kontynuuje przyjęty w poprzednich ustawach (z 1982 r. i 1999 r. dotyczących ochrony informacji) podział kompetencji rzeczowej między podmioty cywilne i wojskowe. W art. 10 ustawy o.i.n. uszczegóławia się, że SKW realizuje zadania w odniesieniu do jednostek organizacyjnych Ministerstwa Obrony Narodowej i instytucji podległych, a także żołnierzy służby czynnej wyznaczonych na stanowiska poza wyżej wymienionymi strukturami. Wobec pozostałych osób i jednostek, do których ustawa ma zastosowanie, właściwym organem jest ABW. Zgodnie z art. 23 ust. 5 wymienieni w tym przepisie pełnomocnicy szefów służb ds. ochrony informacji niejawnych są uprawnieni do prowadzenia poszerzonych postępowań sprawdzających, według trybu określonego dla ABW i SKW. Pełnomocnicy wszczynają dane postępowanie na polecenie ich bezpośrednich przełożonych, tj. szefów wskazanych służb lub kierowników strukturalnych jednostek organizacyjnych tych podmiotów. Warto zauważyć, że w związku z konstrukcją art. 5 § 2 pkt 3 i art. 1 pkt 2 kpa pełnomocników ochrony należy zaliczyć do organów administracji publicznej, ponieważ są uprawnieni do załatwiania spraw indywidualnych w drodze decyzji administracyjnej. W literaturze przedmiotu tego rodzaju podmioty są także określane jako „funkcjonalne organy administracji publicznej"[57].

Podmiot, który zakończył postępowanie sprawdzające z wynikiem pozytywnym, na podstawie art. 29 ustawy o.i.n. jest zobowiązany przekazać osobie sprawdzonej poświadczenie bezpieczeństwa. Doręczenie stronie decyzji o odmowie wydania poświadczenia bezpieczeństwa nakazuje się w art. 30 ust. 5. Natomiast w przypadku przeprowadzenia kontrolnego postępowania sprawdzającego, ze względu na ujawnienie nowych informacji, że osoba mająca poświadczenie bezpieczeństwa nie daje rękojmi zachowania tajemnicy, art. 33 ust. 8 ustawy o.i.n. stanowi podstawę doręczenia decyzji o cofnięciu poświadczenia bezpieczeństwa, która kończy to postępowanie.

Odwołanie do organu II stopnia może wnieść wyłącznie osoba, wobec której organ I stopnia zakończył postępowanie sprawdzające decyzją o cofnięciu poświadczenia bezpieczeństwa albo odmową jego wydania lub decyzją o umorzeniu postępowania sprawdzającego, a także decyzją o umorzeniu kontrolnego postępowania sprawdzającego. Jeżeli strona wnosi odwołanie na decyzję wydaną w I instancji przez ABW lub SKW, a także przez podmioty wymienione w art. 23 ust 5, kieruje je do Prezesa Rady Ministrów RP w terminie 14 dni od dnia jej otrzymania za pośrednictwem organu, który wydał zaskarżaną decyzję. Odwołanie nie wymaga uzasadnienia. Organ I stopnia jest zobowiązany przesłać odwołanie wraz z aktami postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym je otrzymał. Organ II stopnia powinien rozpatrzyć odwołanie nie później niż w ciągu trzech miesięcy. Wniesienie odwołania nie wstrzymuje wykonania decyzji.

[57] Zob. szerzej: W. Chróścielewski, J. Tarno, *Postępowanie administracyjne i postępowanie przed sądami administracyjnymi*, Warszawa 2018, s. 85 i nast.

Wnoszący odwołanie jest uprawniony, na podstawie art. 36 ust. 3 ustawy, do żądania zlecenia przez Prezesa Rady Ministrów przeprowadzenia dodatkowych czynności przez organ I stopnia w celu uzupełnienia dowodów i materiałów w poszerzonym postępowaniu sprawdzającym lub kontrolnym postępowaniu sprawdzającym. Przedmiotem wystąpienia mogą być specjalistyczne badania, o których mowa w art. 26 ust. 6 ustawy o.i.n. Przyznanie stronie inicjatywy dowodowej w postaci prawa do żądania zlecenia przez organ II stopnia przeprowadzenia dowodu jest odstępstwem od ogólnych zasad postępowania administracyjnego. Postępowanie dowodowe powinno bowiem nastąpić przed podjęciem ostatecznego rozstrzygnięcia o istocie sprawy, a więc w ramach postępowania prowadzonego przez organ I stopnia. Pozbawienie strony inicjatywy dowodowej w postępowaniu pierwszoinstancyjnym i przyznanie jej na etapie rozpatrzenia odwołania przez Prezesa RM jest rozwiązaniem, które trudno racjonalnie uzasadnić. Postulowana zmiana przepisów to odpowiednia recepcja tej regulacji do art. 26 ustawy o.i.n., który uszczegóławia zakres poszerzonego postępowania sprawdzającego. Uprawnienie strony do żądania przeprowadzenia określonych czynności w toku postępowania sprawdzającego przed jego rozstrzygnięciem upodmiotowiłoby osobę sprawdzaną, która na tym etapie jest raczej „biernym przedmiotem" rozpoznania przez organ.

Na decyzję organu II stopnia, jeżeli nie rozstrzyga on odwołania według żądania strony, osobie sprawdzanej przysługuje skarga do właściwego miejscowo wojewódzkiego sądu administracyjnego. Do postępowania przed sądem administracyjnym stosuje się odpowiednio przepisy ustawy p.p.s.a. z pewnymi ograniczeniami wynikającymi z art. 38 ustawy o.i.n. Ustawodawca w przywołanym przepisie ustala przebieg procesu w szczególnym trybie, ze względu na to, że skarga rozpoznawana jest przez sąd na posiedzeniu niejawnym, a więc istotnie ogranicza jawność procesu. Brak udziału publiczności, w tym prasy (opinii publicznej), w procesie skutkuje wyłączeniem społecznej kontroli sposobu rozpatrywania sprawy przez sąd. Przywołany przepis poważnie utrudnia stronie skorzystanie z prawa do obrony swojego interesu prawnego przez wniesienie skargi, ponieważ stanowi, że odpis sentencji wyroku wraz z uzasadnieniem zostają doręczone przez sąd tylko właściwemu organowi odwoławczemu. Skarżącemu oraz osobie uprawnionej do obsady stanowiska jest doręczany jedynie odpis wyroku. A zatem strona nie otrzymuje uzasadnienia wyroku. Na jakiej więc podstawie osoba sprawdzana (profesjonalny pełnomocnik) może skonstruować zarzuty uzasadniające skargę kasacyjną, jeżeli wyrok jest dla niej niekorzystny?

Niniejsze zagadnienie było przedmiotem skargi do Trybunału Konstytucyjnego, który w wyroku z 23 maja 2018 r. orzekł, że: *Art. 38 ust. 3 ustawy w zakresie, w jakim przewiduje doręczenie skarżącemu odpisu wyroku sądu administracyjnego bez tej części uzasadnienia, której utajnienie nie jest konieczne dla ochrony informacji niejawnych, jest niezgodny z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 78 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej*[58]. A zatem uzasadnienie wyroku, które nie zawiera informacji niejawnych, powinno być doręczone

[58] Wyrok Trybunału Konstytucyjnego z 23 maja 2018 r., sygn. SK 8/14, OTK ZU 34/A/2018.

stronie w całości. Jeżeli natomiast uzasadnienie zawiera informacje niejawne, wówczas sąd powinien wyłączyć treści stanowiące tajemnice i po modyfikacji przekazać uzasadnienie stronie.

Jeżeli wojewódzki sąd administracyjny orzekł na niekorzyść osoby sprawdzanej, gdy istnieją uzasadnione przesłanki wskazujące na obrazę prawa materialnego w wyniku jego błędnego zastosowania lub wykładni albo na naruszenie przepisów postępowania w stopniu mającym wpływ na wynik sprawy (art. 174 ustawy p.p.s.a.), przysługuje jej skarga kasacyjna albo zażalenie do Naczelnego Sądu Administracyjnego. Należy nadmienić, że zgodnie z art. 175 i art. 194 § 4 ustawy p.p.s.a. skarga kasacyjna na wyrok oraz zażalenie na postanowienie o odrzuceniu skargi kasacyjnej co do zasady powinny być sporządzone i podpisane przez adwokata lub radcę prawnego. Postępowanie przed Naczelnym Sądem Administracyjnym, podobnie jak przed wojewódzkimi sądami administracyjnymi, toczy się według procedury określonej przepisami ustawy p.p.s.a. z ograniczeniami wprowadzonymi w art. 38 ustawy o.i.n.

Wracając do rozważań związanych ze Stanami Zjednoczonymi, należy wskazać, że system bezpieczeństwa informacji niejawnych USA jest bardzo rozbudowany pod względem regulacji normatywnych. Tworzą go ustawy o resortowym charakterze. Za najważniejsze należy uznać następujące akty prawne: *Ustawę o szpiegostwie* z 1917 r.[59], *Ustawę o energetyce atomowej* z 1954 r.[60], *Ustawę o ochronie tożsamości wywiadowczych* z 1982 r.[61] oraz *Ustawę o informacjach infrastruktury krytycznej z 2002 r.*[62], ponieważ w USA nie ma jednej spójnej ustawy regulującej ochronę informacji niejawnych. Drugą grupą normodawczą są zarządzenia wykonawcze prezydenta USA, z których dwa zostały już omówione, jednak nie są to jedyne zarządzenia o szerokim zakresie regulacji. Tak samo istotne jest zarządzenie 13587 dotyczące zwiększenia bezpieczeństwa informacji niejawnych w sieciach informatycznych i ich redystrybucji[63]. W USA obowiązują

[59] *Espionage Act* of 1917, USC, Title 18, § 792 and next (*Ustawa o szpiegostwie* z 1917 r., *Kodeks Stanów Zjednoczonych*, tytuł 18, § 792 i nast.).

[60] *Atomic Energy Act* of 1954, USC, Title 42, § 1801 and next, Public Law 703 (*Ustawa o energetyce atomowej* z 1954 r., *Kodeks Stanów Zjednoczonych*, tytuł 42, § 1801 i nast.).

[61] *Intelligence Identities Protection Act* of 1982, USC, Title 50, § 401, Public Law 97 – 200 (*Ustawa o ochronie tożsamości wywiadowczych* z 1982 r., *Kodeks Stanów Zjednoczonych*, tytuł 50, § 401.) Ustawa dotyczy ochrony danych personalnych agentów lub niejawnych współpracowników Wspólnoty Wywiadów.

[62] *Critical Infrastructure Information Act* of 2002, USC, title 6, § 2135 (*Ustawa o informacjach infrastruktury krytycznej* z 2002 r., *Kodeks Stanów Zjednoczonych*, tytuł 6, § 2135). Ustawa kształtuje krajową politykę departamentów i agencji federalnych USA w celu identyfikacji infrastruktury krytycznej i najważniejszych zasobów w Stanach Zjednoczonych oraz ochrony ich przed atakami terrorystycznymi, a także zasady analizy i ochrony informacji dotyczących tej infrastruktury.

[63] *The President Executive Order 13587* of 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing nad Safeguarding of Classified Information* (*Zarządzenie Wykonawcze Prezydenta 13587* z 2011 r., *Reformy strukturalne w celu poprawy bezpieczeństwa niejawnych sieci internetowych oraz odpowiedzialnego udostępniania i zabezpieczenia informacji niejawnych*).

ponadto regulacje określające postępowanie z tajemnicami o branżowym charakterze. Przykładem mogą być niektóre przepisy *Kodeksu przepisów federalnych* USA dotyczące funkcjonowania banków[64].

Na podstawie umowy zawartej pomiędzy rządem RP a rządem USA dotyczącej środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej[65] strony zobowiązały się do wzajemnej ochrony informacji niejawnych wymienianych w ramach wojskowej współpracy między Ministerstwem Obrony Narodowej RP a Departamentem Obrony USA. Państwa określiły wzajemne przyporządkowanie stosowanych klauzul w celu zapewnienia adekwatnej ochrony wymienianym informacjom. W poniższym zestawieniu zaprezentowano klauzule stosowane przez oba państwa.

Klauzula stosowana w RP	Klauzula stosowana w USA
Ściśle tajne	Top secret
Tajne	Secret
Poufne	Confidential
Zastrzeżone	brak amerykańskiego odpowiednika, traktowane jak Confidential

Ważnym postanowieniem zarządzenia 13526 jest upoważnienie podmiotów, które nie mają uprawnień do zaliczania posiadanych informacji do tajemnic i nadawania im klauzul, do występowania w tej sprawie do właściwych merytorycznie (ze względu na charakter informacji) agencji państwowych. Taka regulacja nie ma odpowiednika w polskich przepisach prawnych.

Oprócz podmiotów rządowych również inne podmioty, które nie są uprawnione do stosowania przepisów właściwych w sprawie klasyfikowania i klauzulowania informacji, mogą wytworzyć informacje, które powinny podlegać ochronie ze względu np. na bezpieczeństwo państwa, a zatem powinny być utajnione. Dlatego zarządzenie 13526 zobowiązuje podmioty rządowe do podjęcia decyzji o klasyfikowaniu przekazanych im

[64] Zob. szerzej: *Code of Federal Regulations*, Title 12, Chapter X, Part 1070, Subpart B. Wymieniony akt w ust. 19 reguluje, jakie podmioty są właściwe w sprawach udzielania odpowiedzi na wnioski dotyczące przekazania informacji niejawnych. Z przywołanego paragrafu wynika, że podmiotem uprawnionym do dysponowania informacją jest wyłącznie ten organ, który nadał jej klauzulę, czyli tylko wytwórca jest właściwy do deklasyfikacji dokumentu. W przywołanym akcie uregulowano również inne aspekty związane z zabezpieczeniem tajemnic w administracji rządowej, między innymi fizyczne zabezpieczenie informacji niejawnych i ich przechowywanie, kontrolowanie przesyłanie do innych podmiotów i warunki, w jakich tego dokonywano.

[65] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej podpisana w Warszawie dnia 8 marca 2007 r.* (DzU z 2007 r. nr 224 poz. 1658). W odniesieniu do sfery cywilnej strony nie zawarły tego rodzaju umowy, dokumenty pochodzące ze wzajemnej wymiany są chronione w wyniku nadania im polskich klauzul na podstawie art. 5 ust. 5 oraz art. 7 ust. 1 pkt 3 ustawy o.i.n.

informacji w terminie 30 dni[66]. Jest to szczególnie ważne w przypadku zamkniętego katalogu podmiotów uprawnionych do klauzulowania informacji na podstawie przepisów prawa, co występuje również w Polsce. Dlatego należy postulować wprowadzenie podobnej instytucji do systemu prawnego RP.

Przepisy federalne kształtujące odpowiedzialność karną za przestępstwa przeciwko tajemnicom USA

Federalne przepisy prawa karnego materialnego USA zostały skodyfikowane w przywołanym wcześniej *Kodeksie Stanów Zjednoczonych*, tytuł 18 – *Crimes nad criminal procedure*, część I – *Crimes*. Ze względu na poruszaną tematykę istotną jednostką redakcyjną rozdziału 37 pt. *Szpiegostwo i cenzura* (*Espionage and censorship*) jest § 798[67]. W tym przepisie amerykański prawodawca penalizuje czyn ujawnienia informacji niejawnych (*disclosure of classified information*). Przed przystąpieniem do omówienia przepisów karnych warto zaznaczyć, że ustalenie zaistnienia przestępstwa w amerykańskim prawie karnym polega na potwierdzeniu wystąpienia jego sześciu

[66] *The President Executive Order 13526*…, Part I, article 1 section 3 letter e (*Zarządzenie Wykonawcze Prezydenta 13526*…, część 1, art.1 ust. 3 lit. e).

[67] USC, Title 18, Part I, Chapter 37, § 798: „(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information – (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes- Shall be fined under this title or imprisoned not more than ten years, or both" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(a) Kto świadomie i celowo komunikuje, dostarcza, przekazuje lub w inny sposób udostępnia osobie nieupoważnionej, lub publikuje, lub wykorzystuje w jakikolwiek sposób z naruszeniem bezpieczeństwa lub interesu Stanów Zjednoczonych, lub na rzecz jakiegokolwiek rządu obcego państwa ze szkodą dla Stanów Zjednoczonych jakiekolwiek informacje niejawne: (1) dotyczące charakteru, przygotowania lub stosowania jakiegokolwiek kodu, szyfru lub systemu kryptograficznego Stanów Zjednoczonych lub jakiegokolwiek rządu obcego państwa; lub (2) dotyczące projektu, konstrukcji, użytkowania, konserwacji lub naprawy jakichkolwiek urządzeń, przyrządów lub sprzętów, stosowanych lub przygotowanych lub planowanych do zastosowania przez Stany Zjednoczone lub jakikolwiek rząd obcego państwa do celów kryptograficznych lub rozpoznania komunikacyjnego; lub (3) dotyczące działalności Stanów Zjednoczonych lub jakiegokolwiek rządu obcego państwa z zakresu rozpoznania komunikacyjnego; lub (4) uzyskane przez procesy rozpoznania komunikacyjnego na podstawie wiadomości przekazywanych przez jakikolwiek rząd obcego państwa, wiedząc, że zostały one uzyskane w wyniku takich procesów; podlega karze grzywny zgodnie z niniejszym tytułem lub pozbawienia wolności na okres do dziesięciu lat, lub obu tym karom jednocześnie").

znamion. Podstawowym determinantem odpowiedzialności jest istnienie generalnej normy zakazu karnego, czyli prawa, którego złamanie w wyniku działania lub zaniechania jest zagrożone reakcją państwa w formie kary. W USA prawo nie zawsze jest prawem stanowionym w formie ustaw, ponieważ pod uwagę mogą być brane precedensy orzecznictwa sądowego. Kolejną przesłanką jest wina powiązana z umyślnością albo nieumyślnością oraz z zabronionym zachowaniem, co najkrócej można ująć zasadą koincydencji lub jej braku (podobnie jak w polskim kodeksie karnym – art. 1 § 3). Jak trafnie zauważa Roman Tokarczyk, rezultatem bezprawnego działania lub zaniechania musi być „zło samo w sobie" (łac. *malum in se*) w sensie krzywdy albo innej szkody wynikającej z naruszenia wartości chronionych przez prawo. Ostatnim znamieniem jest związek przyczynowo-skutkowy (*casual link*) nie tylko między winą a skutkiem, lecz także między zabronionym zachowaniem a złem[68].

Konstrukcja przywołanego § 798 USC pod względem redakcyjnym odbiega nieco od modelu przyjętego w technice legislacyjnej RP. W ustępie (a) amerykański ustawodawca ustanowił normę sankcjonowaną i sankcjonującą, natomiast w kolejnym – (b)[69] – zdefiniował siedem nieostrych pojęć użytych do zbudowania normy

[68] Zob. szerzej: R. Tokarczyk, *Prawo amerykańskie*, Warszawa 2011, s. 230 i nast.

[69] USC, Title 18, Part I, Chapter 37, § 798: „(b) As used in subsection (a) of this section – The term 'classified information' means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution; The terms 'code', 'cipher', and 'cryptographic system' include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications; The term 'foreign government' includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States; The term 'communication intelligence' means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients; The term 'unauthorized person' means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(b) Zgodnie z użyciem w ust. a) niniejszego paragrafu – termin »informacje niejawne« oznacza informacje, które w momencie naruszenia niniejszego paragrafu są ze względu na bezpieczeństwo narodowe konkretnie oznaczone przez dowolną agencję rządową Stanów Zjednoczonych do ograniczonego lub zastrzeżonego rozpowszechniania lub rozprowadzania; terminy »kod«, »szyfr« i »system kryptograficzny« obejmują swoim znaczeniem, oprócz swoich zwyczajowych znaczeń, wszelkie metody tajnego zapisu oraz wszelkie mechaniczne lub elektryczne urządzenia lub metody stosowane w celu maskowania lub ukrywania treści, doniosłości lub znaczenia wiadomości; termin »rząd obcego państwa« obejmuje swoim znaczeniem każdą osobę lub osoby działającą(-e) lub twierdzącą(-e), że działa(-ją) na rzecz lub w imieniu jakiegokolwiek odłamu, partii, departamentu, agencji, biura lub sił wojskowych obcego państwa lub na terytorium takiego państwa, lub na rzecz lub w imieniu jakiegokolwiek rządu lub jakiejkolwiek osoby lub osób, która/które twierdzi(-ą), że działa(-ją)

sankcjonowanej, co ułatwia jej interpretację oraz znacznie ogranicza blankietowość. Mimo zdefiniowania określonych pojęć, w ocenie autora niniejszego artykułu ich zrozumienie jest możliwe na podstawie szerszej wiedzy z danej problematyki. Ustęp (c)[70] omawianego paragrafu zawiera kontratyp, który polega na uwolnieniu od odpowiedzialności karnej osoby wyjawiającej legalnie posiadane informacje niejawne komisjom powołanym w Kongresie USA (Senat i Izba Reprezentantów). Przywołany przepis koresponduje z innymi ustawami i aktami prawnymi wydanymi przez prezydenta USA, np. *Ustawą o ochronie sygnalistów z 1989 r.*[71] Prawodawca ustanowił także podstawy bezpośredniego informowania Kongresu USA o przestępczym działaniu administracji rządowej, nawet jeśli przekazywane przez urzędników informacje są objęte tajemnicą. Wspomniane akty zapewniają ochronę „sygnalistów" przed negatywnymi konsekwencjami wynikającymi ze złożonego zawiadomienia o nieprawidłowościach ze strony ich służbowych przełożonych. Końcowa jednostka redakcyjna, tj. ustęp (d), dotyczy możliwości zastosowania środka karnego (w wyroku skazującym) w postaci orzeczenia przepadku mienia należącego do skazanego, z określeniem warunków jego konfiskaty na rzecz państwa[72]. W odniesieniu do wymiaru zagrożenia karą za popełnienie przedmiotowego

jako rząd na terytorium obcego państwa bez względu na to, czy taki rząd jest uznawany przez Stany Zjednoczone; termin »rozpoznanie komunikacyjne« oznacza wszystkie procedury i metody wykorzystywane do przechwytywania wiadomości i uzyskiwania informacji z takich wiadomości przez osoby inne niż zamierzeni odbiorcy; termin »osoba nieupoważniona« oznacza każdą osobę lub agencję, która nie jest upoważniona do otrzymywania kategorii informacji określonych w ust. (a) niniejszego paragrafu przez prezydenta lub przez szefa departamentu lub agencji rządu Stanów Zjednoczonych wyznaczonego przez prezydenta do podejmowania działań z zakresu rozpoznania komunikacyjnego na rzecz Stanów Zjednoczonych").

[70] Tamże, § 798: „(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof" („(c) Żadne z postanowień niniejszego paragrafu nie zabrania dostarczania informacji na zgodne z prawem żądanie jakiejkolwiek prawidłowo utworzonej komisji Senatu lub Izby Reprezentantów Stanów Zjednoczonych Ameryki lub wspólnej komisji obu tych izb").

[71] Zob. szerzej: *Whistleblower Protection Act* of 1989, USC, Title 5, § 1201 (*Ustawa o ochronie sygnalistów* z 1989 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 1201), https://uscode.house.gov/statutes/pl/101/12.pdf [dostęp: 4 VI 2021]; *Whistleblower Protection Enhancement Act* of 2012, USC, Title 5, § 7211 *(Ustawa o wzmocnieniu ochrony sygnalistów* z 2012 r., *Kodeks Stanów Zjednoczonych*, tytuł 5, § 7211; https://www.govinfo.gov/content/pkg/BILLS-112s743enr/pdf/BILLS-112s743enr.pdf [dostęp: 4 VI 2021]; *Presidential Policy Directive/PPD-19, Protecting Whistleblowers with Access to Classified Information* October 10, 2012 (*Dyrektywa Polityczna Prezydenta/PPD-19*, *Ochrona sygnalistów z dostępem do informacji niejawnych* z 10 października 2012 r.), https://fas.org/irp/offdocs/ppd/ppd-19.pdf [dostęp: 4 VI 2021].

[72] USC, Title 18, Part I, Chapter 37, § 798: „(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law – (A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and (B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część I, rozdział 37, § 798: „(d)(1) Skazany za naruszenie niniejszego paragrafu traci na rzecz Stanów Zjednoczonych, niezależnie od przepisów prawa stanowego – (A) wszelki majątek

przestępstwa amerykański ustawodawca w ust. (a) ustanowił karę grzywny albo karę pozbawienia wolności na okres do 10 lat, z tym że wymienione kary mogą być stosowane łącznie. Analizując zagrożenie karami przewidzianymi w art. 265 polskiej ustawy karnej, można zauważyć, że zaskakująco niskie jest zagrożenie najsurowszą karą, tj. bezwzględnym pozbawienia wolności. Jeżeli bowiem wziąć pod uwagę, że przestępczy czyn jednego człowieka może sprowadzić na państwo np. wyjątkowo poważną szkodę w dziedzinie obronności (może zagrozić niepodległości albo integralności terytorialnej) lub w bezpieczeństwie wewnętrznym, to zastosowanie chociażby górnego wymiaru kary pozbawienia wolności, tj. 5 lat (§ 1) lub 8 lat (§ 2), wydaje się zbyt łagodne.

Nasuwają się wątpliwości co do adekwatność kary do szkody wyrządzonej przestępstwem. Słusznie Ryszard Dębski sygnalizuje, że (…) *należy baczyć, aby pomiędzy zakresem normy sankcjonowanej a sankcją kryminalną, określoną w normie sankcjonującej została zachowana pewna relacja proporcji*[73]. Oznacza to, że wymiar i rodzaj kary powinny być dostosowane do społecznej szkodliwości czynu z uwzględnieniem określających ją kwantyfikatorów, szczególnie rozmiarów wyrządzonej lub grożącej szkody oraz wagi naruszonych obowiązków. Podobny pogląd na temat sprawiedliwościowej funkcji kary prezentuje Wojciech Zalewski: *Za proporcjonalizmem w karaniu przemawia wiele argumentów teoretycznych i praktycznych. Istotą kary była i jest odpłata. Jeśli dalej reakcję na przestępstwo opierać się będzie na karze, musi być to kara sprawiedliwa*[74]. Przedmiotowe rozważania są adekwatne w odniesieniu do dysproporcji zagrożenia karą wynikającą z § 1924 USC, tj. do 5 lat pozbawienia wolności łącznie z karą grzywny lub bez (§ 1924 omówiono poniżej) i zagrożenia karą przewidzianego w art. 266 kk, tj. do 3 lat pozbawienia wolności, w przypadku gdy sprawcą jest funkcjonariusz, i 2 lat wobec pozostałych sprawców.

Amerykański ustawodawca przez użycie w § 798 USC pojęcia „ktokolwiek" (*whoever*) określił podmiot przestępstwa jako powszechny. Strona podmiotowa polega na świadomym (*knowingly*) i umyślnym (*willfully*) działaniu w zamiarze bezpośrednim, polegającym na ujawnieniu lub wykorzystaniu tajemnicy[75]. Ogólnym dobrem chronionym przez § 798 USC jest interes USA, który jest konkretyzowany ochroną tajemnic o wskazanym w przepisie charakterze. Są to między innymi niejawne informacje dotyczące budowy, rozwoju i działania urządzeń kryptograficznych oraz funkcjonowania wywiadu teleinformatycznego i informacji uzyskanych w wyniku tej działalności.

---

stanowiący jakiekolwiek wpływy uzyskane przez tego skazanego bezpośrednio lub pośrednio w wyniku takiego naruszenia lub majątek uzyskany z takich wpływów; i (B) jakikolwiek składnik majątku takiego skazanego, który wykorzystano lub przeznaczono do wykorzystania, w jakikolwiek sposób lub w jakiejkolwiek części, w celu dokonania lub ułatwienia dokonania takiego naruszenia").

[73] R. Dębski, *O przepisach blankietowych w prawie karnym. Uwagi wprowadzające*, „Acta Universitatis Lodziensis. Folia Iuridica" 1991, nr 47, s. 27.

[74] W. Zalewski, *Przestępca „niepoprawny" – jako problem polityki kryminalnej*, Gdańsk 2010, s. 387.

[75] Zob. szerzej: A.M. Taber, *Information control: making secrets and keeping them safe*, „Arizona Law Review" 2015, nr 2, s. 599 i nast.

Naruszenie tajności tego rodzaju informacji (przedmiocie wykonawczym czynu) ma nastąpić przez aktywne lub bierne zachowanie się sprawcy, tj. przekazanie, dostarczanie albo przesłanie informacji niejawnej nieupoważnionej osobie, a także uczynienie takiej informacji dostępnej dla nieupoważnionej osoby w inny sposób. Strona przedmiotowa tego przestępstwa może również polegać na upublicznieniu albo wykorzystaniu niejawnej informacji w sposób szkodliwy dla bezpieczeństwa USA lub przysporzeniu korzyści obcemu rządowi, z jednoczesną szkodą dla USA.

Znamiona czasownikowe użyte do konstrukcji przepisu § 798 USC („przekazuje", „upublicznia", „wykorzystuje" itd.) w istocie skutkują ujawnieniem tajemnicy, a zatem są one tożsame ze znamieniem przestępstwa polegającego na ujawnieniu chronionych informacji, o którym mowa w art. 265 § 1 polskiego kodeksu karnego. W § 798 USC termin „wykorzystanie" ma jednak inny charakter niż w polskim kodeksie, jest ono kryminalizowane wyłącznie w przypadku, gdy jest szkodliwe dla USA[76]. Tak więc przysporzenie korzyści dysponentowi tajemnicy w wyniku wykorzystania informacji niejawnych (bez naruszenia interesu państwa) nie jest karalne. Umieszczenie w omawianym przepisie, w pkt 1–4, katalogu rodzajów informacji niejawnych poważnie zawęża zakres penalizacji i możliwość karnego ścigania sprawcy ujawnienia tajemnic, jeżeli nie są one związane rzeczowo ze wskazanymi w tym przepisie zagadnieniami (materialnie – nie są tajemnicami). Ze względu na niemal kazuistyczny charakter § 798 USC, a przede wszystkim na jego część definicyjną, nie jest przepisem niezupełnym, w przeciwieństwie do adekwatnych regulacji polskich. Na uwagę zasługuje przedmiot wykonawczy czynu zabronionego, amerykański ustawodawca bowiem nie wartościuje odpowiedzialności karnej w zależności od klauzuli ujawnionych informacji, stosuje natomiast termin ogólny – „informacje niejawne" (polski kodeks karny w art. 265 uzależnia wymiar kary od klauzuli ujawnionej informacji).

Szczególnym przepisem prawa karnego materialnego w odniesieniu do § 798 USC jest czyn zabroniony polegający na bezprawnym usuwaniu lub zatrzymaniu niejawnych dokumentów albo materiałów (*unauthorized removal and retention of classified documents or material*), który został stypizowany w § 1924 USC[77].

---

[76] J.K. Elsea, *The Protection of Classified Information: The legal Framework*, Washington 2017, s. 14.

[77] USC, Title 18, Part 1, Chapter 93 – *Public officers and employees*, § 1924: „(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than five years, or both" (*Kodeks Stanów Zjednoczonych*, tytuł 18, część 1, rozdział 93 – *Funkcjonariusze i pracownicy publiczni*, § 1924: „(a) Kto, będąc funkcjonariuszem, pracownikiem, wykonawcą lub konsultantem Stanów Zjednoczonych, i z mocy swojego urzędu, zatrudnienia, stanowiska lub umowy, mając dostęp do dokumentów lub materiałów zawierających informacje niejawne Stanów Zjednoczonych, świadomie wynosi takie dokumenty lub materiały bez upoważnienia z zamiarem zatrzymania takich dokumentów lub materiałów w niedozwolonym miejscu, podlega karze grzywny na mocy niniejszego tytułu lub pozbawienia wolności na okres do pięciu lat lub obu tym karom jednocześnie").

Podmiot tego przestępstwa jest określony rodzajowo, indywidualnie. Amerykański prawodawca ogranicza penalizację wyłącznie do osób związanych z rządem USA stosunkiem służby, pracy albo umową, w tym kooperacją handlową, które są podstawą legalnego dostępu do informacji niejawnych USA. Przez użycie pojęcia „świadomie" (*knowingly*) w opisie czynu ustawodawca wskazuje na umyślność sprawstwa. Dobrem chronionym przez omawiany przepis jest bezpieczeństwo informacji niejawnych USA. Przedmiot ochrony przejawia się przede wszystkim w dostępie do tajemnic osób uprawnionych oraz zabezpieczeniu tych tajemnic przed dostępem osób nieupoważnionych w trakcie przechowywania w warunkach sprzecznych z prawem.

Definicję pojęcia „informacje niejawne Stanów Zjednoczonych" zawarto w ustępie (c) omawianego paragrafu[78]. Prawodawca odwołuje się w niej do aktów wydanych przez władzę wykonawczą, które w interesie bezpieczeństwa narodowego USA były podstawą zakwalifikowania danych informacji jako niejawnych i wprowadziły zakaz ich ujawniania. Tak więc w części odnoszącej się do przedmiotu wykonawczego jest to przepis blankietowy, ponieważ w celu zdekodowania normy zakazu należy użyć definicji zawartych w innych aktach. Ten przepis odnosi się jedynie do informacji niejawnych mających formę dokumentów albo materiałów, wyłączone zatem z zakresu jego regulacji są informacje nieposiadające nośnika, tj. przekazywane ustnie albo gestami, co jest wynikiem warunkowania odpowiedzialności karnej nieautoryzowanym miejscem przechowywania tajemnic.

Strona przedmiotowa przestępstwa jest określona czynnością polegającą na bezprawnym usuwaniu informacji niejawnych albo na ich przechowywaniu w miejscu, które nie jest – zgodnie z prawem – do tego przeznaczone, np. w urządzeniu nieposiadającym certyfikatu bezpieczeństwa wydanego przez uprawniony organ państwowy. Inaczej mówiąc, polega na naruszeniu zasad regulujących fizyczne zabezpieczenia nośników tajemnicy. Zgodnie z ustępem (b) § 798 USC, podobnie jak w ustępie (c), ujawnienie informacji niejawnych wobec przedstawicieli Kongresu USA nie jest penalizowane.

Odrębnym aktem normującym wykorzystanie informacji niejawnych jest *Ustawa o postępowaniu z informacjami niejawnymi* z 1980 r.[79], w której został uregulowany

[78] Tamże, § 1924: „(c) In this section, the term 'classified information of the United States' means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security" (tamże, § 1924: „(c) W niniejszym paragrafie termin »informacje niejawne Stanów Zjednoczonych« oznacza informacje pochodzące od rządu Stanów Zjednoczonych, będące jego własnością lub przez niego posiadane, dotyczące obrony narodowej lub stosunków zagranicznych Stanów Zjednoczonych, które zostały określone zgodnie z prawem lub rozporządzeniem wykonawczym jako wymagające ochrony przed nieuprawnionym ujawnieniem w interesie bezpieczeństwa narodowego").

[79] Zob. szerzej: *Classified Information Procedures Act* of 1980, USC, Title 18, Appendix III (*Ustawa o postępowaniu z informacjami niejawnymi* z 1980 r., *Kodeks Stanów Zjednoczonych*, tytuł 18, załącznik III), https://uscode.house.gov/browse/prelim@title18/title18a/node16&edition=prelim [dostęp: 4 VI 2021].

sposób postępowania z informacjami niejawnymi znajdującymi się w materiałach postępowań karnych. W paragrafie pierwszym informacje niejawne zostały zdefiniowane jako wszelkie informacje albo materiały, które zostały zakwalifikowane przez rząd USA do kategorii „niejawne". Podstawą tej kwalifikacji są: zarządzenia wykonawcze (w literaturze występują często jako dekrety prezydenta USA), ustawy federalne oraz wewnętrzne akty normatywne administracji rządowej. Zgodnie z ustawą zaliczenia informacji do tajemnic dokonuje się w celu wymuszenia ich ochrony przed nieuprawnionym ujawnieniem w związku z bezpieczeństwem narodowym albo danymi zastrzeżonymi na mocy rozdziału 11 *Ustawy o energetyce atomowej* z 1954 r.

Na marginesie niniejszych rozważań warto dodać, że ważną inicjatywą zmieniającą przepisy prawa materialnego jest projekt nowelizacji federalnych przepisów karnych. Zmiana ma polegać na zwolnieniu oskarżyciela publicznego z obowiązku dowodzenia przed sądem zamiaru wyrządzenia szkody interesom USA przez oskarżonego urzędnika, który utracił informację niejawną w wyniku rażącego zaniedbania albo celowego bezprawnego jej przechowywania[80].

Podsumowanie

Wielopłaszczyznowość struktury systemu ochrony informacji niejawnych w Stanach Zjednoczonych, wielość aktów i brak unifikacji pojęć, jak chociażby zaprezentowane definicje „*classified information*" w rozumieniu § 798 oraz § 1924 USC, powodują zawiłość regulacji prawnych. Powyższe może stwarzać niepewność co do przesłanek złamania norm zakazów karnych albo administracyjnych, skutkujące odpowiedzialnością karną albo administracyjną dla ich adresatów. Odmienność modelu systemu prawnego USA i RP może wywołać u polskich odbiorców błędne przekonanie o wadliwej strukturze regulacji prawnych USA. Warto jednak zaznaczyć, że problematyka ochrony informacji niejawnych naszego partnera jest określona prawem stanowionym, jednak praktyka stosowania tych przepisów i kultura prawna kształtuje się w USA również przez stosowanie prawa precedensowego. Skuteczne wykorzystanie gwarancji procesowych przysługujących potencjalnemu sprawcy przestępstwa w dużej mierze jest determinowane łatwością dostępu do usług profesjonalnych prawników wykonujących zawód bez spełniania uciążliwych wymogów formalnych i korporacyjnych, z którymi mamy do czynienia w Polsce.

Ważnym postulatem *de lege ferenda* jest wprowadzenie do polskiego prawa karnego – przy uwzględnieniu adekwatnych regulacji prawnych USA – kontratypu, który uwalniałby od odpowiedzialności karnej depozytariuszy tajemnic przekazujących

[80] Zob. szerzej: projekt ustawy *Classified Information Protection Act* of 2016 nr H.R. 6034 –14th, złożony do Kongresu USA 14 IX 2016 r., skierowany do Podkomisji ds. Przestępczości, Terroryzmu, Bezpieczeństwa Wewnętrznego i Dochodzeń 27 IX 2016 r. (nowelizacja pozostała w fazie projektu), https://www.congress.gov/bill/114th-congress/house-bill/6034/text [dostęp: 4 VI 2021].

organom ścigania informacje niejawne bez uzyskiwania zgody organów określonych prawem, w celu ścigania sprawców przestępstw.

Konkludując, zarówno polski, jak i amerykański system ochrony tajemnic publicznoprawnych jest unormowany aktami prawa administracyjnego oraz jest oparty na karnoprawnej ochronie informacji niejawnych. Przyjęty w obu krajach sposób weryfikacji osób przed udostępnieniem im informacji niejawnych wykazuje duże podobieństwa. Co do zasady sprawdzenia są wykonywane w obu krajach przez służby specjalne na podstawie wniosku zainteresowanej instytucji oraz osoby mającej zostać sprawdzoną. Ze względu na niejawny sposób dokonywania czynności, w tym sprawdzeń danej osoby, trudno odnieść się do ich zakresu. Wyraźne podobieństwa regulacji polskich i amerykańskich zachodzą w przypadku przepisów ustanawiających uniwersalne kryteria klasyfikacji informacji i obejmowanie ich ochroną państwa. W RP zrezygnowano z konstruowania wykazów informacji, którym należy nadać określoną klauzulę wraz z rozpoczęciem obowiązywania ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Istotną różnicą jest charakter wydawanego poświadczenia bezpieczeństwa oraz decyzji o odmowie jego wydania. W Polsce jest to szczególnego rodzaju decyzja administracyjna, od której przysługują środki zaskarżenia do sądów administracyjnych, w USA natomiast negatywne rozstrzygnięcie postępowania co do jego istoty nie ma takiego przymiotu. Brak unifikacji aktów normatywnych kształtujących system ochrony informacji niejawnych w USA oraz ich duża liczba nie pozwala na przeprowadzenie rzetelnych porównań z aktami polskimi w formie zwięzłego artykułu. Powyższe pozwala zidentyfikować pewne różnice w sposobie zapewnienia bezpieczeństwa informacjom niejawnym w RP i USA, a ponieważ nie są one krańcowo różne, przyjęta na wstępie hipoteza robocza nie została potwierdzona.

Bibliografia

Abel J., *Do you have to keep the Government's secrets? Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record*, „University of Pennsylwania Law Review" 2015, nr 4, s. 1037–1098.

Bochentyn A., *Dopuszczalność dowodu z opinii biegłego na okoliczność treści prawa krajowego i europejskiego w jurysdykcyjnym postępowaniu administracyjnym*, w: *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, t. 2, J. Sługocki (red.), Wrocław 2014, Presscom, s. 359–375.

Borowicz J., *Przetwarzanie informacji niejawnych w stosunkach pracy*, „Praca i Zabezpieczenie Społeczne" 2011, nr 7, s. 23–33.

Chromicka D., *Struktura regulacji ochrony informacji niejawnych*, w: *Jawność i jej ograniczenia*, t. 4: *Struktura tajemnic*, A. Gryszczyńska (red.), Warszawa 2016, C.H. Beck, s. 233–255.

Dębski R., *O przepisach blankietowych w prawie karnym. Uwagi wprowadzające*, „Acta Universitatis Lodziensis. Folia Iuridica" 1991, nr 47, s. 17–45.

Elsea J.K., *The Protection of Classified Information*: *The Legal Framework*, Washington 2017, Library of Congress, Congressional Research Service.

Kitrosser H., *Leak prosecutions and first amendment: New developments and a closer look at the feasibility of protecting leakers*, „William and Mary Law Review" 2015, nr 4, s. 1221–1277.

Leciak M., *Karnoprawna ochrona informacji niejawnych*, Toruń 2012, TNOiK – Towarzystwo Naukowe Organizacji i Kierowania „Dom Organizatora".

Lewandowski K., *Przestępstwa przeciwko ochronie informacji w świetle rozdziału XXXIII Kodeksu karnego, orzecznictwa doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 61–76.

Marek A., Konarska-Wrzosek V., *Prawo karne*, Warszawa 2016, C.H. Beck.

Jawność i jej ograniczenia, t. 11: *Standardy europejskie*, C. Mik (red.), rozdz. 8: *Analiza pojmowania i działania zasady jawności oraz jej ograniczeń z perspektywy prawa Stanów Zjednoczonych Ameryki*, Warszawa 2016, C.H. Beck, s. 251–280.

Pułło A., *Konstytucja Stanów Zjednoczonych Ameryki*, Warszawa 2002, Wydawnictwo Sejmowe.

Taber A.M., *Information control: making secrets nad keeping them safe*, „Arizona Law Review" 2015, nr 2, s. 581–607.

Zalewski W., *Przestępca „niepoprawny" – jako problem polityki kryminalnej*, Gdańsk 2010, ARCHE.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzmocnionej współpracy obronnej, podpisana w Warszawie dnia 15 sierpnia 2020 r. (DzU z 2020 r. poz. 2153).

Memorandum o porozumieniu między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzajemności w ramach zamówień obronnych, podpisane w Waszyngtonie dnia 27 sierpnia 2011 r. oraz w Warszawie dnia 8 września 2011 r. (DzU z 2012 r. poz. 975).

Umowa o zabezpieczeniu społecznym między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisana w Warszawie dnia 2 kwietnia 2008 r. (DzU z 2009 r. nr 46 poz. 374).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej z dnia 8 marca 2007 r. (DzU z 2007 r. nr 224 poz. 1658).

Protokół dodatkowy między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, podpisany w Brukseli dnia 12 stycznia 2004 r., do Traktatu o stosunkach handlowych i gospodarczych między Rzecząpospolitą Polską a Stanami Zjednoczonymi Ameryki, sporządzonego w Waszyngtonie dnia 21 marca 1990 r. (DzU z 2005 r. nr 3 poz. 14).

Ustawa z dnia 20 marca 2015 r. o ratyfikacji Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie (DzU z 2015 r. poz. 686).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j.: DzU z 2019 r. poz. 742).

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j.: DzU z 2019 r. poz. 2325, ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j.: DzU z 2020 r. poz. 2176).

Ustawa z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (t.j.: DzU z 2021 r. poz. 177).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j.: DzU z 2021 r. poz. 735).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (DzU z 2016 r. poz. 283).

Amerykańskie akty prawne

Constitution of the United States of America, House of Representatives, doc. No 110 – 50, 110th Congress.

Classified Information Protection Act of 2016, nr H.R. 6034 –14th, projekt ustawy.

Whistleblower Protection Enhancement Act of 2012, *United States Code*, Title 5, § 7211.

Intelligence Reform and Terrorism Prevention Act of 2004, *United States Code*, Title 50, § 401.

Critical Infrastructure Information Act of 2002, *United States Code*, Title 6, § 2135.

Whistleblower Protection Act of 1989, *United States Code*, Title 5, § 1201.

Intelligence Identities Protection Act of 1982, *United States Code*, Title 50, § 401.

Classified Information Procedures Act of 1980, *United States Code*, Title 18, Appendix III.

Freedom of Information Act of 1966, *United States Code*, Title 5, § 552.

Atomic Energy Act of 1954, *United States Code*, Title 42, § 1801.

Espionage Act of 1917, *United States Code*, Title 18, § 792.

Code of Federal Regulations, Title 18, Chapter I, Part 17, Subpart A, Section 17.13.

Code of Federal Regulations, Title 12, Chapter X, Part 1070, Subpart B, Section 1070, 1301.

United States Code, Title 18, Part I, Chapter 37, § 798.

United States Code, Title 18, Part 1, Chapter 93.

United States Code, Title 18, Part I, § 1924.

Zarządzenia wykonawcze prezydenta USA

The President Executive Order 13741 of 2016, *Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters*.

Presidential Policy Directive/PPD-19, *Protecting Whistleblowers with Access to Classified Information*, October 10, 2012.

The President Executive Order 13587 of 2011, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing nad Safeguarding of Classified Information*.

The President Executive Order 13526 of 2009, *Classified National Security Information*.

The President Executive Order 13470 of 2008, *United States Intelligence Activities*.

The President Executive Order 13467 of 2008, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*.

The President Executive Order 12968 of 1995, *Access to Classified Information*.

The President Executive Order 12958 of 1995, *Classified National Security Information*.

The President Executive Order 12333 of 1981, *United States Intelligence Activities*.

The President Executive Order 12065 of 1978, *National Security Information*.

Rosyjskie akty prawne

Конституция Российской Федерации от 12 декабря 1993 г., принятая всенародным голосованием 12 декабря 1993 года, вступила в силу в день её официального опубликования в газете „Российская газета" от 25.12.1993 № 237.

Уголовное уложение от 1903 г., Собрание узаконений и распоряжений правительства от 16 Апреля 1903 г. номер 88.

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z 23 V 2018 r., sygn. SK 8/14.

Wyrok Trybunału Konstytucyjnego z 15 X 2009 r., sygn. akt K 26/08.

Wyrok Naczelnego Sądu Administracyjnego z 6 VII 2017 r., sygn. akt. I OSK 932/16.

Wyrok Sądu Najwyższego USA w sprawie Hustler Magazine v. Falwell, 485 U.S. 46, 02.24.1988.

Abstrakt

W artykule omówiono regulacje administracyjne związane z organizacją systemu ochrony informacji niejawnych, a także przedstawiono przepisy karne dotyczące ujawniania informacji niejawnych obowiązujące w USA wraz z ich interpretacją. Omówiono również przepisy administracyjne regulujące procedurę realizacji postępowań sprawdzających wobec urzędników administracji publicznej w celu wydania poświadczenia bezpieczeństwa umożliwiającego dostęp do informacji niejawnych. Ponadto wskazano przesłanki klasyfikacji informacji i obejmowania ich ochroną adekwatnej klauzuli niejawności. Na podstawie analizy przepisów USA między innymi sformułowano wniosek, że polskie ustawodawstwo nie obejmuje kontratypu, który uwalniałby od odpowiedzialności karnej depozytariuszy tajemnic przekazujących informacje niejawne (bez uzyskiwania zgody określonych prawem organów) w celu ścigania sprawców przestępstw. Powyższe może być podstawą legislacyjnego postulatu *de lege ferenda*, przy uwzględnieniu adekwatnych regulacji prawnych USA.

Należy zaznaczyć, że artykuł nie wyczerpuje poruszanego tematu, a jedynie wskazuje wybrane zagadnienia ochrony informacji niejawnych USA. Może to zostać wykorzystane do przeprowadzenia w przyszłości pogłębionych badań komparatystycznych dotyczących przedmiotowego zagadnienia.

Słowa kluczowe: kodeks karny, ujawnienie tajemnicy, informacje niejawne, postępowanie sprawdzające, poświadczenie bezpieczeństwa, kontrwywiad.

Protection of classified information in the USA. Selected penal and administrative regulations

Abstract

The article discusses the administrative regulations regarding the classified information protection system in the USA. Moreover, it presents the effective penal code provisions directed against the disclosure of classified information in the USA and their interpretations. What is more, the paper presents the administrative provisions regulating the procedure for carrying out security background investigation of public administration officials in order to issue a security clearance which grants them access to classified information. Further, the reasons for the classification of information and its protection with an adequate classification clause are explained. On the basis of the analysis of US regulations, a conclusion is drawn that Polish legislation does not include a justification for depositaries of secrets who disclose classified information (without obtaining the affirmation from the authorities specified by law) to prosecute the perpetrators of crimes. This could be the basis to formulate postulates *de lege ferenda*. It should be noted that the article does not exhaust the topic, but only indicates selected issues of the protection system of classified information in the USA. Initiated study can be used to carry out in-depth comparative research in this field in the future.

Keywords: penal code, disclosure, classified information, verifying screening, security background investigation, security clearance, counterintelligence.

PAWEŁ GACEK
ORCID: 0000-0001-6365-3146

DOI: 10.4467/20801335PBW.21.026.14303

Wszczęcie postępowania karnego o przestępstwo umyślne ścigane z oskarżenia publicznego jako przesłanka zawieszenia funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu w czynnościach służbowych

Bezpieczeństwo państwa i jego obywateli jest zagadnieniem na tyle istotnym, że zdeterminowało ustawodawcę do utworzenia szczególnych służb mających na celu ochronę tego dobra prawnego[1]. O ile zapewnienie bezpieczeństwa i porządku publicznego zostało scedowane na Policję[2], o tyle zapewnienie i utrzymanie bezpieczeństwa państwa zostało powierzone służbom specjalnym[3], m.in. Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Jak wynika wprost z art. 1 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[4] (dalej: u.a.b.w.a.w.), Agencja Bezpieczeństwa Wewnętrznego jest formacją właściwą w sprawach bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, Agencja Wywiadu natomiast, zgodnie z art. 2 u.a.b.w.a.w., jest właściwa w sprawach ochrony bezpieczeństwa zewnętrznego państwa. Realizowanie zastrzeżonych dla tych formacji istotnych zadań wymaga zapewnienia odpowiednich wykonawców – funkcjonariuszy.

---

1 B. Opaliński, *Przedmowa do rozdziału 1*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el.

2 Zgodnie z art. 1 ust. 1 *Ustawy z dnia 6 kwietnia 1990 r. o Policji* (t.j.: DzU z 2021 r. poz. 1882) Policja jest umundurowaną i uzbrojoną formacją służącą społeczeństwu i przeznaczoną do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego.

3 Zgodnie z art. 11 u.a.b.w.a.w. są nimi: ABW, AW, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i Centralne Biuro Antykorupcyjne. „Określenie «służby specjalne» jest pojęciem normatywnym. Można mówić o nich wyłącznie w znaczeniu podmiotowym. Ustawodawca nie nadał natomiast temu pojęciu znaczenia przedmiotowego". Zob. M. Rogalski, *Komentarz do art. 2*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el., teza 5.

4 Tekst jednolity: DzU z 2020 r. poz. 27, ze zm.

Funkcjonariuszem ABW albo AW nie może być jednak każdy, ponieważ w u.a.b.w.a.w. przewidziano wiele wymogów formalnych dla kandydatów do służby w ABW albo w AW, których spełnienie jest niezbędne nie tylko do nawiązania stosunku służbowego, lecz także umożliwia nieprzerwane jego trwanie[5]. Te wymogi mają gwarantować zatrudnienie właściwych osób, które zasilą szeregi wymienionych organizacji. Innym istotnym elementem umożliwiającym właściwą realizację zadań i celów wyznaczonych przez ustawodawcę obu służbom jest węzeł prawny łączący osobę fizyczną z odpowiednią formacją. Jest nim stosunek służbowy, mający stricte administracyjnoprawny charakter[6]. Stosunek służbowy funkcjonariuszy ABW i AW (a także funkcjonariuszy innych służb zmilitaryzowanych) cechuje się wieloma elementami, które nie są w takim stopniu wyeksponowane w innego rodzaju stosunkach zatrudnienia. Oczywiście kształt poszczególnych stosunków służbowych funkcjonariuszy różnych formacji określają stosowane przepisy pragmatyk służbowych, które mogą przewidywać pewne odrębności. Można więc mówić o pewnym modelu stosunku służbowego jako konstrukcji usytuowanej wyłącznie w sferze prawa administracyjnego i mającej swoiste cechy wyróżniające ją spośród innych stosunków prawnych. Jest on szczególnego rodzaju więzią prawną, uprawnia bowiem funkcjonariusza do działania nie tylko w imieniu formacji, którą reprezentuje i której jest członkiem, lecz przede wszystkim w imieniu państwa. Stosunek służbowy nawiązany przez daną formację z funkcjonariuszem, a przede wszystkim prawa i obowiązki z niego wynikające, musi być zatem ukształtowany w ten sposób, aby stanowił sprawny instrument optymalnego (najbardziej pełnego) realizowania przez funkcjonariuszy zadań wytyczonych danej formacji przez ustawodawcę.

Charakterystycznymi cechami stosunku służbowego są nie tylko nierównorzędność stron tej więzi prawnej oraz prawo do jednostronnego i władczego kształtowania go stosownie do odpowiednich przepisów pragmatyki służbowej przez szefów ABW i AW, lecz także zwiększona dyspozycyjność funkcjonariusza (co do miejsca, czasu oraz

---

[5] Szerzej na ten temat zob. P. Gacek, *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56 i nast.

[6] Stosunek służbowy jest wspólny wszystkim służbom mundurowym (np. Policji, Straży Granicznej, Służbie Więziennej, Służbie Wywiadu Wojskowego, Służbie Kontrwywiadu Wojskowego, ABW i AW). Nie jest on stosunkiem pracy. Usytuowany jest wyłącznie w sferze prawa administracyjnego. Służby mundurowe ze względu na swoją specyfikę, tj. zadania, dla których zostały utworzone, nie tworzą jednak bezwzględnie jednolitej kategorii zawodowej w odniesieniu do zatrudnionych w nich funkcjonariuszy. W związku z tym poszczególne pragmatyki służbowe mogą ustanawiać pewne instytucje różnicujące status funkcjonariuszy tych służb. Szerzej na temat stosunku służbowego zob. P. Gacek, *Nawiązanie stosunku służbowego z funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Charakter prawny mianowania – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 98 i nast.; T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), seria: System Prawa Administracyjnego, Warszawa 2011; M. Wieczorek, *Charakter prawny stosunków służbowych funkcjonariuszy służb mundurowych*, Toruń 2017; także: wyrok Trybunału Konstytucyjnego z 19 X 2004 r., K 1/04, Legalis nr 65688; wyrok Naczelnego Sądu Administracyjnego z 3 X 2006 r., I OSK 210/06, Legalis nr 606379.

rodzaju wykonywanych czynności), podporządkowanie wobec przełożonych, a także zwiększona odpowiedzialność o charakterze dyscyplinarnym i karnym.

Wszystkie wskazane wyżej elementy mają stanowić swoistego rodzaju gwarancje dla społeczeństwa, że funkcjonariusze dopuszczeni do wykonywania zadań tak istotnych dla państwa i społeczeństwa – w tym zadań, których realizacja może pociągać za sobą ingerencję w prawa i wolności osób, szczególnie użycie środków przymusu bezpośredniego (również broni palnej) – będą poza wszelkimi podejrzeniami o zachowania niezgodne z rotą złożonego ślubowania, naruszające przepisy prawa powszechnie obowiązującego albo wewnętrznego, a także o zachowania wyczerpujące znamiona przewinienia dyscyplinarnego.

Funkcjonariusz ABW albo AW, jak to zostało już wcześniej zaznaczone, aby nieprzerwanie mógł kontynuować stosunek służbowy, musi spełniać wymogi, o których mowa w art. 44 u.a.b.w.a.w., w tym wykazywać się nieskazitelną postawą moralną, obywatelską i patriotyczną[7]. Jakiekolwiek wątpliwości w tym zakresie mogą być podstawą do wykluczenia takiej osoby z grona funkcjonariuszy ABW albo AW. Służy temu m.in. fakultatywna podstawa zwolnienia ze służby, gdy wymaga tego ważny interes służby (art. 60 ust. 2 pkt 5 u.a.b.w.a.w.)[8].

Możliwe jest jednak zaistnienie takich okoliczności, w których skorzystanie z instrumentu prawnego najdalej ingerującego w stosunek służbowy nie jest konieczne, ale zaistniałe okoliczności determinują natychmiastowe odsunięcie funkcjonariusza od zadań i czynności służbowych. Służy temu instytucja zawieszenia w czynnościach służbowych, uregulowana w art. 58 u.a.b.w.a.w. Jak słusznie zaznacza Przemysław Szustakiewicz: (…) *funkcjonariusz, którego postawa została podważona w trakcie służby, nie powinien do czasu wyjaśnienia wątpliwości wykonywać czynności służbowych, ponieważ nie sprzyja to wizerunkowi służby specjalnej w społeczeństwie i może wpływać na jakość wykonywanych przez nią zadań*[9]. Jak wynika wprost z art. 58 ust. 4 u.a.b.w.a.w., zawieszenie w czynnościach służbowych polega na odsunięciu funkcjonariusza od wykonywania obowiązków służbowych[10]. Przepisy pragmatyki służbowej przewidują przypadki, gdy zawieszenie w czynnościach służbowych jest obligatoryjne (art. 58 ust. 1 u.a.b.w.a.w.)[11], oraz takie, gdy zastosowanie tego instrumentu jest możliwe (art. 58 ust. 2

---

[7] P. Szustakiewicz, *Komentarz do art. 58*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el., teza 1.

[8] Funkcjonariusza ABW albo AW można zwolnić ze służby, w przypadku gdy wymaga tego ważny interes służby.

[9] P. Szustakiewicz, *Komentarz do art. 58*, teza 1…

[10] Jak wskazuje Przemysław Szustakiewicz, zawieszenie funkcjonariusza ABW albo AW w czynnościach służbowych nie oznacza jednak, że przestają go obowiązywać nakazy i zakazy związane ze służbą, ponieważ nadal pozostaje on czynnym funkcjonariuszem. Zob. P. Szustakiewicz, *Komentarz do art. 58*, teza 5…

[11] Zgodnie z tym przepisem funkcjonariusza zawiesza się rozkazem personalnym w czynnościach służbowych, na czas nie dłuższy niż 3 miesiące, w razie wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego.

u.a.b.w.a.w.)[12]. Ustalenie, czy zaistniała podstawa obligatoryjnego bądź fakultatywnego zawieszenia w czynnościach służbowych, wymaga uprzedniego zbadania, czy zmaterializowała się odpowiednia przesłanka ujęta w art. 58 ust. 1 albo ust. 2 u.a.b.w.a.w. Zawieszenie w czynnościach służbowych jest bowiem dopuszczalne wyłącznie w sytuacjach wymienionych enumeratywnie w pragmatyce służbowej. Należy również zaznaczyć, że są one wobec siebie niezależne i niekonkurencyjne. Zmaterializowanie się przesłanki wskazanej w art. 58 ust. 1 u.a.b.w.a.w. zobowiązuje do automatycznego zawieszenia funkcjonariusza w czynnościach służbowych, zaistnienie którejkolwiek z przesłanek wymienionych w art. 58 ust. 2 u.a.b.w.a.w. uprawnia natomiast do takiego zawieszenia, co oznacza jedynie możliwość zastosowania tej instytucji.

Omówienie wszystkich przesłanek, tj. obligatoryjnego i fakultatywnego zawieszenia w czynnościach służbowych, z uwagi na zakres i złożoność tej problematyki, nie jest możliwe w ramach tego opracowania. Stąd też dalsza jego część zostanie ograniczona wyłącznie do analizy przesłanki zawartej w art. 58 ust. 1 u.a.b.w.a.w. Istota zagadnienia sprowadza się zatem do ustalenia, w jakim momencie w czasie materializuje się przesłanka zawarta w art. 58 ust. 1 u.a.b.w.a.w., z tą bowiem chwilą podmiot, o którym mowa w art. 50 ust. 1 u.a.b.w.a.w., jest zobligowany do zastosowania tej instytucji. Obligatoryjne zawieszenie w czynnościach służbowych funkcjonariusza ABW albo AW nie było dotychczas w doktrynie opracowane w sposób kompleksowy. Ta instytucja ma kluczowe znaczenie, pozwala bowiem szefom ABW i AW na natychmiastową reakcję. Z jednej strony umożliwia ustalenie statusu służbowego funkcjonariusza, z drugiej zaś chroni interes służby (dobro służby), a w szerszym aspekcie – interes społeczny. Każde uprawnienie szefa ABW albo AW powinno być skutecznym instrumentem do osiągnięcia celu, jaki został przewidziany w pragmatyce służbowej dla danej instytucji. Musi służyć natychmiastowej reakcji na zaistniałe zdarzenie, ale też musi być efektywnym narzędziem, pozwalającym na adekwatną reakcję w stosunku do funkcjonariusza, którego dane zdarzenie dotyczy. Tak więc musi uwzględniać nie tylko wymieniony wcześniej interes społeczny, lecz także dobro funkcjonariusza, wobec którego jest podejmowana określona decyzja personalna.

Nie oznacza to, oczywiście, automatycznego równoważenia tych dóbr. Nie budzi wątpliwości, że w sytuacji konieczności obligatoryjnego zawieszenia funkcjonariusza ABW albo AW dochodzi do kolizji między tymi dobrami. Decyzja o obligatoryjnym zawieszeniu funkcjonariusza ABW albo AW świadczy o tym, któremu z tych dóbr należy dać prymat w świetle zaistniałych okoliczności i jakie są tego przyczyny. Obligatoryjność zawieszenia w czynnościach służbowych wymaga jednak uprzedniego wykazania zaistnienia przesłanki zawartej w art. 58 ust. 1 u.a.b.w.a.w., bo tylko jej spełnienie materializuje ten obowiązek. Dlatego na podmiocie, o którym mowa w art. 50 ust. 1

[12] Zgodnie z tym przepisem funkcjonariusza można zawiesić w czynnościach służbowych, na czas nie dłuższy niż 3 miesiące, w razie wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo nieumyślne ścigane z oskarżenia publicznego, postępowania w sprawie o wykroczenie oraz postępowania dyscyplinarnego, jeśli jest to celowe z uwagi na dobro postępowania lub dobro służby.

u.a.b.w.a.w., ciąży obowiązek dowiedzenia tej okoliczności. W praktyce jednak mogą rodzić się pewne wątpliwości co do tego, od jakiego momentu, na gruncie pragmatyki służbowej, można w sposób bezsprzeczny stwierdzić, że przeciwko funkcjonariuszowi ABW albo AW zostało wszczęte postępowanie karne w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Z tą chwilą bowiem aktywuje się obowiązek szefa ABW albo AW do zawieszenia takiego funkcjonariusza w czynnościach służbowych.

Z uwagi na powyższe dalsze rozważania zostaną skoncentrowane na przesłance z art. 58 ust. 1 u.a.b.w.a.w. – na użytym w nim sformułowaniu „wszczęcie postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego przeciwko funkcjonariuszowi ABW albo AW", gdyż dopiero od momentu zainicjowania takiego postępowania powstaje obowiązek szefa ABW albo AW do zastosowania instytucji zawieszenia w czynnościach służbowych. Wcześniejsze zawieszenie byłoby nie tylko niezasadne, lecz przede wszystkim niedopuszczalne i bezprawne, ze względu na cel, jaki ma zostać osiągnięty dzięki zastosowaniu tej instytucji. Tym celem jest wyznaczenie na osi czasowej punktu, od którego następuje wszczęcie (zainicjowanie) – w odpowiednim trybie – postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego przeciwko funkcjonariuszowi ABW albo AW (co świadczy o zaistnieniu przesłanki, o której mowa w art. 58 ust. 1 u.a.b.w.a.w.).

Przesłanka obligatoryjnego zawieszenia w czynnościach służbowych

Jak wynika wprost z art. 58 ust. 1 u.a.b.w.a.w., funkcjonariusza zawiesza się w czynnościach służbowych rozkazem personalnym[13] na czas nie dłuższy niż 3 miesiące, w razie wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Ten przepis przewiduje tylko ten jeden przypadek, którego zaistnienie obliguje do niezwłocznego zawieszenia funkcjonariusza w czynnościach służbowych. Jak słusznie zauważa Lech Gardocki, większość przestępstw to przestępstwa publicznoskargowe, co oznacza, że ich ściganiem zajmuje się oskarżyciel publiczny (prokurator) działający w imieniu państwa[14]. Przepisy karne[15] przewidują także ściganie przestępstwa z oskarżenia prywatnego (w trybie prywatnoskargowym), ale nie są to liczne przypadki. Z przepisu ustawy musi wówczas wynikać wprost, że ściganie określonego przestępstwa odbywa się w takim trybie[16]. W polskim porządku prawnym

[13] Stanowi o tym art. 50 ust. 3 u.a.b.w.a.w. Rozkaz personalny w sprawie zawieszenia w czynnościach służbowych jest decyzją administracyjną. Kwestie z tym związane przekraczają jednak ramy niniejszego opracowania.

[14] L. Gardocki, *Prawo karne*, Warszawa 1999, s. 58; F. Prusak, *Postępowanie karne*, Warszawa 2001, s. 70.

[15] Zawarte przede wszystkim w *Ustawie z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.), a także w innych ustawach zawierających przepisy karne.

[16] Na przykład: naruszenie czynności narządu ciała lub rozstrój zdrowia trwający nie dłużej niż 7 dni albo nieumyślne naruszenie czynności narządu ciała lub rozstrój zdrowia, o którym mowa

zasadą jest, że sprawy dotyczące przestępstw prowadzi się w trybie publicznoskargowym (z urzędu)[17]. Jeżeli jednak wymaga tego interes społeczny, prokurator wszczyna postępowanie albo wstępuje do już wszczętego postępowania w sprawie o przestępstwo ścigane z oskarżenia prywatnego (art. 60 § 1 kpk[18]). W takiej sytuacji postępowanie toczy się z urzędu i jest objęte skargą publiczną[19]. Oznacza to, że przestępstwem ściganym w trybie publicznoskargowym może być przestępstwo, które generalnie jest przestępstwem prywatnoskargowym, ale zostanie ono objęte przez oskarżyciela publicznego ściganiem z urzędu[20].

Nie dokonując pogłębionej analizy i nie przesądzając o tym, czy objęcie skargą publiczną przestępstwa prywatnoskargowego skutkuje tym, że staje się ono przestępstwem publicznoskargowym bądź jedynie przestępstwem prywatnoskargowym ściganym z oskarżenia publicznego, należy zwrócić uwagę na cel zawieszenia funkcjonariusza w czynnościach służbowych wskazany w pragmatyce służbowej. Jest nim zabezpieczenie interesu służby (w szerszym aspekcie – interesu społecznego). Zawieszenie w czynnościach służbowych polega na odsunięciu funkcjonariusza od wykonywania obowiązków służbowych (art. 58 ust. 4 u.a.b.w.a.w.) i nałożeniu na niego obowiązków określonych w art. 58 ust. 6 u.a.b.w.a.w., które są związane z odsunięciem go od tych obowiązków. Objęcie skargą publiczną przestępstwa prywatnoskargowego również ma swoje źródło w konieczności zabezpieczenia interesu społecznego, ponieważ obliguje oskarżyciela publicznego do wszczęcia postępowania lub wstąpienia do postępowania w sprawach o przestępstwa ścigane z oskarżenia prywatnego, jeżeli wymaga tego interes społeczny. Co do zasady ciężar gatunkowy przestępstw prywatnoskargowych jest mniejszy niż przestępstw ściganych z oskarżenia publicznego. Obligatoryjność objęcia ściganiem z urzędu przestępstw prywatnoskargowych, gdy wymaga tego interes społeczny, jest uzasadnione w sytuacjach, gdy z określonych powodów ich ciężar gatunkowy może być porównywalny z innymi przestępstwami publicznoskargowymi, tj. gdy są z określonych powodów na tyle społecznie niebezpieczne, że ich ściganie musi przejąć oskarżyciel publiczny. W tym kontekście, na gruncie pragmatyki służbowej (art. 58 ust. 1 u.a.b.w.a.w.), zasadne wydaje się zrównanie wszczęcia postępowania karnego o umyślne przestępstwo publicznoskargowe z umyślnym przestępstwem prywatnoskargowym, objętym ściganiem z urzędu na zasadzie art. 60 § 1 kpk

w art. 157 § 1 lub 2 kk – art. 157 § 4 kk; zniesławienie – art. 212 § 4 kk; zniewaga – art. 216 § 5 kk; naruszenie nietykalności cielesnej – art. 217 § 3 kk.

[17] Postanowienie Sądu Najwyższego – Izba Dyscyplinarna z 8 II 2019 r., I DO 18/18, Legalis nr 1872771.

[18] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: DzU z 2021 r. poz. 534, ze zm.).

[19] L. Gardocki, *Prawo karne…*, s. 58.

[20] „Po wydaniu przez prokuratora decyzji o wszczęciu postępowania o czyn ścigany z oskarżenia prywatnego toczy się ono z urzędu". Zob. S. Szołucha, *Komentarz do art. 60*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 3.

jako przesłanki uzasadniającej obligatoryjne zawieszenie funkcjonariusza ABW albo AW w czynnościach służbowych.

Z perspektywy zakresu przesłanki, o której mowa w art. 58 ust. 1 u.a.b.w.a.w., nie ma natomiast znaczenia, czy przedmiotem postępowania karnego jest czyn wypełniający znamiona przestępstwa powszechnego bądź przestępstwa skarbowego[21], czy ten czyn ma związek ze służbą pełnioną przez funkcjonariusza ABW albo AW, jego prawami lub obowiązkami, wykonywanymi zadaniami jako funkcjonariusza publicznego lub czynnościami służbowymi, a także z trybem, w jakim postępowanie karne jest prowadzone. Istotne jest to, aby było ono umyślnym przestępstwem publicznoskargowym. Wszczęcie postępowania w sprawie o ściganie niektórych przestępstw publicznoskargowych jest bowiem uzależnione od uprzedniego złożenia przez uprawniony podmiot wniosku o ściganie (tryb warunkowy), w przeciwieństwie do większości postępowań, które są inicjowane w sposób bezwarunkowy, tj. z urzędu, i niezależnie od woli innych podmiotów (nawet tych, których przestępstwo dotyczy).

Złożenie takiego wniosku jest jedynie warunkiem wszczęcia takiego postępowania karnego. Po złożeniu wniosku postępowanie karne toczy się tak samo jak inne postępowanie, którego przedmiotem jest przestępstwo publicznoskargowe[22]. Istotne jest również to, że przestępstwo publicznoskargowe musi być popełnione z winy umyślnej. Nie ma jednak znaczenia, czy sprawca działał w zamiarze bezpośrednim

---

[21] Należy oczywiście zaznaczyć, że art. 39 ust. 1 ustawy o Policji obliguje do zawieszenia funkcjonariusza Policji w czynnościach służbowych w razie wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo lub przestępstwo skarbowe, umyślne, ścigane z oskarżenia publicznego, ale wydaje się, że różnica w brzmieniu między wymienionym przepisem a art. 58 ust. 1 u.a.b.w.a.w. nie może stanowić podstawy do stwierdzenia, że wszczęcie postępowania karnego o umyślne przestępstwo skarbowe nie stanowi podstawy do obligatoryjnego zawieszenia funkcjonariusza ABW albo AW w czynnościach służbowych. Należy bowiem zwrócić uwagę przede wszystkim na cel obligatoryjnego zawieszenia w czynnościach służbowych. Rygorystyczne utożsamienie użytego w art. 58 ust. 1 u.a.b.w.a.w. pojęcia „przestępstwo" wyłącznie z przestępstwem powszechnym skutkowałoby tym, że wszczęcie postępowania karnego przeciwko funkcjonariuszowi ABW albo AW w sytuacji popełnienia przez nich umyślnego przestępstwa skarbowego nie stanowiłoby ani obligatoryjnej, ani fakultatywnej podstawy do zawieszenia w czynnościach służbowych. Tym samym wypaczony byłby sens przedmiotowej regulacji. Popełnienie przez funkcjonariusza ABW albo AW wykroczenia (ale nie wykroczenia skarbowego) mogłoby stanowić podstawę do (fakultatywnego) zawieszenia go w czynnościach służbowych, a popełnienie umyślnego przestępstwa skarbowego, które skutkowałoby albo mogło skutkować wielomilionowym uszczerbkiem finansowym Skarbu Państwa, nie mogłoby stanowić podstawy ani do obligatoryjnego, ani do fakultatywnego zawieszenia w czynnościach służbowych. Tak więc podstawą do fakultatywnego zawieszenia w czynnościach służbowych mogłoby być wyłącznie wszczęcie postępowania w sprawie o wykroczenie, ale nie o wykroczenie skarbowe. Należy również zaznaczyć, że ustawa o Policji w pierwotnym brzmieniu (DzU z 1990 r. nr 30 poz. 179, ze zm.) także odnosiła się do przestępstw, bez dodatkowych określeń. Treść art. 39 ust. 1 ustawy o Policji została zmieniona *Ustawą z dnia 29 października 2003 r. o zmianie ustawy o Policji* (DzU z 2003 r. nr 192 poz. 1873). *De lege ferenda*, aby wykluczyć możliwość przyjęcia wielości ocen, należałoby postulować dokonanie zmiany przepisu art. 58 ust. 1 u.a.b.w.a.w. na wzór art. 39 ust. 1 ustawy o Policji.

[22] L. Gardocki, *Prawo karne…*, s. 58 i nast.; F. Prusak, *Postępowanie karne…*, s. 71.

(*dolus directus*[23]) czy ewentualnym (*dolus eventualis*). Zasadą jest, że przestępstwo może być popełnione umyślnie. Nieumyślnie można je popełnić tylko wtedy, jeśli ustawa tak stanowi (art. 8 kk)[24]. Norma zawarta w przepisie art. 58 ust. 1 u.a.b.w.a.w. nie obliguje natomiast do zawieszenia funkcjonariusza ABW lub AW w czynnościach służbowych w przypadku wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo nieumyślne ścigane z oskarżenia publicznego albo z oskarżenia prywatnego (które nie zostało objęte skargą publiczną na podstawie art. 60 § 1 kpk), albo postępowania w sprawie o czyn wyczerpujący znamiona wykroczenia[25]. Analogicznie postępuje się w sytuacji przestępstw skarbowych. Zgodnie z art. 113 § 1 kks[26] w postępowaniu w sprawach o przestępstwa skarbowe stosuje się odpowiednio przepisy kpk, jeżeli przepisy kks nie stanowią inaczej[27]. Przestępstwo skarbowe można popełnić umyślnie bądź nieumyślnie, jeżeli kodeks tak stanowi (art. 4 § 1 kks)[28]. Podstawą obligatoryjnego zawieszenia w czynnościach służbowych może być wyłącznie wszczęcie postępowania w sprawie o umyślne przestępstwo skarbowe, nie może nim być natomiast wszczęcie postępowania przeciwko funkcjonariuszowi ABW albo AW o czyn wyczerpujący znamiona wykroczenia skarbowego.

Organ zobowiązany do zawieszenia funkcjonariusza ABW albo AW w czynnościach służbowych nie dokonuje samodzielnych ustaleń w zakresie kwalifikacji prawnej czynu będącego przedmiotem postępowania karnego, ale jest związany treścią decyzji

[23] Wszystkie zwroty obcojęzyczne użyte w artykule pochodzą z łaciny, dlatego Redakcja nie podaje za każdym razem tej informacji (przyp. red.).

[24] „O ile więc odpowiedzialność za przestępstwa umyślne jest regułą i nie wymaga wyraźnego ustawowego wskazania, o tyle odpowiedzialność karna za przestępstwa nieumyślne stanowi swoisty wyjątek, w tym sensie, że ponosi się odpowiedzialność karną za przestępstwa nieumyślne tylko wtedy, gdy ustawa tak stanowi. Jeżeli więc ustawodawca zamierza wprowadzić odpowiedzialność karną za występki nieumyślne, powinien to stwierdzić *expressis verbis* w tekście przepisu, wymieniając nieumyślność wśród ustawowych znamion czynu zabronionego". Zob. A. Grześkowiak, *Komentarz do art. 8 – Strona podmiotowa przestępstwa*, w: *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, Legalis/el., teza 1.

[25] Wszczęcie postępowania karnego przeciwko funkcjonariuszowi ABW albo AW o przestępstwo nieumyślne ścigane z oskarżenia publicznego, postępowania w sprawie o wykroczenie oraz postępowania dyscyplinarnego jest bowiem fakultatywną podstawą do zawieszenia go w czynnościach służbowych (art. 58 ust. 2 u.a.b.w.a.w.). Co ciekawe, zainicjowanie postępowania karnego o przestępstwo prywatnoskargowe, jeśli nie zostało ono objęte ściganiem publicznym, na zasadzie art. 60 § 1 kpk, nie stanowi (nawet fakultatywnej) podstawy do zawieszenia funkcjonariusza ABW albo AW w czynnościach służbowych.

[26] *Ustawa z dnia 10 września 1999 r. – Kodek karny skarbowy* (t.j.: DzU z 2021 r. poz. 408, ze zm.).

[27] W postępowaniu w sprawach o przestępstwa skarbowe kodeksu postępowania skarbowego nie stosuje się w zakresie dotyczącym pokrzywdzonego i mediacji. Nie stosuje się również art. 325f kpk.

[28] Czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, tj. chce go popełnić albo, przewidując możliwość jego popełnienia, na to się godzi (art. 4 § 2 kks). Czyn zabroniony popełniony jest nieumyślnie, jeżeli sprawca, nie mając zamiaru jego popełnienia, popełnia go jednak na skutek niezachowania ostrożności wymaganej w danych okolicznościach, mimo że możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć (art. 4 § 3 kks).

procesowych, które zapadły w procesie karnym. Wyłącznie na ich podstawie może dokonać stosownej oceny czynu zarzuconego funkcjonariuszowi, w kontekście zmaterializowania się przesłanki obligującej do zawieszenia w czynnościach służbowych[29]. Kwestionowanie tych decyzji, zwłaszcza w świetle materiału dowodowego zebranego w sprawie karnej, dokonanych tam ustaleń, kwalifikacji prawnej czynu przyjętej przez organ procesowy, byłoby nieuprawnionym wkroczeniem w kompetencje zastrzeżone dla organu prowadzącego postępowanie karne, tj. prokuratora lub nieprokuratorskiego organu prowadzącego postępowanie karne.

Funkcjonariusza ABW albo AW, zgodnie z art. 58 ust. 1 u.a.b.w.a.w., zawiesza się w czynnościach służbowych w przypadku wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Nie budzi zatem wątpliwości, że wymieniony przepis łączy obowiązek zastosowania tej instytucji ze zmianą stadium postępowania karnego z *in rem* w *ad personam*. W sytuacji gdy przedmiotem postępowania karnego jest przestępstwo ścigane z oskarżenia publicznego (albo też prywatnoskargowe, które zostało objęte skargą publiczną zgodnie z art. 60 § 1 kpk), zmiana stadium postępowania jest związana z instytucją przedstawienia zarzutów[30]. Przedstawienie zrzutów skutkuje tym, że od tego momentu postępowanie karne jest skierowane przeciwko indywidualnie określonej osobie, która w związku z przedstawieniem jej zarzutów staje się stroną tego postępowania, tj. podejrzanym.

Przedstawienie zarzutów zostało uregulowane w art. 313 § 1 kpk. Zgodnie z tym przepisem, jeżeli dane istniejące w chwili wszczęcia śledztwa lub zebrane w jego toku uzasadniają podejrzenie, że czyn popełniła określona osoba, sporządza się postanowienie o przedstawieniu podejrzanemu zarzutów, ogłasza się je mu niezwłocznie i przesłuchuje się go[31]. Jak wynika z powyższego, przedstawienie zarzutów jest instytucją procesową sformalizowaną przez przepisy procedury karnej, stanowiącą pewną sekwencje czynności, z których można wyodrębnić co najmniej trzy zasadnicze, tj. sporządzenie postanowienia o przedstawieniu zarzutów, ogłoszenie ich podejrzanemu oraz

---

[29] „Przełożony jest zobowiązany zawiesić funkcjonariusza w czynnościach służbowych w przypadku wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Przy tym rodzaju zawieszenia czynności przełożonego ograniczają się jedynie do sprawdzenia, czy toczy się przeciwko funkcjonariuszowi postępowanie karne o czyn wskazany w art. 58 ust. 1 u.a.b.w.a.w., nie jest on zobowiązany do zbadania zasadności zarzutów czy też okoliczności popełnienia czynu. Wystarczy sam fakt wszczęcia postępowania przeciwko funkcjonariuszowi, aby zawiesić go w czynnościach na okres do trzech miesięcy". Zob. P. Szustakiewicz, *Komentarz do art. 58*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el., teza 2.

[30] „Przedstawienie zarzutów oznacza przejście postępowania przygotowawczego z fazy *in rem* w fazę *in personam*". Zob. Z. Brodzisz, *Komentarz do art. 313*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 1; C. Golik, *Problem dopuszczalności uzupełnienia lub zmiany zarzutów w sposób uproszczony*, „Iustitia" 2014, nr 2, s. 81.

[31] Porównaj z § 137 ust. 1 *Rozporządzenia Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury* (t.j.: DzU z 2017 r. poz. 1206, ze zm.).

przesłuchanie go w tym charakterze[32]. Regułą jest więc, że zmiana stadium postępowania karnego polega na dopełnieniu powyższych czynności. Przedstawienie zarzutów stanowi pewną linię demarkacyjną rozgraniczającą postępowanie prowadzone w sprawie (*in rem*) od prowadzonego przeciwko indywidualnie oznaczonej osobie (*ad personam*)[33]. Na gruncie procesu karnego sporządzenie postanowienia o przedstawieniu zarzutów co do zasady nie jest równoznaczne z wydaniem postanowienia o przedstawieniu zarzutów[34]. Sporządzenie postanowienia o przedstawieniu zarzutów stanowi bowiem tylko jeden z elementów instytucji przedstawienia zarzutów, który musi być dopełniony także czynnościami: ogłoszenia ich podejrzanemu i przesłuchania go w tym charakterze[35]. Prezentowana reguła nie ma jednak charakteru bezwzględnego. Pewne wyjątki od niej zostały wyszczególnione w treści art. 313 § 1 *in fine* kpk[36]. Samo sporządzenie postanowienia o przedstawieniu zarzutów może być w pewnych okolicznościach uznane za równoznaczne z przedstawieniem zarzutów (z wydaniem postanowienia o przedstawieniu zarzutów), a tym samym może skutkować zmianą stadium postępowania

[32] Według Stanisława Waltosia i Piotra Hofmańskiego czynnościami stanowiącymi instytucję przedstawienia zarzutów są: sporządzenie postanowienia o przedstawieniu zarzutów, niezwłoczne ogłoszenie jego treści podejrzanemu oraz pouczenie go o uprawnieniach i obowiązkach, przesłuchanie podejrzanego, chyba że nie jest to możliwe z powodu jego ukrywania się lub nieobecności w kraju, pouczenie podejrzanego o prawie żądania – do czasu zawiadomienia go o terminie zaznajomienia z materiałami śledztwa – podania mu ustnie podstaw zarzutów oraz żądania sporządzenia uzasadnienia na piśmie, sporządzenie takiego uzasadnienia oraz jego doręczenie podejrzanemu i ustanowionemu obrońcy w terminie 14 dni. Zob. S. Waltoś, P. Hofmański, *Proces karny. Zarys systemu*, Warszawa 2018, s. 504 i nast. Por. także: J. Zagrodnik, *Postępowanie przygotowawcze*, w: *Proces karny. Przebieg postępowania*, K. Marszał (red.), Katowice 2012, s. 57.

[33] J. Zagrodnik, *Postępowanie przygotowawcze*…, s. 56.

[34] Wyrok SN – Izba Karna z 24 VI 2013 r., V KK 453/12, Legalis nr 712236; wyrok Sądu Okręgowego w Łodzi – V Wydział Karny z 14 III 2012 r., V KZ 148/12, Legalis nr 548065; postanowienie SN – Izba Karna z 16 I 2009 r., IV KK 256/08, Legalis nr 210120.

[35] „(…) dla przyjęcia, że nastąpiło przekształcenie postępowania z fazy *in rem* w fazę *in personam*, niezbędne jest łączne spełnienie 3 warunków: sporządzenie postanowienia o przedstawieniu zarzutów, jego niezwłoczne ogłoszenie i przesłuchanie podejrzanego, oczywiście o ile nie skorzysta on z prawa do odmowy składania wyjaśnień oraz gdy nie wystąpią sytuacje wskazane w art. 313 § 1 *in fine* kpk. W praktyce sporządzenie postanowienia o przedstawieniu zarzutów, jego ogłoszenie i ewentualne przesłuchanie podejrzanego powinno nastąpić w ciągu jednego dnia, chyba że zachodzą okoliczności wskazane w art. 313 § 1 kpk *in fine*". Zob. wyrok SN – Izba Karna z 24 VI 2013 r., V KK 453/12); także: wyrok SN – Izba Karna z 5 III 2014 r., IV KK 341/13, Legalis nr 924802; wyrok SA w Katowicach – II Wydział Karny z 28 II 2014 r., II AKa 21/14, Legalis nr 1045021; postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z 27 III 2013 r., II AKz 97/13, Legalis nr 732815; wyrok SN – Izba Karna z 2 VI 2010 r., V KK 376/09, Legalis nr 451571.

[36] „Jeżeli po sporządzeniu postanowień o przedstawieniu zarzutów nie doszło wprawdzie do ich ogłoszenia sprawcy i do przesłuchania go w charakterze podejrzanego, co nie było możliwe wskutek ukrywania się podejrzanego i jego nieobecności w kraju, w myśl art. 313 § 1 *in fine* kpk należało w takiej sytuacji przyjąć, że postanowienie o przestawieniu zarzutów zostało wydane i nastąpiło wszczęcie postępowania przeciwko osobie (*in personam*)". Zob. wyrok SN – Izba Karna z 4 VII 2019 r., III KK 273/18, Legalis nr 1973396. Porównaj także z § 137 ust. 2 rozporządzenia Ministra Sprawiedliwości – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury.

z *in rem* w *ad personam*, jeżeli czynności ogłoszenia zarzutów podejrzanemu i przesłuchania go w tym charakterze nie da się przeprowadzić z uwagi na jego ukrywanie się lub nieobecność w kraju[37].

Przedstawiona sekwencja czynności stanowiąca instytucję przedstawienia zarzutów może także, na gruncie kpk, ulegać pewnym modyfikacjom, z reguły bowiem przedstawienie zarzutów następuje po formalnym wszczęciu postępowania karnego (po uprzednim wydaniu postanowienia o wszczęciu śledztwa albo dochodzenia). Jest to tzw. zwykłe przedstawienie zarzutów. Procedura karna przewiduje jednak możliwość przedstawienia zarzutów już na wstępnym etapie postępowania karnego, przed jego formalnym wszczęciem. Jest to uproszczone przedstawienie zarzutów. Jeżeli zmiana stadium postępowania następuje już na etapie prowadzonego postępowania w niezbędnym zakresie (w trybie art. 308 § 1 kpk)[38], to niezależnie od tego, czy właściwą dla tego postępowania formą jest śledztwo czy dochodzenie, nie sporządza się odrębnego postanowienia o przedstawieniu zarzutów. Treść zarzutów wpisuje się w takim przypadku do protokołu przesłuchania podejrzanego, sama czynność sprowadza się natomiast do ogłoszenia treści tych zarzutów podejrzanemu i przesłuchania go w tym charakterze (art. 308 § 2 kpk)[39].

W przypadku prowadzenia postępowania w formie dochodzenia po jego formalnym wszczęciu (wydaniu postanowienia o wszczęciu dochodzenia) nie jest wymagane sporządzenie odrębnego postanowienia o przedstawieniu zarzutów i ponowne ich ogłoszenie podejrzanemu oraz jego przesłuchanie. Dotyczy to sytuacji, w której zmiana stadium postępowania z *in rem* w *ad personam* nastąpiła na etapie postępowania w niezbędnym zakresie (jeśli przesłuchano osobę w charakterze podejrzanego w trybie art. 308 § 2 kpk), chyba że podejrzany jest tymczasowo aresztowany (art. 325g § 1 kpk)[40]. Analogicznie, jeśli zmiana stadium postępowania z *in rem* w *ad personam*

---

[37] „Przepis art. 313 § 1 kpk *in fine* wskazuje tylko na dwie kategorie przeszkód leżących po stronie podejrzanego, które pozwalają na uznanie wydanego postanowienia o przedstawieniu zarzutów za prawnie skuteczne, mimo nieprzeprowadzenia czynności promulgacyjnych". Zob. wyrok SN – Izba Karna z 2 IX 2016 r., III KK 97/16, Legalis nr 1522323; także: wyrok SA w Katowicach – II Wydział Karny z 18 IX 2015 r., II AKa 268/15, Legalis nr 1398816; wyrok SN – Izba Karna z 5 III 2015 r., III KK 414/14, Legalis nr 1231789; postanowienie SA w Szczecinie – II Wydział Karny z 16 X 2012 r., II AKz 404/12, Legalis nr 680282; wyrok SN – Izba Karna z 7 XI 2006 r., IV KK 150/06, Legalis nr 88729; postanowienie SN – Izba Karna z 22 VI 2001 r., III KKN 44/01, Legalis nr 52788.

[38] Szerzej na ten temat zob. B. Szyprowski, *Dochodzenie w niezbędnym zakresie jako faktyczne wszczęcie postępowania przygotowawczego*, „Prokuratura i Prawo" 2006, nr 11, s. 140 i nast.

[39] Analogicznie w postępowaniu przyspieszonym, zgodnie z art. 517c kpk, nie sporządza się odrębnego postanowienia o przedstawieniu zarzutów, a czynności z udziałem podejrzanego ograniczają się do jego przesłuchania w tym charakterze.

[40] „W art. 325g § 1 kpk ustanowione zostało odstępstwo od obowiązującej w śledztwie zasady, że za podejrzanego uważa się osobę, co do której wydano postanowienie o przedstawieniu zarzutów, przewidując że status taki osoba podejrzana uzyskuje już z chwilą rozpoczęcia przesłuchania, po powiadomieniu jej o treści zarzutu wpisanego do protokołu przesłuchania". Zob. Z. Brodzisz, *Komentarz do art. 325g*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 1.

następuje po formalnym wszczęciu dochodzenia (po wydaniu postanowienia o wszczęciu dochodzenia), przedstawienie zarzutów również może nastąpić w taki sam sposób jak w postępowaniu w niezbędnym zakresie, tj. przez wpisanie treści zarzutów do protokołu przesłuchania podejrzanego, ogłoszenie mu ustnie zarzutów i przesłuchanie go w tym charakterze. Zgodnie bowiem z art. 325g § 1 kpk jest regułą, że w całym dochodzeniu dopuszczalne jest uproszczone przedstawienie zarzutów, z zastrzeżeniem wyjątku, o którym mowa w wymienionym przepisie. Stanowi to pewien przykład odformalizowania postępowania karnego prowadzonego w formie dochodzenia w stosunku do śledztwa[41].

W postępowaniu, którego właściwą formą jest śledztwo, jeśli przedstawienie zarzutów nastąpiło w postępowaniu w niezbędnym zakresie, wówczas najpóźniej w ciągu pięciu dni od dnia przesłuchania podejrzanego niezbędne jest wydanie postanowienia o przedstawieniu zarzutów, a w razie braku warunków do jego sporządzenia, konieczne jest umorzenie postępowania w stosunku do osoby przesłuchanej w charakterze podejrzanego (art. 308 § 3 kpk)[42].

Jak zauważa Cezary Golik, w przypadku uproszczonego przedstawienia zarzutów rozpoczęcie fazy *ad personam* postępowania następuje dokładnie w chwili, gdy organ procesowy kończy odczytywanie osobie zarzutu wpisanego w treść protokołu tej czynności i przystępuje do przesłuchania jej w charakterze podejrzanego[43].

Zgodnie z art. 309 pkt 1 i 2 kpk[44] śledztwo prowadzi się m.in. w sprawach, których rozpoznanie w pierwszej instancji należy do właściwości sądu okręgowego[45], a także w sprawach o występki, gdy osobą podejrzaną jest m.in. funkcjonariusz ABW albo AW. W każdym zatem przypadku – niezależnie od tego, czy została popełniona zbrodnia czy występek – jeśli osobą podejrzaną jest funkcjonariusz ABW albo AW, to formą prowadzonego postępowania jest śledztwo. Z uwagi na omawianą problematykę przedmiotem postępowania karnego może być każdego rodzaju zbrodnia, można ją bowiem popełnić tylko umyślnie, oraz umyślne występki ścigane z oskarżenia publicznego (albo prywatnoskargowe objęte skargą publiczną). Jeżeli postępowanie było uprzednio prowadzone w formie dochodzenia, to organ procesowy jest zobligowany do wszczęcia i prowadzenia

---

41 Tamże.

42 Według C. Golika, jeżeli przedstawienie zarzutów nastąpiło w trybie art. 308 § 2 kpk, w zakresie spraw, w których prowadzenie śledztwa jest obowiązkowe, konieczne jest niejako potwierdzenie tej decyzji o uproszczonym przedstawieniu zarzutów przez dokonanie tej czynności w sposób zwyczajny. Ponadto, w takich przypadkach uproszczone przedstawienie zarzutów w toku tzw. czynności prowadzonych w niezbędnym zakresie ma charakter terminowy, gdyż w okresie do pięciu dni musi zostać zatwierdzone przez przedstawienie zarzutów podejrzanemu w sposób zwyczajny, gdyż w przeciwnym razie ustawa wymaga umorzenia prowadzonego postępowania wobec tej osoby. Zob. C. Golik, *Moment procesowej skuteczności przedstawienia zarzutów w sposób uproszczony*, „Prokuratura i Prawo" 2020, nr 2, s. 18.

43 Tamże, s. 24 i nast.

44 Pozostałe przypadki wymienione w art. 309 pkt 3–5 kpk nie są aż tak istotne z punktu widzenia omawianej problematyki.

45 Chodzi tutaj o zbrodnie i enumeratywnie wskazane występki (art. 25 § 1 kpk).

śledztwa od momentu, w którym powziął informacje (odkąd jest mu to wiadome), że osobą podejrzaną lub podejrzanym będzie lub może być osoba wymieniona w tym przepisie, tj. funkcjonariusz ABW albo AW[46]. We wstępnej fazie prowadzonego postępowania karnego organ procesowy może nie wiedzieć, że osoba, przeciwko której prowadzi lub będzie prowadził postępowanie karne, jest funkcjonariuszem ABW albo AW, zwłaszcza jeśli w toku wykonywanych z nim wstępnych czynności podejrzany (osoba podejrzana) zatai tę okoliczność. Dlatego w sytuacji wcześniejszego przedstawienia zarzutów i przesłuchania podejrzanego w trybie określonym w art. 308 § 2 kpk, w przypadku wszczęcia dochodzenia, a następnie zmiany formy prowadzonego postępowania i jego przejścia z dochodzenia w śledztwo, niezbędne jest wydanie postanowienia o przedstawieniu zarzutów[47]. Analogicznie jest w sytuacji przedstawienia zarzutów we wszczętym dochodzeniu w trybie art. 325g § 2 kpk. Zmiana formy postępowania skutkująca zainicjowaniem śledztwa, w wyniku ujawnienia się okoliczności, że podejrzanym jest funkcjonariusz ABW albo AW, zobowiązuje do zastosowania art. 313 § 1 kpk.

Zarówno zwykłe (art. 313 § 1 kpk), jak i uproszczone[48] (art. 308 § 2 kpk) przedstawienie zarzutów wywołuje ten sam skutek w postaci zmiany stadium postępowania karnego z *in rem* w *ad personam*. Nie ma przy tym znaczenia, czy taka zmiana nastąpiła w prowadzonym śledztwie, czy też – z jakichkolwiek przyczyn, nawet niezasadnie – organ procesowy prowadził postępowanie wobec funkcjonariusza ABW albo AW w formie dochodzenia. Badając podstawy zawieszenia w czynnościach służbowych, przełożony nie ocenia ewentualnych uchybień natury procesowej w postępowaniu karnym, ale ogranicza się wyłącznie do ustalenia, czy to postępowanie toczy się przeciwko danej osobie.

W sytuacji zmiany stadium postępowania karnego w *ad personam* istotne znaczenie ma to, że takie postępowanie (o czyn objęty zarzutem) zostaje skierowane przeciwko danej osobie tylko raz i jest prowadzone przeciwko niej do jego zakończenia. Niemożliwe jest bowiem co do zasady wielokrotne inicjowanie postępowania karnego o ten sam czyn przeciwko tej samej osobie (art. 327 § 1 kpk), z zastrzeżeniem wyjątków wskazanych w art. 327 § 2 kpk i art. 328 § 1 kpk. Wniesienie przez oskarżyciela publicznego (prokuratora) aktu oskarżenia do sądu kończy jedynie postępowanie przygotowawcze i inicjuje postępowanie jurysdykcyjne, a także zmienia status jego uczestnika z podejrzanego na oskarżonego. Nie zmienia jednak tego, że nadal jest ono prowadzone przeciwko konkretnie wskazanej osobie.

Jak wcześniej wspomniano, w postępowaniu karnym zmiana stadium postępowania jest związana immanentnie z przedstawieniem zarzutów, stanowiącym pewien zespół czynności, których dopełnienie umożliwia stwierdzenie, że od określonego

---

[46] Z. Brodzisz, *Komentarz do art. 309*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 5.

[47] Tamże, teza 6.

[48] Uproszczone lub zredukowane przedstawienie zarzutów. Zob. C. Golik, *Moment procesowej skuteczności*…, s. 17.

momentu postępowanie karne jest skierowane przeciwko ściśle określonej osobie. Regulacja kpk musi bowiem stanowić właściwą gwarancję zabezpieczającą prawa strony tego postępowania. Niewątpliwie wskutek przedstawienia zarzutów pojawia się w procesie karnym strona, tj. podejrzany (art. 299 § 1 kpk[49])[50]. Skuteczne korzystanie przez niego z prawa do obrony wymaga, aby miał świadomość tego, że jest stroną tego postępowania, oraz że toczy się ono przeciwko niemu. Mechanizm ustanowiony w przepisach prawa karnego procesowego jest gwarancją właściwego zabezpieczenia tych praw podejrzanego.

Instytucja zawieszenia w czynnościach służbowych, o której mowa w art. 58 ust. 1 u.a.b.w.a.w., w żaden sposób nie oddziałuje na tok prowadzonego postępowania karnego, nie kształtuje również praw i obowiązków strony tego postępowania. Nie wpływa także na status takiej osoby. Zawieszenie w czynnościach służbowych, o którym mowa w pragmatyce służbowej, nie jest tożsame ze środkiem zapobiegawczym zamieszczonym w art. 276 kpk[51]. Są to niezależne od siebie instrumenty prawne służące zgoła odmiennym celom[52]. Inne są również podstawy umożliwiające ich stosowanie. Wobec tego przyjęcie założenia, że obowiązek zawieszenia funkcjonariusza w czynnościach służbowych, na podstawie art. 58 ust. 1 u.a.b.w.a.w., materializuje się wyłącznie po przedstawieniu mu zarzutów, tj. po dopełnieniu wszystkich niezbędnych czynności stanowiących tę instytucję, mogłoby skutkować wypaczeniem jej funkcji i celu, dla którego została ona ustanowiona. W pierwszej kolejności należy mieć bowiem na uwadze, że tym celem jest, jak wynika wprost z art. 58 ust. 4 u.a.b.w.a.w., niezwłoczne odsunięcie funkcjonariusza od wykonywania obowiązków służbowych, a nie – jak to ma miejsce w sytuacji zawieszenia w czynnościach służbowych na podstawie art. 276 kpk – zabezpieczenia prawidłowego toku postępowania karnego (art. 249 § 1 kpk). Zawieszenie w czynnościach służbowych, o którym mowa w kpk, spełnia więc funkcję procesową[53]. Natomiast zawieszenie w czynnościach służbowych, o którym mowa w art. 58 ust. 1 u.a.b.w.a.w., ma chronić interes służby (jej dobro), a w szerszym aspekcie – interes społeczny. Zmierza zatem do niezwłocznego odsunięcia od pełnienia służby i wykonywania czynności służbowych tych funkcjonariuszy, którzy znaleźli się w kręgu podejrzeń

---

[49] M. Korcyl-Wolska, *Postępowanie przygotowawcze*, w: *Postępowanie karne. Przebieg*, A.R. Światłowski (red.), Warszawa 1999, s. 35.

[50] „Stronami postępowania karnego są ci jego uczestnicy, którzy działają w procesie we własnym imieniu, mając interes prawny w określonym rozstrzygnięciu o przedmiocie procesu". Zob. T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2007, s. 279; S. Waltoś, *Proces karny. Zarys systemu*, Warszawa 2003, s. 176 i nast.

[51] Zgodnie z tym przepisem tytułem środka zapobiegawczego można zawiesić oskarżonego w czynnościach służbowych lub w wykonywaniu zawodu albo nakazać powstrzymanie się od określonej działalności lub od prowadzenia określonego rodzaju pojazdów, lub zakazać ubiegania się o zamówienia publiczne na czas trwania postępowania.

[52] Wyrok NSA z 3 II 2017 r., I OSK 1495/15, Legalis nr 1578651 (dotyczy policjanta).

[53] J. Kosonoga, *Komentarz do art. 276*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 2.

o popełnienie czynu wypełniającego znamiona przestępstwa umyślnego ściganego z oskarżenia publicznego.

W praktyce natomiast, w postępowaniu karnym, między sporządzeniem postanowienia o przedstawieniu zarzutów a ich ogłoszeniem podejrzanemu i przesłuchaniem go w tym charakterze może upłynąć wiele czasu. Zwłaszcza gdy wobec osoby, której mają być przedstawione zarzuty, nie stosuje się środków represyjnych przewidzianych przez przepisy procedury karnej, umożliwiających niezwłoczne dopełnienie wszystkich czynności składających się na instytucję przedstawienia zarzutów (zatrzymanie i przymusowe doprowadzenie, o którym mowa w art. 247 kpk), a funkcjonariusz podejmuje działania nakierowane na opóźnienie w ich dopełnieniu. Podmiot, o którym mowa w art. 50 ust. 1 u.a.b.w.a.w., byłby zobowiązany w takich sytuacjach do samodzielnego dalszego ustalania, czy w danym przypadku doszło do zmiany stadium postępowania karnego. Dotyczy to szczególnie sytuacji, gdy prokurator, realizując swój obowiązek wynikający z art. 21 § 1 pkt 1 kpk[54], poinformowałby szefa ABW albo AW wyłącznie o sporządzeniu postanowienia o przedstawieniu zarzutów wobec funkcjonariusza ABW albo AW[55], nie wskazałby natomiast innych okoliczności, które umożliwiłyby stwierdzenie, że na gruncie procedury karnej niewątpliwie doszło do zmiany stadium tego postępowania. Oznacza to, że automatyczne i bezkrytyczne przenoszenie mechanizmów przewidzianych w przepisach procedury karnej na grunt pragmatyki służbowej mogłoby doprowadzić do znacznego utrudnienia realizacji tego obowiązku, a tym samym wypaczałoby sens tej instytucji. Również w samej procedurze karnej przewiduje się wyjątki w tym zakresie i umożliwia się, w pewnych okolicznościach, utożsamienie samego sporządzenia postanowienia o przedstawieniu zarzutów ze zmianą fazy tego postępowania, mimo że zmiana stadium wpływa bezpośrednio na prawa i obowiązki podejrzanego. Skoro zawieszenie w czynnościach służbowych z art. 58 ust. 1 u.a.b.w.a.w. nie oddziałuje w żaden sposób na tok prowadzonego postępowania karnego, ale ma na celu jak najszybsze odsunięcie funkcjonariusza od pełnienia służby i wykonywania czynności służbowych, to należy przyjąć, że użyte w treści tego przepisu sformułowanie „wszczęcie postępowania karnego przeciwko osobie" i związaną z nim zmianę stadium postępowania karnego powinno się utożsamiać już z samym sporządzeniem postanowienia o przedstawieniu zarzutów (chyba że przedstawienie zarzutów następuje bez wydania takiego postanowienia w związku z przesłuchaniem osoby w charakterze podejrzanego, po uprzednim ogłoszeniu mu zarzutów wpisanych do treści protokołu). Tylko taka wykładnia normy zawartej w art. 58 ust. 1 u.a.b.w.a.w.

---

[54] Ten przepis statuuje obowiązek poinformowania jego przełożonego o wszczęciu i ukończeniu postępowania toczącego się z urzędu m.in. przeciwko funkcjonariuszowi publicznemu.

[55] Funkcjonariusz, mając świadomość konsekwencji, nie spełniłby natomiast swojego obowiązku wynikającego z § 17 pkt 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 2 lipca 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* (t.j.: DzU z 2013 r. poz. 862, ze zm.) albo z § 17 pkt 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 28 listopada 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Wywiadu* (DzU z 2003 r. nr 210 poz. 2039, ze zm.).

umożliwia szybką, skuteczną i efektywną realizację tego obowiązku, polegającą na odsunięciu funkcjonariusza od wykonywania obowiązków służbowych.

To stanowisko potwierdza również judykatura. W wyroku z 17 lipca 2018 r.[56] Naczelny Sąd Administracyjny, oceniając, czy zmaterializowała się przesłanka obligatoryjnego zawieszenia policjanta w czynnościach służbowych, o którym mowa w art. 39 ust. 1 ustawy o Policji, wskazał, że chociaż ten przepis stanowi podstawę do obligatoryjnego zawieszenia funkcjonariusza w czynnościach służbowych w razie wszczęcia przeciwko niemu postępowania karnego w sprawie o przestępstwo lub przestępstwo skarbowe, umyślne, ścigane z oskarżenia publicznego, to nie definiuje on pojęcia „wszczęcie postępowania karnego". W tym zakresie konieczne staje się odwołanie do regulacji procedury karnej – do art. 71 § 1 kpk. Zwrot „wydano" (postanowienie) jest natomiast odczytywany w praktyce przez pryzmat regulacji art. 313 § 1 kpk. „Sporządzenie postanowienia o przedstawieniu zarzutów" to niejako jego spisanie, „wydanie" zaś to: sporządzenie, ogłoszenie i przesłuchanie podejrzanego. Wykładnia tych pojęć nie jest jednolita, przepisy procedury karnej bowiem dopuszczają przejście postępowania karnego z fazy *in rem* w fazę *ad personam* w sytuacji, w której zapadło postanowienie o przedstawieniu zarzutów konkretnej osobie, nawet wtedy, gdy tego postanowienia nie ogłoszono i nie przesłuchano podejrzanego niezwłocznie po jego sporządzeniu. Do wszczęcia postępowania karnego przeciwko osobie może w niektórych sytuacjach dochodzić już wówczas, gdy sporządzono takie postanowienie, ale jeszcze go nie wydano w ścisłym (literalnym) rozumieniu hipotezy art. 71 § 1 kpk. Zdaniem sądu ma to podstawowe znaczenie, zwłaszcza na gruncie pragmatyki służbowej (w tym przypadku art. 39 ust. 1 ustawy o Policji). Według sądu:

> Trzeba bowiem mieć przede wszystkim na uwadze cel tej regulacji, którym jest natychmiastowe odsunięcie od czynności służbowych osób podejrzanych o popełnienie określonych w tym przepisie przestępstw. Nie wdając się więc w tym miejscu w szerszy dyskurs na temat rozumienia „podejrzanego" na gruncie procedury karnej, zwłaszcza na tle art. 71 § 1 kpk, trzeba stwierdzić, że zawarte w nim określenie „wydanie": może być utożsamione z pojęciem „sporządzenia" z art. 313 § 1 kpk na gruncie omawianej regulacji szczególnej. Naczelny Sąd Administracyjny wyraża przy tym pogląd, wedle którego przepisy procesowe karne pełnią funkcje m.in. gwarancyjne, zapewniając podejrzanemu określone uprawnienia w tym postępowaniu. Przenoszenie ich *in extenso* na inny grunt, w tym obecnie rozpoznawanej sprawy, nie jest poprawne. Zwłaszcza nie może znaleźć aprobaty z uwagi na inny charakter obu reżimów prawnych. Zatem transponowanie w procesie interpretacji przepisów ustawy o Policji uregulowań należących do postępowania karnego musi odbywać się z uwzględnieniem specyfiki służby, a także celu zawieszenia. Nie jest przy tym rolą organów Policji badanie prawidłowości i skuteczności procesowej podejmowanych czynności przez inny podmiot powołany do ich realizacji. (…) Zaakcentować wypada tu nie tylko aspekt celowościowy tej regulacji, ale i rozbieżności interpretacyjne

[56] Wyrok NSA z 17 VII 2018 r., I OSK 19113/16, Legalis nr 1833570.

> powołanych przepisów procedury karnej, które powszechnie uznawane są za sprzeciwiające się przyjęciu tezy o rażącym naruszeniu prawa w sytuacji stosowania niejednoznacznie rozumianego przepisu. Dokonana przez Sąd *meriti* ocena zgodności z prawem zaskarżonej decyzji była więc prawidłowa[57].

Zeprezentowane przez Naczelny Sąd Administracyjny stanowisko można odnieść *per analogiam* do omawianej problematyki i można je podzielić w całej rozciągłości z uwagi na podobne brzmienie przepisu art. 39 ust. 1 ustawy o Policji oraz art. 58 ust. 1 u.a.b.w.a.w., a także z uwagi na przedstawione argumenty.

W uzupełnieniu należy również podkreślić, że skoro zawieszenie w czynnościach służbowych polega na niezwłocznym odsunięciu funkcjonariusza od wykonywania obowiązków służbowych, to korzystanie z tego instrumentu prawnego, aby mogło być efektywne i skuteczne, musi umożliwiać niezwłoczną i adekwatną do zaistniałego stanu faktycznego reakcję uprawnionego podmiotu. Jeżeli organ procesowy ustalił, że dane istniejące w chwili wszczęcia postępowania karnego lub zebrane w jego toku uzasadniają dostatecznie podejrzenie, że czyn popełniła określona osoba – a już to stanowi dostateczną podstawę do sporządzenia wobec funkcjonariusza postanowienia o przedstawieniu zarzutów – to samo sporządzenie takiego postanowienia musi stanowić wystarczającą podstawę do zastosowania wobec funkcjonariusza ABW albo AW zawieszenia w czynnościach służbowych. Dokonywanie innych ustaleń w tym zakresie może skutkować zwłoką w podjęciu decyzji o zawieszeniu, zwłaszcza że, zgodnie z art. 309 pkt 2 kpk, postępowanie karne przeciwko funkcjonariuszowi ABW albo AW ma formę śledztwa i jest zastrzeżone do wyłącznego prowadzenia przez prokuratora (art. 311 § 2 kpk). Trudno zakładać, aby była możliwa niezwłoczna reakcja przełożonego, jeśli konieczne stałoby się uzupełnienie pierwotnie przekazanej przez prokuratora informacji o sporządzeniu wobec funkcjonariusza ABW albo AW postanowienia o przedstawieniu zarzutów. Instrument, o którym mowa w art. 58 ust. 1 u.a.b.w.a.w., musi być natomiast adekwatnym środkiem do osiągnięcia celu, dla którego ten przepis został zamieszczony w pragmatyce służbowej. Odsunięcie funkcjonariusza od wykonywania obowiązków służbowych powinno nastąpić niezwłocznie, z chwilą ustalenia, że znalazł się on w kręgu podejrzeń o popełnienie przestępstwa umyślnego ściganego z oskarżenia publicznego. Te podejrzenia zostają potwierdzone przez sporządzenie wobec funkcjonariusza postanowienia o przedstawieniu zarzutów, chociażby nie zostały mu one jeszcze ogłoszone. Na gruncie pragmatyki służbowej samo sporządzenie takiego postanowienia powinno być więc traktowane jako równoznaczne z wszczęciem przeciwko

---

[57] W tym samym tonie wyrok NSA z 10 XI 2017 r., I OSK 70/16, Legalis nr 1710801; także: wyrok WSA w Poznaniu z 29 VII 2014 r., II SA/Po 273/14, Legalis nr 1104412. Przeciwnie – zob. M. Nowikowska, *Komentarz do art. 39*, w: *Ustawa o Policji. Komentarz*, K. Chałubińska-Jentkiewicz, J. Kurek (red.), Warszawa 2021, Legalis/el., teza 2 i tam przywołany wyrok WSA w Warszawie z 27 X 2015 r., II SA/Wa 358/15, Legalis nr 1364493; podobnie: wyrok WSA w Gdańsku z 5 VII 2018 r., III SA/Gd 335/18, Legalis nr 1810427; wyrok WSA w Białymstoku z 21 I 2016 r., II SA/Bk 740/15, Legalis nr 1432094 (dotyczy funkcjonariusza celnego); wyrok WSA w Gdańsku z 2 IV 2014 r., III SA/Gd 60/14, Legalis nr 953297.

funkcjonariuszowi postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego i powinno stanowić podstawę do obligatoryjnego zawieszenia go w czynnościach służbowych.

Należy ponadto zwrócić uwagę na szczególny przypadek wszczęcia postępowania karnego przeciwko osobie w wyniku wniesienia subsydiarnego aktu oskarżenia, o którym mowa w art. 55 § 1 kpk[58]. Trzeba jednak zastrzec, że subsydiarny akt oskarżenia, aby obligował do zawieszenia w czynnościach służbowych funkcjonariusza ABW albo AW, musi dotyczyć przestępstwa umyślnego ściganego z oskarżenia publicznego. Nie może nim być, z oczywistych względów, przestępstwo nieumyślne ścigane z oskarżenia publicznego. Nie może nim być również przestępstwo prywatnoskargowe, które zostało objęte skargą publiczną na zasadzie art. 60 kpk. Jeżeli prokurator wszczęłby postępowanie w sprawie o przestępstwo ścigane z oskarżenia prywatnego, a następnie od oskarżenia by odstąpił, wówczas pokrzywdzony może złożyć przeciwko funkcjonariuszowi ABW albo AW prywatny akt oskarżenia lub oświadczenie, że podtrzymuje oskarżenie jako prywatne (art. 60 § 4 kpk)[59]. Dlatego też w wymienionych przypadkach instytucja, o której mowa w art. 55 § 1 kpk, nie ma zastosowania.

Nie ma natomiast znaczenia, że subsydiarny akt oskarżenia nie stanowi skargi publicznej. Podmiotem, który go wnosi i popiera, jest oskarżyciel posiłkowy subsydiarny. Przesłanka, o której mowa w art. 58 ust. 1 u.a.b.w.a.w., materializuje się natomiast w sytuacji wszczęcia postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego albo gdy umyślne przestępstwo prywatnoskargowe jest objęte skargą publiczną. Może być wówczas traktowane na gruncie pragmatyki służbowej, tak jakby było przestępstwem publicznoskargowym. Jeśli zatem czyn stanowi umyślne przestępstwo publicznoskargowe, to nie jest istotne, czy jest objęte skargą publiczną, jak ma to miejsce w przypadku przestępstwa prywatnoskargowego. Przestępstwo publicznoskargowe nie zmienia bowiem swojego charakteru, nawet gdy podmiotem inicjującym postępowanie przeciwko danej osobie jest podmiot inny niż oskarżyciel publiczny, tj. oskarżyciel posiłkowy subsydiarny – wnoszący subsydiarny akt oskarżenia. W kontekście przesłanki zawartej w art. 58 ust. 1 u.a.b.w.a.w. w odniesieniu do umyślnego przestępstwa ściganego z oskarżenia publicznego chodzi o charakter przestępstwa będącego przedmiotem postępowania karnego, a nie o tryb inicjujący to postępowanie karne, czyli skargę publiczną. Jak słusznie zaznacza Anna Dziergawka: *Istota subsydiarnego aktu oskarżenia sprowadza się zasadniczo do możliwości wniesienia przez pokrzywdzonego aktu oskarżenia (skargi subsydiarnej) w sprawach ściganych z oskarżenia publicznego w sytuacji, gdy odmawia tego prokurator*[60]. Nie może zatem budzić wątpliwości,

[58] Szerzej na ten temat zob. A. Porębska, P. Graczyk, *Subsydiarny akt oskarżenia – wybrane zagadnienia proceduralne*, w: *Problemy współczesnego prawa karnego. Część pierwsza*, B. Bieńkowska, Z. Jędrzejewski (red.), 2016, Legalis/el.

[59] Wyrok Trybunału Konstytucyjnego z 2 IV 2001 r., SK 10/00, Legalis nr 49670.

[60] A. Dziergawka, *Subsydiarny akt oskarżenia w świetle nowelizacji dokonanej ustawą z dnia 19 lipca 2019 r.*, „Prokuratura i Prawo" 2020, nr 1, s. 153.

że wniesienie takiego aktu oskarżenia przez oskarżyciela posiłkowego subsydiarnego, jeśli inicjuje postępowanie karne przeciwko osobie o umyślne przestępstwo ścigane z oskarżenia publicznego[61], jest objęte przepisem art. 58 ust. 1 u.a.b.w.a.w. Późniejsze wstąpienie do tego postępowania oskarżyciela publicznego[62] (art. 55 § 4 kpk)[63], skutkujące dalszym toczeniem się tego postępowania z oskarżenia publicznego, nie przekształca jednak wniesionego w danej sprawie aktu oskarżenia z subsydiarnego na publiczno-skargowy[64]. Tym samym nie wpływa na to, że już w chwili skutecznego wniesienia subsydiarnego aktu oskarżenia przez oskarżyciela posiłkowego subsydiarnego właśnie przez niego zostało zainicjowane postępowanie karne w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego.

Tę tezę potwierdza także art. 39 ust. 2a ustawy o Policji, zgodnie z którym wniesienie przeciwko policjantowi aktu oskarżenia określonego w art. 55 § 1 kpk powoduje, że możliwe jest odpowiednie stosowanie przepisu art. 39 ust. 2 ustawy o Policji. Ten ostatni przepis jest z kolei fakultatywną podstawą do zawieszenia w czynnościach służbowych. Analogiczną treść ma art. 43 ust. 2a *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*[65]. Gdyby intencją ustawodawcy było wyłączenie określonej kategorii spraw karnych o przestępstwo umyślne ścigane z oskarżenia publicznego wobec funkcjonariuszy ABW albo AW ze względu na sposób jego zainicjowania, tak jak jest to ujęte w wymienionych pragmatykach służbowych dotyczących funkcjonariuszy Policji czy Straży Granicznej, to dokonałby tego *expressis verbis* w treści konkretnego przepisu pragmatyki służbowej, tj. w u.a.b.w.a.w.

Instytucja subsydiarnego aktu oskarżenia może mieć zastosowanie wyłącznie w sytuacji powtórnego wydania postanowienia o odmowie wszczęcia lub umorzenia postępowania w wypadku, o którym mowa w art. 330 § 2 kpk (warunek wniesienia subsydiarnego aktu oskarżenia[66]). Pokrzywdzony może wówczas – w terminie miesiąca od

---

[61] Jak wskazuje Jacek Kosonoga, skarga subsydiarna pełni funkcję inicjującą, polegającą na wszczęciu postępowania jurysdykcyjnego (postępowania głównego). Zob. J. Kosonoga, *Instytucja skargi subsydiarnej – zarys problematyki*, „Monitor Prawniczy" 2006, nr 9, Legalis/el.

[62] Szerzej na ten temat zob. J. Zagrodnik, *Udział prokuratora w postępowaniu sądowym wszczętym przez oskarżyciela posiłkowego subsydiarnego*, „Prokuratura i Prawo" 2017, nr 2, s. 5 i nast.; tenże, *Udział prokuratora w postępowaniu sądowym na podstawie art. 55 § 4 kodeksu postępowania karnego*, „Prokuratura i Prawo" 2005, nr 3, s. 58 i nast.; I. Zgoliński, *Udział prokuratora w postępowaniu karnym inicjowanym posiłkowym aktem oskarżenia – zarys problematyki*, „Iustitia" 2013, nr 2, s. 83 i nast.

[63] „Data uprawomocnienia się wyroku stanowi punkt graniczny dla możliwości skorzystania przez prokuratora z uprawnień wynikających z tego przepisu art. 55 § 4 kpk". Zob. postanowienie SN – Izba Karna z 18 IV 2018 r., V KZ 12/18, Legalis nr 1835828.

[64] Postanowienie SN – Izba Karna z 9 X 2020 r., IV KK 268/19, Legalis nr 2508657.

[65] Tekst jednolity: DzU z 2021 r. poz. 1486, ze zm.

[66] „Warunek «powtórnego wydania postanowienia o odmowie wszczęcia lub o umorzeniu postępowania» (art. 55 § 1 kpk) należy rozumieć jako ponowne wydanie postanowienia tego samego rodzaju, jak poprzednie uchylone, czyli odpowiednio powtórnego postanowienia o odmowie wszczęcia lub powtórnego postanowienia o umorzeniu postępowania" (postanowienie SN – Izba

doręczenia mu zawiadomienia o postanowieniu prokuratora nadrzędnego o utrzymaniu w mocy zaskarżonego postanowienia – wnieść akt oskarżenia do sądu[67]. Istotą sformułowania „wniesienie aktu oskarżenia" jest jego wniesienie przez uprawniony podmiot do sądu. W tej sytuacji to prawo przysługuje pokrzywdzonemu, który odgrywa rolę oskarżyciela posiłkowego subsydiarnego. Istotne jest, aby wniesienie aktu oskarżenia było prawnie skuteczne, gdyż tylko takie łączy się z wszczęciem postępowania karnego przed sądem. Postępowanie przed sądem, ze swej istoty, ma charakter kontradyktoryjny (sporny), co oznacza, że toczy się ono z udziałem stron, tj. oskarżyciela i oskarżonego. Z kolei oskarżonym, zgodnie z art. 71 § 1 kpk, jest osoba, przeciwko której wniesiono oskarżenie do sądu albo wniosek wskazany w art. 335 § 1 kpk albo wniosek o warunkowe umorzenie postępowania karnego. Osoba wskazana w subsydiarnym akcie oskarżenia z chwilą skutecznego wniesienia tego aktu oskarżenia staje się zatem stroną tego postępowania. Toczy się ono od tego momentu przeciwko niej. Obligatoryjne zawieszenie w czynnościach służbowych będzie dotyczyć więc takiego subsydiarnego aktu oskarżenia, którego przedmiotem jest przestępstwo umyślne ścigane z oskarżenia publicznego. Powinno ono być poprzedzone albo dwukrotnie wydanymi decyzjami procesowymi o odmowie wszczęcia postępowania karnego albo decyzją umarzającą postępowanie karne prowadzone w sprawie (*in rem*) bądź przeciwko osobie (*ad personam*). Nie stoi to w opozycji do tego, że w toku postępowania karnego, które następnie dwukrotnie umorzono, przedstawiono osobie zarzuty o przestępstwo umyślne ścigane z oskarżenia publicznego. Wówczas przesłanka do obligatoryjnego zawieszenia funkcjonariusza w czynnościach służbowych zmaterializowała się w związku z przedstawieniem tych zarzutów.

Subsydiarny akt oskarżenia skutkuje natomiast tym, że postępowanie karne jest inicjowane przez oskarżyciela posiłkowego subsydiarnego w sprawie, która została uprzednio zakończona decyzją procesową o jej umorzeniu. Wymieniona decyzja procesowa uzyskuje przymiot prawomocności. Prawo pokrzywdzonego do wniesienia subsydiarnego aktu oskarżenia, jak zaznacza Jacek Kosonoga, powstaje natomiast z prawomocnością ponownego postanowienia prokuratora o odmowie wszczęcia bądź ponownego postanowienia o umorzeniu postępowania po uchyleniu przez sąd poprzedniego postanowienia o takiej samej treści[68]. Subsydiarny akt oskarżenia ponownie inicjuje to postępowanie, jednak od razu przenosi sprawę do etapu postępowania jurysdykcyjnego. Jeśli funkcjonariusza zawieszono w czynnościach służbowych, a następnie – na podstawie art. 58 ust. 3 u.a.b.w.a.w. – przedłużono mu okres tego zawieszenia na dalszy czas oznaczony, nie dłuższy niż do dnia uprawomocnienia się orzeczenia wydanego w postępowaniu karnym, to wymienione zawieszenie nie

Karna z 2 IX 2020 r., V KK 355/19, Legalis nr 2539282); także: W. Kotowski, *Podstawa wniesienia subsydiarnego aktu oskarżenia*, „n.ius", 4 III 2021 r., Legalis /el.

[67] Postanowienie SA w Krakowie – II Wydział Karny z 30 XI 2016 r., II AKz 395/17, Legalis nr 1594912; postanowienie SA we Wrocławiu – II Wydział Karny z 3 VIII 2011 r., II AKz 303/11, Legalis nr 424323; także: A. Kociemba, *Wniesienie subsydiarnego aktu oskarżenia po terminie a skutki wstąpienia prokuratora*, „n.ius", 22 I 2021 r., Legalis/el.

[68] Zob. J. Kosonoga, *Instytucja skargi subsydiarnej*...

rozciąga się na postępowanie jurysdykcyjne zainicjowane wskutek wniesienia subsydiarnego aktu oskarżenia, ale konieczne jest ponowne zawieszenie w czynnościach służbowych z uwagi na wniesiony subsydiarny akt oskarżenia. Inne jest bowiem źródło tego zawieszenia, którym jest skutecznie wniesiony do sądu subsydiarny akt oskarżenia.

Skuteczność subsydiarnego aktu oskarżenia nakazuje jednak uprzednie spełnienie wymogów wynikających z art. 55 § 2 kpk, tj. sporządzenia i podpisania go przez adwokata, radcę prawnego albo radcę Prokuratorii Generalnej Rzeczpospolitej Polskiej, z zachowaniem warunków określonych w art. 332 i art. 333 § 1 kpk. Subsydiarny akt oskarżenia musi także dotyczyć czynu tożsamego z tym, który był przedmiotem postępowania karnego zakończonego umorzeniem, albo czynu wskazanego w postanowieniu o odmowie wszczęcia postępowania[69]. Jego wniesienie do sądu, o ile jest prawnie skuteczne, powoduje zawisłość sprawy[70]. Od tego momentu postępowanie karne toczy się przeciwko osobie wskazanej w subsydiarnym akcie oskarżenia. Stąd też subsydiarny akt oskarżenia wymaga wstępnej weryfikacji przez sąd pod względem formalnym oraz tego, czy został on wniesiony w terminie i przez uprawniony podmiot. W sytuacji ujawnienia braków w tym zakresie sąd zwraca oskarżycielowi subsydiarny akt oskarżenia w celu jego uzupełnienia w terminie siedmiu dni (art. 337 kpk)[71]. Nieusunięcie braków formalnych wskazanych przez sąd bądź nieusunięcie ich w terminie wyznaczonym przez sąd powoduje, że wniesiony uprzednio subsydiarny akt oskarżenia nie wywołuje skutków prawnych, tj. nie powoduje stanu zawisłości sprawy. Tę sytuację należy traktować w taki sposób, jakby uprawniony podmiot w ogóle nie skorzystał ze swojego

---

[69] „Skarga subsydiarna może jedynie obejmować zarzut popełnienia czynu, który zachowuje przymiot tożsamości z tym, którego oceny dotyczyły decyzje kończące postępowanie przygotowawcze. Kryteria tożsamości czynu wyznacza opis czynu, co do którego dwukrotnie zapadły decyzje o odmowie wszczęcia lub o umorzeniu postępowania" (wyrok SA w Warszawie – II Wydział Karny z 22 XI 2019 r., II AKa 280/18, Legalis nr 2271634); postanowienie SN – Izba Karna z 7 I 2019 r., III KK 69/18, Legalis nr 1861035; wyrok SA w Katowicach z 12 X 2017 r., II AKa 244/17, Legalis nr 1809167; postanowienie SA w Katowicach – II Wydział Karny z 11 X 2017 r., II AKz 618/17, Legalis nr 1732966; wyrok SA w Szczecinie – II Wydział Karny z 23 V 2017 r., II AKa 48/17, Legalis nr 1683401; postanowienie SN – Izba Karna z 9 II 2017 r., IV KK 299/16, Legalis nr 1587617; wyrok SA w Warszawie – II Wydział Karny z 18 I 2017 r., II AKa 436/15, Legalis nr 1692396; wyrok SA w Warszawie – II Wydział Karny z 18 I 2017 r., II AKa 436/16, Legalis nr 1588036; postanowienie SN – Izba Karna z 24 XI 2016 r., III KK 274/16, Legalis nr 1544282; także: A. Dziergawka, *Subsydiarny akt oskarżenia*…, s. 160; A. Porębska, P. Graczyk, *Subsydiarny akt oskarżenia*… i tam przywołane orzecznictwo.

[70] „Wystąpienie przez pokrzywdzonego z subsydiarnym aktem oskarżenia rodzi określone skutki procesowe. Przede wszystkim powoduje stan zawisłości sprawy". Zob. wyrok SA w Lublinie z 11 VIII 2009 r., II AKa 107/09, Legalis nr 242777); także: A. Dziergawka, *Subsydiarny akt oskarżenia*…, s. 159.

[71] Możliwość stwierdzenia aktu oskarżenia za bezskuteczny jest warunkowana bowiem wcześniejszym wezwaniem strony do uzupełnienia wskazanych jej braków skargi w określonym terminie (postanowienie SN – Izba Karna z 23 I 2018 r., IV KK 186/17, Legalis nr 1713813).

uprawnienia, czyli nie wniósł subsydiarnego aktu oskarżenia[72]. Z kolei uzupełnienie braków formalnych w terminie powoduje uznanie, że postępowanie karne zostało zainicjowane z chwilą wniesienia subsydiarnego aktu oskarżenia, a nie z chwilą jego uzupełnienia. Ponowne wniesienie subsydiarnego aktu oskarżenia, bez uzupełnienia pierwotnie wniesionego, mającego braki formalne, ale po upływie terminu wskazanego w art. 55 § 1 kpk, także nie wywołuje skutków prawnych, tj. nie powoduje stanu zawisłości sprawy. Termin ten ma bowiem charakter prekluzyjny[73], co oznacza, że czynność dokonana po jego upływie jest prawnie nieskuteczna.

Jak już wcześniej zaznaczono, przesłanką wskazaną w art. 58 ust. 1 u.a.b.w.a.w. nie są objęte przypadki wniesienia prywatnego aktu oskarżenia bądź ustnej (lub pisemnej) skargi, o których mowa w art. 487 kk i art. 488 § 1 kk. Ich przedmiotem jest przestępstwo ścigane z oskarżenia prywatnego. Zainicjowanie postępowania karnego o przestępstwo ścigane z oskarżenia prywatnego przez oskarżyciela prywatnego nie obliguje, a także nie uprawnia do zawieszenia funkcjonariusza ABW albo AW w czynnościach służbowych. Wyjątek stanowią sytuacje, w których umyślne przestępstwa prywatnoskargowe objęte są skargą publiczną na zasadzie art. 60 § 1 kpk. Wówczas zmienia się tryb ścigania tych przestępstw, a postępowanie toczy się wówczas z urzędu (art. 60 § 2 kpk). Takie przestępstwo, w kontekście przesłanki z art. 58 ust. 1 u.a.b.w.a.w., powinno być traktowane w taki sam sposób, jakby było przestępstwem publicznoskargowym. Jeśli zatem prokurator obejmuje skargą publiczną umyślne przestępstwo prywatnoskargowe, to postępowanie karne zmienia stadium z *in rem* w *ad personam* w związku z przedstawieniem zarzutów konkretnej osobie[74], co wpływa na zmaterializowanie się przesłanki wskazanej w art. 58 ust. 1 u.a.b.w.a.w. Jeśli natomiast prokurator wstępuje do postępowania już wszczętego, zainicjowanego przez oskarżyciela prywatnego, to tryb prywatnoskargowy zmienia się w publicznoskargowy z chwilą tego wstąpienia[75].

---

[72] „Niezłożenie przez pokrzywdzonego subsydiarnego aktu oskarżenia w terminie przewidzianym w art. 55 § 1 k.p.k. nie powoduje wygaśnięcia tego uprawnienia na stałe. W sytuacji podjęcia przez prokuratora postępowania na podstawie art. 327 § 1 k.p.k., a następnie powtórnego jego umorzenia, na nowo rozpoczyna swój bieg termin do realizacji uprawnienia, które pokrzywdzony nabył już wcześniej, a więc w chwili spełnienia przesłanek przewidzianych w art. 330 § 2 k.p.k." Zob. W. Kotowski, *Uprawnienie do złożenia subsydiarnego aktu oskarżenia*, „n.ius", 19 II 2021 r., Legalis/el.; także: postanowienie SN – Izba Karna z 3 IX 2020 r., III KK 194/20, Legalis nr 2533735.

[73] Postanowienie SA w Krakowie – II Wydział Karny z 5 VII 2019 r., II AKz 320/19, Legalis nr 2269222; wyrok SA w Krakowie – II Wydział Karny z 10 XII 2018 r., II AKa 236/18, Legalis nr 2233118; wyrok SN – Izba Karna z 12 XII 2016 r., V KK 243/16, Legalis nr 1565032; także: S. Jaworski, *Pełnomocnik w sprawie z subsydiarnego aktu oskarżenia*, w: *Metodyka pracy adwokata i radcy prawnego w sprawach karnych*, Warszawa 2020, Legalis/el.

[74] S. Szołucha, *Komentarz do art. 60…*, teza 3.

[75] „Prokurator może wstąpić do postępowania toczącego się ze skargi oskarżyciela prywatnego, aż do czasu jego prawomocnego zakończenia. Postępowanie toczy się wówczas z urzędu, a pokrzywdzony, który przedtem wniósł oskarżenie prywatne, zyskuje uprawnienia oskarżyciela posiłkowego". Zob. tamże, teza 5.

W tym momencie materializuje się również przesłanka, o której mowa w art. 58 ust. 1 u.a.b.w.a.w., pod warunkiem, że dotyczy czynu będącego przestępstwem umyślnym.

Odrębnego potraktowania wymagają również przypadki wskazane w art. 327 § 2 kpk i art. 328 § 1 kpk[76]. Zgodnie z pierwszym z wymienionych przepisów prawomocnie umorzone postępowanie przygotowawcze wznawia się przeciwko osobie, która występowała w charakterze podejrzanego, na mocy postanowienia prokuratora nadrzędnego nad tym, który wydał lub zatwierdził postanowienie o umorzeniu, tylko wtedy, gdy ujawnią się nowe istotne fakty lub dowody nieznane w poprzednim postępowaniu albo gdy zachodzi okoliczność określona w art. 11 § 3 kpk[77]. Drugi z kolei przepis uprawnia prokuratora generalnego do uchylenia prawomocnego postanowienia o umorzeniu postępowania przygotowawczego w stosunku do osoby, która występowała w charakterze podejrzanego, w razie stwierdzenia, że umorzenie postępowania było niezasadne. Nie dotyczy to jednak wypadku, w którym sąd utrzymał w mocy postanowienie o umorzeniu. W obu sytuacjach wznowienie postępowania albo nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego łączy się ze wzruszeniem (uchyleniem – dop. red.) prawomocnej decyzji o umorzeniu postępowania karnego przeciwko osobie (*ad personam*)[78]. Okres zawieszenia w czynnościach służbowych funkcjonariusza ABW albo AW – zawieszonego na podstawie art. 58 ust. 1 u.a.b.w.a.w., po przedłużeniu tego okresu, zgodnie z ust. 3 tego artykułu – nie może trwać dłuższej niż do dnia uprawomocnienia się orzeczenia wydanego w postępowaniu karnym.

Uprawomocnienie się decyzji procesowej w postępowaniu karnym skutkuje tym, że odpada podstawa zawieszenia w czynnościach służbowych, a decyzja w przedmiocie zawieszenia staje się bezprzedmiotowa. Przestaje ona wywoływać skutki prawne,

---

[76] Po prawomocnym umorzeniu postępowania przygotowawczego prokurator nie dysponuje już prawem do skargi publicznej i nie może go odzyskać w sposób dorozumiany w drodze kontynuowania czynności procesowych w ramach dotychczasowego postępowania lub ich przeprowadzenia w innym postępowaniu. Wyjątek stanowią instytucje przewidziane w art. 327 § 1 i 2 kpk oraz art. 328 kpk (wyrok SN – Izba Karna z 9 X 2008 r., V KK 252/08, Legalis nr 303197; wyrok SA w Poznaniu – II Wydział Karny z 27 II 2019 r., II AKa 6/19, Legalis nr 2107325; postanowienie SA w Katowicach z 27 VII 2011 r., II AKz 416/11, Legalis nr 402576).

[77] Zgodnie z tym przepisem postępowanie umorzone na podstawie art. 11 § 1 kpk można wznowić w wypadku uchylenia lub istotnej zmiany treści prawomocnego wyroku, z powodu którego zostało ono umorzone.

[78] „Wznowieniu podlega tylko postępowanie, które zostało umorzone prawomocnym postanowieniem prokuratora o umorzeniu postępowania przeciwko osobie (*in personam)*. Prawomocność postanowienia następuje z chwilą wydania, gdy ustawa uznaje je za niezaskarżalne lub wówczas, gdy nie podlega ono już zaskarżeniu. W innym przypadku postanowienie o umorzeniu postępowania przygotowawczego staje się prawomocne po upływie terminu do wniesienia zażalenia lub po nieuwzględnieniu wniesionego zażalenia. W przypadku wydania zarządzenia o odmowie przyjęcia zażalenia z uwagi na fakt, iż zostało ono złożone po terminie lub przez osobę nieuprawnioną albo z uwagi na jego niedopuszczalność z mocy ustawy (art. 429 § 1 kpk), zaskarżone postanowienie staje się prawomocne nie wcześniej, niż z dniem uprawomocnienia się zarządzenia o odmowie przyjęcia tego środka odwoławczego lub postanowienia o pozostawieniu go bez rozpoznania". Zob. Z. Brodzisz, *Komentarz do art. 327*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el., teza 13.

zniknęła bowiem przyczyna, dla której zawieszono funkcjonariusza w czynnościach służbowych – zakończono postępowanie karne przeciwko osobie. Z chwilą uprawomocnienia się decyzji procesowej o umorzeniu postępowania karnego nie można już wskazać, aby się ono toczyło, a także aby było skierowane do konkretnej osoby, która miałaby przymiot strony postępowania karnego (podejrzanego). Wznowienie uprzednio umorzonego postępowania karnego prowadzonego przeciwko danemu funkcjonariuszowi ABW albo AW albo nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego nie może z mocy prawa aktywować poprzedniego zawieszenia w czynnościach służbowych. Żaden przepis pragmatyki służbowej nie przewiduje takiej możliwości. Wznowienie postępowania karnego albo nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego przeciwko funkcjonariuszowi ABW albo AW o przestępstwo umyślne ścigane z oskarżenia publicznego powinno jednak obligować do zawieszenia danego funkcjonariusza w czynnościach służbowych z uwagi na zmaterializowanie się przesłanki określonej w art. 58 ust. 1 u.a.b.w.a.w. Nie jest to jednak kontynuacja poprzedniego zawieszenia w czynnościach służbowych, ale nowe zawieszenie w czynnościach służbowych wskutek zainicjowania postępowania karnego przeciwko funkcjonariuszowi ABW albo AW.

Sformułowanie użyte w art. 58 ust. 1 u.a.b.w.a.w. – „wszczęcie postępowania karnego" – powinno być odniesione do każdego sposobu, który powoduje zainicjowanie postępowania karnego przeciwko danej osobie, a więc takiego, które jest związane nie tylko z przedstawieniem zarzutów danej osobie, wniesieniem wobec niej subsydiarnego aktu oskarżenia, lecz także ze wznowieniem wobec niej prawomocnie umorzonego postępowania karnego albo z nadzwyczajnym uchyleniem prawomocnego postanowienia o umorzeniu postępowania przygotowawczego. Należy również podkreślić, że wznowienie (zgodnie z art. 327 § 2 kpk) i nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego (art. 328 § 1 kpk) inicjują postępowanie przeciwko tej samej osobie, wobec której uprzednio prowadzono postępowanie karne, wcześniej już umorzone. Tę tezę potwierdza również Naczelny Sąd Administracyjny, który w wyroku z 16 października 2009 r., I OSK 167/09[79], wskazał, że w sformułowaniu „w razie wszczęcia przeciwko niemu postępowania karnego" istotne znaczenie ma aspekt uruchomienia w sprawach karnych procedury *ad personam*. W kontekście przesłanki zwartej w art. 58 ust. 1 u.a.b.w.a.w. wszczęcie postępowania karnego niewątpliwie należy więc odnieść do każdego sposobu zainicjowania postępowania karnego przeciwko funkcjonariuszowi ABW albo AW w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego.

Zgodnie natomiast z § 3 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie przebiegu służby funkcjonariuszy ABW, a także § 3 ust. 4 w zw. z § 3 ust. 1 pkt 5 rozporządzenia Prezesa Rady Ministrów w sprawie przebiegu służby funkcjonariuszy AW

[79] Legalis nr 212027 (dotyczy policjanta), w tym samym tonie wyrok WSA w Warszawie z 15 VII 2020 r., II SA/Wa 1929/19, Legalis nr 2500402.

w sprawach nieuregulowanych pragmatyką służbową oraz tymi rozporządzeniami, dotyczącymi m.in. zawieszenia w czynnościach służbowych, stosuje się przepisy *Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego*[80]. Tym samym zagadnienie odnoszące się do obligatoryjnego zawieszenia w czynnościach służbowych wytycza granice konkretnej sprawy administracyjnej[81].

Zawieszenie w czynnościach służbowych, które następuje w związku ze zmianą stadium postępowania z *in rem* w *ad personam* w wyniku przedstawienia zarzutów nie jest tą samą sprawą administracyjną dotyczącą zawieszenia w czynnościach służbowych wskutek wniesienia subsydiarnego aktu oskarżenia, wznowienia postępowania karnego albo nadzwyczajnego uchylenia prawomocnego postanowienia o umorzeniu postępowania przygotowawczego przeciwko tej samej osobie. Przy ocenie tożsamości spraw administracyjnych należy brać pod uwagę zarówno elementy podmiotowe, jak i przedmiotowe. Istotne jest jednak to, że te elementy muszą być relewantne dla przedmiotu danej sprawy[82]. W obu przypadkach podmiot, tj. funkcjonariusz ABW albo AW, jest tożsamy, tak samo jak przedmiot postępowania karnego, tj. przestępstwo umyślne ścigane z oskarżenia publicznego. Różnicującym obie sprawy administracyjne jest jednak ten element, który w jednej sprawie skutkuje zmianą stadium postępowania z *in rem* w *ad personam* (przedstawienie zarzutów), w drugiej natomiast od razu inicjuje postępowanie przeciwko danej osobie (postanowienie o wznowieniu postępowania karnego albo o nadzwyczajnym uchyleniu prawomocnego postanowienia o umorzeniu postępowania przygotowawczego). W sytuacji wznowienia postępowania karnego materializuje się więc przesłanka do obligatoryjnego zawieszenia w czynnościach służbowych, o której mowa w art. 58 ust. 1 u.a.b.w.a.w., niezależnie od poprzednio zmaterializowanej przesłanki do obligatoryjnego zawieszenia w czynnościach służbowych w wyniku przedstawienia zarzutów. To zawieszenie może być również przedłużone na dalszy czas oznaczony, nie dłuższy niż do dnia uprawomocnienia się orzeczenia wydanego w postępowaniu karnym, jeśli zaistnieją ku temu przesłanki wskazane w art. 58 ust. 3 u.a.b.w.a.w. Nie ma przy tym znaczenia, że w sprawie o to samo przestępstwo umyślne ścigane z oskarżenia publicznego funkcjonariusz ABW albo AW był już zawieszony w czynnościach służbowych w związku z przedstawieniem mu zarzutów, a także to, że zawieszenie przedłużono do dnia uprawomocnienia się orzeczenia wydanego w postępowaniu karnym umarzającego to postępowanie. Umorzenie tego

[80] Tekst jednolity: DzU z 2021 r. poz. 735 , ze zm.

[81] Sprawa administracyjna występuje wtedy, gdy o prawach lub obowiązkach, wynikających z przepisów prawa administracyjnego (przedmiot), indywidualnie określonego podmiotu ma rozstrzygnąć upoważniony do tego organ administracyjny, w określonej prawem formie – decyzji administracyjnej. Zob. R. Suwaj, *Wydanie decyzji administracyjnych*, Wrocław 2011, s. 20.

[82] Stan faktyczny sprawy musi być brany pod uwagę przy ocenie tożsamości sprawy, lecz tylko w odniesieniu do faktów prawotwórczych. Elementy prawnie obojętne, niewpływające w żaden sposób na załatwienie sprawy, powinny być pominięte w tej ocenie. Zob. G. Łaszczyca, C. Marzysz, A. Matan, *Postępowanie administracyjne ogólne*, Warszawa 2003, s. 821; także: B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2017, s. 880 i nast.

postępowania spowodowało odpadnięcie podstawy tego (pierwotnego) zawieszenia. Wznowienie tego samego postępowania karnego albo nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego zmaterializowało natomiast przesłankę z art. 58 ust. 1 u.a.b.w.a.w., ponieważ to wznowienie albo nadzwyczajne uchylenie prawomocnego postanowienia o umorzeniu postępowania przygotowawczego nie stanowi tej samej sprawy administracyjnej z tą, która była podstawą poprzedniego (pierwotnego) zawieszenia w czynnościach służbowych[83]. Analogicznie jest w sytuacji omawianego wcześniej subsydiarnego aktu oskarżenia. Możliwość jego wniesienia materializuje się dla pokrzywdzonego po prawomocnym zakończeniu postępowania karnego albo prawomocnej decyzji procesowej odmawiającej jego wszczęcia. W tym przypadku relewantnym elementem statuującym odrębną sprawę administracyjną jest skuteczne wniesienie subsydiarnego aktu oskarżenia do sądu, z tą chwilą bowiem zostaje zainicjowane postępowanie jurysdykcyjne przeciwko indywidualnie określonej osobie.

Podmiot, o którym mowa w art. 50 ust. u.a.b.w.a.w., nie może badać, czy zostały spełnione przesłanki do wznowienia postępowania karnego albo nadzwyczajnego uchylenia prawomocnego postanowienia o umorzeniu postępowania przygotowawczego, nie ustala, czy zaistniały podstawy do wydania takiego postanowienia, ale uwzględnia jego wydanie przez podmiot wskazany w art. 327 § 2 kpk albo w art. 328 § 1 kpk. W tym aspekcie decyzja o zawieszeniu w czynnościach służbowych ma charakter związany, ponieważ obliguje do takiego zawieszenia w związku ze wznowieniem postępowania karnego albo nadzwyczajnym uchyleniem prawomocnego postanowienia o umorzeniu postępowania przygotowawczego przeciwko funkcjonariuszowi ABW albo AW.

Uwagi końcowe

Służba w formacji, jaką jest ABW albo AW, ma szczególny charakter, ponieważ te formacje stanowią służby specjalne, a co za tym idzie, są one zobowiązane do realizowania zadań istotnych z punktu widzenia bezpieczeństwa państwa i jego porządku konstytucyjnego. Tak ważne zadania mogą wykonywać wyłącznie funkcjonariusze mający nie tylko odpowiednie kwalifikacje zawodowe, lecz także wykazujący właściwą postawę etyczno-moralną. Z kolei podejrzenie o zachowanie sprzeczne z przepisami prawa determinuje przynajmniej czasowe odsunięcie takiego funkcjonariusza od wykonywania zadań (czynności służbowych). Sprzyja temu konstrukcja prawna zawieszenia

[83] „Dopuszczalne jest natomiast ponowne uruchomienie przedmiotowej procedury, jeżeli odpadła dotychczasowa podstawa zawieszenia policjanta w czynnościach służbowych. Orzeczenie o zawieszeniu z powodu wszczęcia określonego postępowania karnego wygasa między innymi z powodu prawomocnego zakończenia tego postępowania. Nie stanowi to jednak przeszkody do ponownego obligatoryjnego zawieszenia w czynnościach służbowych, w trybie art. 39 ust. 1 ustawy o Policji, gdy prawomocnie zakończone postępowanie karne zostanie podjęte na nowo". Zob. wyrok NSA z 16 X 2009 r., I OSK 167/09.

w czynnościach służbowych. Jak wynika wprost z art. 58 ust. 3 u.a.b.w.a.w., zawieszenie w czynnościach służbowych polega na odsunięciu funkcjonariusza od wykonywania obowiązków służbowych. Z uwagi na znaczenie naruszenia przepisów prawa ustawodawca dokonał wyodrębnienia przesłanek, które obligują do zawieszenia w czynnościach służbowych oraz uprawniających do zastosowania tej instytucji.

Trudno byłoby jednak – w ramach jednego opracowania – odnieść się do wszystkich aspektów związanych z konstrukcją prawną zawieszenia w czynnościach służbowych. Dlatego też ograniczono się do dokonania analizy przesłanki zamieszczonej w art. 58 ust. 1 u.a.b.w.a.w., której zmaterializowanie się zobowiązuje do zawieszenia funkcjonariusza w czynnościach służbowych. Zawieszenie w czynnościach służbowych jest obligatoryjne w razie wszczęcia przeciwko funkcjonariuszowi ABW albo AW postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Spełnienie się tej przesłanki wyklucza zatem możliwość odstąpienia przez szefa ABW albo AW od zastosowania tego instrumentu prawnego wobec funkcjonariusza, przeciwko któremu takie postępowanie jest prowadzone. Decyzja w tym zakresie ma charakter związany, a nie uznaniowy, jak to ma miejsce w sytuacji zmaterializowania się którejkolwiek z przesłanek zamieszczonych w art. 58 ust. 2 u.a.b.w.a.w.

Analiza sformułowania „wszczęcie postępowania karnego przeciwko funkcjonariuszowi", użytego w tekście przepisu art. 58 ust. 1 u.a.b.w.a.w., nie pozostawia wątpliwości, że zostaje ono wypełnione, jeśli tylko zostanie zainicjowane postępowanie karne przeciwko funkcjonariuszowi ABW albo AW o przestępstwo umyślne ścigane z oskarżenia publicznego. Nieistotne jest przy tym, w jaki sposób zostaje ono zainicjowane *ad personam*. Nastąpi to w kilku sytuacjach: 1) zmiany stadium postępowania przygotowawczego z *in rem* w *ad personam* w związku z przedstawieniem zarzutów (i to już od chwili sporządzenia postanowienia o przedstawieniu zarzutów, jeśli między tą czynnością a pozostałymi czynnościami dopełniającymi instytucję przedstawienia zarzutów, tj. ogłoszeniem zarzutów podejrzanemu i przesłuchaniem go w tym charakterze, zaistnieje pewien okres, tzn. gdy nie są wykonywane w tym samym czasie), 2) skutecznego wniesienia do sądu subsydiarnego aktu oskarżenia, 3) wstąpienia oskarżyciela publicznego (prokuratora) do już wszczętego postępowania przed sądem, zainicjowanego przez oskarżyciela prywatnego, w sprawie z oskarżenia prywatnego (z chwilą tego wstąpienia tryb prywatnoskargowy zmienia się w publicznoskargowy), 4) w momencie wydania postanowienia o wznowieniu postępowania karnego, o którym mowa w art. 327 § 2 kpk, oraz o nadzwyczajnym uchyleniu prawomocnego postanowienia o umorzeniu postępowania przygotowawczego, o którym mowa w art. 328 § 1 kpk. Przepis art. 58 ust. 1 u.a.b.w.a.w. wymaga wyłącznie wszczęcia postępowania karnego przeciwko funkcjonariuszowi ABW albo AW o przestępstwo umyślne ścigane z oskarżenia publicznego. Nie warunkuje natomiast zmaterializowania się przesłanki zawartej w art. 58 ust. 1 u.a.b.w.a.w. od określonego podmiotu, który inicjuje postępowanie karne przeciwko funkcjonariuszowi ABW albo AW (mającemu uprawnienie do wniesienia i popierania skargi). Może nim być więc oskarżyciel publiczny (tj. prokurator – i tak jest w większości przypadków), ale może nim być również oskarżyciel posiłkowy (gdy wnosi subsydiarny akt oskarżenia). Istotne jest

bowiem to, czy w danym przypadku zostało zainicjowane postępowanie karne przeciwko osobie, a także czy jego przedmiotem jest przestępstwo umyślne ścigane z oskarżenia publicznego. Szef ABW albo AW jest zobligowany do ustalenia, czy w danym przypadku postępowanie karne zostało zainicjowane przeciwko funkcjonariuszowi ABW albo AW, a także czy jego przedmiotem jest czyn wypełniający znamiona przestępstwa umyślnego ściganego z oskarżenia publicznego. Nie może on natomiast kwestionować ustaleń dokonanych w postępowaniu karnym, a zwłaszcza przyjętej kwalifikacji prawnej czynu. Jest on związany decyzjami procesowymi wydanymi w postępowaniu karnym i zobligowany wyłącznie do ich uwzględnienia w prowadzonym postępowaniu administracyjnym w sprawie zawieszenia w czynnościach służbowych funkcjonariusza ABW albo AW.

Treść przepisu art. 58 ust. 1 u.a.b.w.a.w., co wynika z niniejszego opracowania, może budzić, a w niektórych przypadkach budzi uzasadnione wątpliwości. Dotyczy to zarówno ustalenia, czy umyślne przestępstwa skarbowe stanowią podstawę do obligatoryjnego zawieszenia w czynnościach służbowych funkcjonariusza ABW albo AW, czy też – z uwagi na kształt regulacji zawartej w art. 39 ust. 1 ustawy o Policji – nie są objęte treścią przepisu art. 58 ust. 1 u.a.b.w.a.w. Te same wątpliwości mogą nasuwać się w odniesieniu do sformułowania „wszczęcie postępowania karnego" użytego w wymienionym przepisie. Wydaje się zasadne postulowanie *de lege ferenda* rozważenia przez ustawodawcę możliwości uzupełnienia przepisu art. 58 ust. 1 u.a.b.w.a.w. o przestępstwa skarbowe, a także zmianę formuły tego przepisu. W ten sposób zostałaby wyeliminowana możliwość dokonywania wielości ocen, które są skutkiem odnoszenia wprost do pragmatyki służbowej instytucji ukształtowanych na gruncie odmiennej regulacji, jaką są przepisy procedury karnej.

Wymienione regulacje służą natomiast zgoła odmiennym celom. Celem zawieszenia w czynnościach służbowych, o którym mowa w art. 58 u.a.b.w.a.w., jest możliwie jak najszybsze odsunięcie funkcjonariusza od wykonywania przez niego czynności służbowych. Zadania realizowane przez służby specjalne są na tyle wrażliwą materią, że nie mogą zostać zakwestionowane z powodu okoliczności dotyczących danego funkcjonariusza ABW albo AW, w których (na skutek działań podjętych przez organy procesowe) się znalazł. Czynności wykonywane przez funkcjonariuszy ABW albo AW mogą bowiem ingerować bardzo głęboko w prawa i wolności obywatelskie. Stąd też konieczność przynajmniej czasowego odsunięcia od ich wykonywania funkcjonariusza, który znalazł się w kręgu podejrzeń o popełnienie umyślnego przestępstwa ściganego z oskarżenia publicznego. Decyzja procesowa, tj. postanowienie o przedstawieniu zarzutów, wydana na podstawie art. 313 § 1 kpk przez uprawniony do tego podmiot (prokuratora), musi być poparta materiałem dowodowym zebranym w sprawie. Jest to gwarancja tego, że istnieje dostatecznie uzasadnione podejrzenie w odniesieniu do konkretnej osoby, tj. wyższy stopień podejrzenia (niż wynikający z art. 303 kpk), zarówno w odniesieniu do faktu popełnienia samego przestępstwa, jak i do osoby sprawcy. Uzasadnieniem zawieszenia nie jest zatem ustalenie, że określona osoba popełniła przestępstwo, lecz to, że zebrane dowody wskazują na wysokie prawdopodobieństwo popełnienia przestępstwa przez tę osobę.

Ustalenie (stwierdzenie), że konkretna osoba popełniła przestępstwo, następuje w wydanym przez sąd wyroku, ale takie orzeczenie skutkuje koniecznością zastosowania innego instrumentu prawnego przewidzianego w pragmatyce służbowej, jakim jest zwolnienie ze służby. Z kolei znalezienie się przez funkcjonariusza w kręgu podejrzeń (co potwierdza wydane wobec niego postanowienie o przedstawieniu zarzutów) stanowi uzasadnienie dla czasowego odsunięcia go od wykonywania zadań i czynności służbowych. Instytucja ta chroni interes służby, nawet w sytuacji, gdy zarzuty nie zostaną potwierdzone, a postępowanie karne zostanie zakończone umorzeniem albo uniewinnieniem funkcjonariusza. Zastosowana ochrona ma charakter prewencyjny, zanim szef ABW albo AW zdobędzie pełną wiedzę o sytuacji, w jakiej znalazł się jego podwładny, a co za tym idzie, zanim będzie wiedzieć, czy wskutek tych okoliczności istnieje ryzyko naruszenia dobra prawnego, jakim jest interes służby, albo czy jest ono w ogóle zagrożone. Prokurator może bowiem odmówić we wstępnej fazie prowadzonego postępowania jakichkolwiek informacji o materiale dowodowym zebranym przeciwko funkcjonariuszowi. Dlatego też już sama informacja o wszczęciu postępowania karnego przeciwko funkcjonariuszowi ABW albo AW o umyślne przestępstwo ścigane z oskarżenia publicznego jest podstawą do zawieszenia funkcjonariusza w czynnościach służbowych (do odsunięcia go od wykonywania obowiązków służbowych). Informacje o sytuacji procesowej funkcjonariusza uzyskane w późniejszym czasie mogą nie potwierdzać, że istnieje zagrożenie dla tego dobra prawnego (dobra służby). Stąd też czasowy charakter zawieszenia w czynnościach służbowych, a także fakultatywny charakter przedłużenia jego okresu (art. 58 ust. 3 u.a.b.w.a.w.).

Należy też rozważyć, czy uruchomienie postępowania karnego przeciwko funkcjonariuszowi ABW albo AW na skutek wniesienia subsydiarnego aktu oskarżenia nie powinno – wzorem ustawy o Policji – statuować odrębnej i fakultatywnej przesłanki umożliwiającej zawieszenie funkcjonariusza ABW albo AW w czynnościach służbowych. Ocena prokuratora, w kontekście zebranego w sprawie materiału dowodowego jako podstawy do sporządzenia postanowienia o przedstawieniu zarzutów, jest bardziej miarodajna i obiektywna niż oskarżyciela posiłkowego subsydiarnego, który może nie mieć stosownej wiedzy w tym zakresie i może kierować się pobudkami stricte emocjonalnymi, a nie merytorycznymi, inicjując postępowanie przeciwko danej osobie.

Bibliografia

Adamiak B., Borkowski J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2017, C.H. Beck.

Brodzisz Z., *Komentarz do art. 309*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Brodzisz Z., *Komentarz do art. 313*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Brodzisz Z., *Komentarz do art. 325g*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Brodzisz Z., *Komentarz do art. 327*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Dziergawka A., *Subsydiarny akt oskarżenia w świetle nowelizacji dokonanej ustawą z dnia 19 lipca 2019 r.*, „Prokuratura i Prawo" 2020, nr 1, s. 152–170.

Gacek P., *Nawiązanie stosunku służbowego z funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Charakter prawny mianowania – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2020, nr 22, s. 98–119.

Gacek P., *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56–86.

Gardocki L., *Prawo karne*, Warszawa 1999, C.H. Beck.

Golik C., *Moment procesowej skuteczności przedstawienia zarzutów w sposób uproszczony*, „Prokuratura i Prawo" 2020, nr 2, s. 16–30.

Golik C., *Problem dopuszczalności uzupełnienia lub zmiany zarzutów w sposób uproszczony*, „Iustitia" 2014, nr 2, s. 81–92.

Grzegorczyk T., Tylman J., *Polskie postępowanie karne*, Warszawa 2007, LexisNexis.

Grześkowiak A., *Komentarz do art. 8 – Strona podmiotowa przestępstwa*, w: *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, Legalis/el.

Jaworski S., *Pełnomocnik w sprawie z subsydiarnego aktu oskarżenia*, w: *Metodyka pracy adwokata i radcy prawnego w sprawach karnych*, Warszawa 2020, Legalis/el.

Kociemba A., *Wniesienie subsydiarnego aktu oskarżenia po terminie a skutki wstąpienia prokuratora*, „n.ius", 22 I 2021 r., Legalis/el.

Korcyl-Wolska M., *Postępowanie przygotowawcze*, w: *Postępowanie karne. Przebieg*, A.R. Światłowski (red.), Warszawa 1999, C.H. Beck.

Kosonoga J., *Instytucja skargi subsydiarnej – zarys problematyki*, „Monitor Prawniczy" 2006, nr 9, Legalis/el.

Kosonoga J., *Komentarz do art. 276*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Kotowski W., *Podstawa wniesienia subsydiarnego aktu oskarżenia*, „n.ius", 4 III 2021 r., Legalis/el.

Kotowski W., *Uprawnienie do złożenia subsydiarnego aktu oskarżenia*, „n.ius", 19 II 2021 r., Legalis/el.

Kuczyński T., Mazurczak-Jasińska E., Stelina J., *Stosunek służbowy*, seria: System Prawa Administracyjnego, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011, C.H. Beck.

Łaszczyca G., Marzysz C., Matan A., *Postępowanie administracyjne ogólne*, Warszawa 2003, C.H. Beck.

Nowikowska M., *Komentarz do art. 39*, w: *Ustawa o Policji. Komentarz*, K. Chałubińska-Jentkiewicz, J. Kurek (red.), Warszawa 2021, Legalis/el.

Opaliński B., *Przedmowa do rozdziału 1*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el.

Porębska A., Graczyk P., *Subsydiarny akt oskarżenia – wybrane zagadnienia proceduralne*, w: *Problemy współczesnego prawa karnego. Część pierwsza*, B. Bieńkowska, Z. Jędrzejewski (red.), 2016, Legalis/el.

Prusak F., *Postępowanie karne*, Warszawa 2001, Wyższa Szkoła Handlu i Prawa im. Ryszarda Łazarskiego w Warszawie.

Rogalski M., *Komentarz do art. 2*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el.

Suwaj R., *Wydanie decyzji administracyjnych*, Wrocław 2011, Wydawnictwo PRESSCOM.

Szołucha S., *Komentarz do art. 60*, w: *Kodeks postępowania karnego. Komentarz*, J. Skorupka (red.), Warszawa 2020, Legalis/el.

Szustakiewicz P., *Komentarz do art. 58*, w: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis/el.

Szyprowski B., *Dochodzenie w niezbędnym zakresie jako faktyczne wszczęcie postępowania przygotowawczego*, „Prokuratura i Prawo" 2006, nr 11, s. 140–167.

Waltoś S., *Proces karny. Zarys systemu*, Warszawa 2003, LexisNexis.

Waltoś S., Hofmański P., *Proces karny. Zarys systemu*, Warszawa 2018, Wolters Kluwer Polska.

Wieczorek M., *Charakter prawny stosunków służbowych funkcjonariuszy służb mundurowych*, Toruń 2017, Wydawnictwo Adam Marszałek.

Zagrodnik J., *Postępowanie przygotowawcze*, w: *Proces karny. Przebieg postępowania*, K. Marszał (red.), Katowice 2012, WOLUMEN.

Zagrodnik J., *Udział prokuratora w postępowaniu sądowym na podstawie art. 55 § 4 kodeksu postępowania karnego*, „Prokuratura i Prawo" 2005, nr 3, 58–73.

Zagrodnik J., *Udział prokuratora w postępowaniu sądowym wszczętym przez oskarżyciela posiłkowego subsydiarnego*, „Prokuratura i Prawo" 2017, nr 2, s. 5–17.

Zgoliński I., *Udział prokuratora w postępowaniu karnym inicjowanym posiłkowym aktem oskarżenia – zarys problematyki*, „Iustitia" 2013, nr 2, 83–85.

Akty prawne

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j.: DzU z 2020 r. poz. 27, ze zm.).

Ustawa z dnia 10 września 1999 r. – Kodek karny skarbowy (t.j.: DzU z 2021 r. poz. 408, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j.: DzU z 2021 r. poz. 534, ze zm.).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j.: DzU z 2021 r. poz. 1486, ze zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j.: DzU z 2021 r. poz. 1882).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j.: DzU z 2021 r. poz. 735, ze zm.).

Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (t.j.: DzU z 2017 r. poz. 1206, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 28 listopada 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Wywiadu (DzU z 2003 r. nr 210 poz. 2039, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 2 lipca 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego (t.j.: DzU z 2013 r. poz. 862, ze zm.).

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z 19 X 2004 r., K 1/04, Legalis nr 65688.

Wyrok Trybunału Konstytucyjnego z 2 IV 2001 r., SK 10/00, Legalis nr 49670.

Postanowienie Sądu Najwyższego – Izba Karna z 9 X 2020 r., IV KK 268/19, Legalis nr 2508657.

Postanowienie Sądu Najwyższego – Izba Karna z 3 IX 2020 r., III KK 194/20, Legalis nr 2533735.

Postanowienie Sądu Najwyższego – Izba Karna z 2 IX 2020 r., V KK 355/19, Legalis nr 2539282.

Wyrok Sądu Najwyższego – Izba Karna z 4 VII 2019 r., III KK 273/18, Legalis nr 1973396.

Postanowienie Sądu Najwyższego – Izba Dyscyplinarna z 8 II 2019 r., I DO 18/18, Legalis nr 1872771.

Postanowienie Sądu Najwyższego – Izba Karna z 7 I 2019 r., III KK 69/18, Legalis nr 1861035.

Postanowienie Sądu Najwyższego – Izba Karna z 18 IV 2018 r., V KZ 12/18, Legalis nr 1835828.

Postanowienie Sądu Najwyższego – Izba Karna z 23 I 2018 r., IV KK 186/17, Legalis nr 1713813.

Postanowienie Sądu Najwyższego – Izba Karna z 9 II 2017 r., IV KK 299/16, Legalis nr 1587617.

Wyrok Sądu Najwyższego – Izba Karna z 12 XII 2016 r., V KK 243/16, Legalis nr 1565032.

Postanowienie Sądu Najwyższego – Izba Karna z 24 XI 2016 r., III KK 274/16, Legalis nr 1544282.

Wyrok Sądu Najwyższego – Izba Karna z 5 III 2015 r., III KK 414/14, Legalis nr 1231789.

Wyrok Sądu Najwyższego – Izba Karna z 5 III 2014 r., IV KK 341/13, Legalis nr 924802.

Wyrok Sądu Najwyższego – Izba Karna z 24 VI 2013 r., V KK 453/12, Legalis nr 712236.

Wyrok Sądu Najwyższego – Izba Karna z 2 VI 2010 r., V KK 376/09, Legalis nr 451571.

Postanowienie Sądu Najwyższego – Izba Karna z 16 I 2009 r., IV KK 256/08, Legalis nr 210120.

Wyrok Sądu Najwyższego – Izba Karna z 9 X 2008 r., V KK 252/08, Legalis nr 303197.

Wyrok Sądu Najwyższego – Izba Karna z 7 XI 2006 r., IV KK 150/06, Legalis nr 88729.

Postanowienie Sądu Najwyższego – Izba Karna z 22 VI 2001 r., III KKN 44/01, Legalis nr 52788.

Wyrok Sądu Apelacyjnego w Warszawie – II Wydział Karny z 22 XI 2019 r., II AKa 280/18, Legalis nr 2271634.

Postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z 5 VII 2019 r., II AKz 320/19, Legalis nr 2269222.

Wyrok Sądu Apelacyjnego w Poznaniu – II Wydział Karny z 27 II 2019 r., II AKa 6/19, Legalis nr 2107325.

Wyrok Sądu Apelacyjnego w Krakowie – II Wydział Karny z 10 XII 2018 r., II AKa 236/18, Legalis nr 2233118.

Wyrok Sądu Apelacyjnego w Katowicach z 12 X 2017 r., II AKa 244/17, Legalis nr 1809167.

Postanowienie Sądu Apelacyjnego w Katowicach – II Wydział Karny z 11 X 2017 r., II AKz 618/17, Legalis nr 1732966.

Wyrok Sądu Apelacyjnego w Szczecinie – II Wydział Karny z 23 V 2017 r., II AKa 48/17, Legalis nr 1683401.

Wyrok Sądu Apelacyjnego w Warszawie – II Wydział Karny z 18 I 2017 r., II AKa 436/15, Legalis nr 1692396.

Wyrok Sądu Apelacyjnego w Warszawie – II Wydział Karny z 18 I 2017 r., II AKa 436/16, Legalis nr 1588036.

Postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z 30 XI 2016 r., II AKz 395/17, Legalis nr 1594912.

Wyrok Sądu Apelacyjnego w Katowicach – II Wydział Karny z 18 IX 2015 r., II AKa 268/15, Legalis nr 1398816.

Wyrok Sądu Apelacyjnego w Katowicach – II Wydział Karny z 28 II 2014 r., II AKa 21/14, Legalis nr 1045021.

Postanowienie Sądu Apelacyjnego w Krakowie – II Wydział Karny z 27 III 2013 r., II AKz 97/13, Legalis nr 732815.

Postanowienie Sądu Apelacyjnego w Szczecinie – II Wydział Karny z 16 X 2012 r., II AKz 404/12, Legalis nr 680282.

Postanowienie Sądu Apelacyjnego we Wrocławiu – II Wydział Karny z 3 VIII 2011 r., II AKz 303/11, Legalis nr 424323.

Postanowienie Sądu Apelacyjnego w Katowicach z 27 VII 2011 r., II AKz 416/11, Legalis nr 402576.

Wyrok Sądu Apelacyjnego w Lublinie z 11 VIII 2009 r., II AKa 107/09, Legalis nr 242777.

Wyrok Sądu Okręgowego w Łodzi – V Wydział Karny z 14 III 2012 r., V KZ 148/12, Legalis nr 548065.

Wyrok Naczelnego Sądu Administracyjnego z 17 VII 2018 r., I OSK 19113/16, Legalis nr 1833570.

Wyrok Naczelnego Sądu Administracyjnego z 10 XI 2017 r., I OSK 70/16, Legalis nr 1710801.

Wyrok Naczelnego Sądu Administracyjnego z 3 II 2017 r., I OSK 1495/15, Legalis nr 1578651.

Wyrok Naczelnego Sądu Administracyjnego z 16 X 2009 r., I OSK 167/09, Legalis nr 212027.

Wyrok Naczelnego Sądu Administracyjnego z 3 X 2006 r., I OSK 210/06, Legalis nr 606379.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 15 VII 2020 r., II SA/Wa 1929/19, Legalis nr 2500402.

Wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z 5 VII 2018 r., III SA/Gd 335/18, Legalis nr 1810427.

Wyrok Wojewódzkiego Sądu Administracyjnego w Białymstoku z 21 I 2016 r., II SA/Bk 740/15, Legalis nr 1432094.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 27 X 2015 r., II SA/Wa 358/15, Legalis nr 1364493.

Wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 29 VII 2014 r., II SA/Po 273/14, Legalis nr 1104412.

Wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z 2 IV 2014 r., III SA/Gd 60/14, Legalis nr 953297.

Abstrakt

Artykuł został poświęcony problematyce związanej z przesłanką obligatoryjnego zawieszenia funkcjonariusza ABW albo AW w czynnościach służbowych. Ta regulacja jest zawarta w art. 58 ust. 1 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Zawieszenie w czynnościach służbowych jest obowiązkowe w przypadku wszczęcia postępowania karnego w sprawie o przestępstwo umyślne ścigane z oskarżenia publicznego. Uwagę skoncentrowano na sformułowaniu „wszczęcie postępowania karnego o przestępstwo umyślne ścigane z oskarżenia publicznego przeciwko funkcjonariuszowi ABW albo AW" jako na przesłance warunkującej zastosowanie konstrukcji prawnej zawartej w art. 58 ust. 1 ustawy o ABW i AW. Następuje to w sytuacji zmiany stadium postępowania przygotowawczego prowadzonego wobec funkcjonariusza ABW albo AW z *in rem* w *ad personam*, wniesienia subsydiarnego aktu oskarżenia do sądu, a także wznowienia postępowania karnego.

Słowa kluczowe: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, funkcjonariusz, służba, zawieszenie w czynnościach służbowych.

Initiation of criminal proceedings in the case of intent offence subject to a public accusation as a prerequisite of suspending an officer of the Internal Security Agency and the Foreign Intelligence Agency

Abstract

This paper is entirely devoted to the prerequisite of obligatory suspension of an officer of the Internal Security Agency or the Foreign Intelligence Agency. This regulation is included in the Article 58 sec. 1 of the Act on the Internal Security Agency and the Foreign Intelligence Agency. Suspension from official duties is obligatory in the event of an initiation of criminal proceedings in the case of an intent offence subjected to

a public accusation. Therefore, attention was focused on the wording: "initiation of criminal proceedings in the case of intent offence prosecuted with public accusation against an officer of the International Security Agency and the Foreign Intelligence Agency" as a condition enabling the use of the legal construct included in Article 58 sec. 1 of the Act on the International Security Agency and the Foreign Intelligence Agency. This happens in a situation of changing the phase of preparatory proceedings in the criminal case prosecuted against an officer of the International Security Agency or the Foreign Intelligence Agency from in rem to ad personam, submitting subsidiary indictment to the court and reopening of the criminal proceedings.

Keywords: The Internal Security Agency, the Foreign Intelligence Agency, an officer, service, suspension from official duties.

KRZYSZTOF IZAK
ORCID: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.027.14304

Dwadzieścia lat od ataku z 11 września 2001 roku. Przygotowania do ataku terrorystycznego na USA oraz jego przebieg i skutki

Al-Kaida, przeprowadzając 20 lat temu spektakularny atak terrorystyczny na Stany Zjednoczone, stała się pośrednio również sprawcą zmian w polityce wewnętrznej i zagranicznej USA oraz wielu innych państw na świecie. Dzień 11 września 2001 r. stał się datą przełomową w walce z terroryzmem, która nabrała niemal globalnego charakteru. Nigdy wcześniej rządy tak wielu państw na świecie nie udzieliły przynajmniej werbalnego wsparcia stronie zaatakowanej przez terrorystów, w tym przypadku USA. Tę międzynarodową jednomyślność można jednak uzasadnić kategorycznym stwierdzeniem prezydenta George'a W. Busha: *Kto nie z nami, ten przeciw nam.* Żaden kraj oficjalnie nie mógł sobie pozwolić na przypisanie mu poparcia dla terroryzmu, z wyjątkiem tzw. osi zła, do której prezydent Bush w swoim słynnym przemówieniu z 29 stycznia 2002 r. zaliczył: Irak, Iran i Koreę Północną. Nie było w niej Afganistanu, do którego Amerykanie wkroczyli w październiku 2001 r., ani Arabii Saudyjskiej, wspierającej od wielu lat islamskich ekstremistów (15 obywateli tego państwa znajdowało się w grupie 19 zamachowców, którzy zaatakowali wybrane cele w Nowym Jorku i Waszyngtonie). Konsekwencją tych ataków była amerykańska inwazja na Afganistan, a następnie na Irak. Natomiast pokłosiem tych wydarzeń było nasilenie się islamskiego terroryzmu trwającego do dziś. Terroryzm raz się wzmaga, raz słabnie, ale jest wciąż obecny i z pewnością będzie nam jeszcze długo towarzyszyć. W Stanach Zjednoczonych, aby usprawiedliwić niezamierzone, negatywne skutki własnych działań, opisano zaistniałą rzeczywistość, używając pojęcia z dziedziny ekonomii – „czarny łabędź", które odnosi się do sytuacji nieprzewidywalnej, niosącej za sobą poważne konsekwencje i wymykającej się prognozowaniu. W rzeczywistości można było jednak przewidzieć skutki tzw. wojny z terroryzmem. Przejęcie władzy przez talibów w Kabulu 15 sierpnia 2021 r. oraz wycofanie ostatnich amerykańskich żołnierzy z Afganistanu, 20 lat po ich wkroczeniu do tego

państwa, można postrzegać jako powrót do poprzedniej sytuacji, czyli do reaktywacji Islamskiego Emiratu Afganistanu[1].

Celem artykułu jest ukazanie złożonego procesu przygotowań do ataku na Stany Zjednoczone przeprowadzonego 11 września 2001 r., jego precyzyjnej realizacji i skutków, które doprowadziły do nieodwracalnych zmian w globalnej polityce. Zamachowcy samobójcy, którzy przeszli kursy pilotażu w USA, należeli do nowego pokolenia islamskich bojowników. W większości byli oni wykształconymi przedstawicielami klasy średniej o ustabilizowanej sytuacji materialnej. Celowe będzie więc poszukanie odpowiedzi na pytanie, co skłoniło ich do samobójczej operacji i zabicia kilku tysięcy niewinnych ludzi. Al-Kaida nie mogłaby planować i organizować tych ataków, gdyby nie dysponowała środkami finansowymi, urządzeniami umożliwiającymi komunikowanie się między sobą, a przede wszystkim schronieniem, w którym było możliwe przeprowadzenie szkoleń i odpowiednie inspirowanie młodych ludzi. Niewątpliwie to ta organizacja zapoczątkowała bieg wydarzeń, które doprowadziły do największego w historii ataku terrorystycznego. Istotne będzie również przedstawienie zdarzeń i towarzyszących im okoliczności, które mogłyby przeszkodzić w ataku z 11 września 2001 r. lub nawet częściowo go powstrzymać. W związku z tym autor postara się odpowiedzieć na pytanie, czy w ogóle można było przeciwdziałać tym prawie symultanicznym zamachom. Ich zwiastunem było dokonanie zaledwie dwa dni wcześniej zabójstwa lidera Zjednoczonego Frontu Muzułmańskiego na rzecz Wyzwolenia Afganistanu Ahmeda Szacha Masuda, najbardziej wiarygodnego przywódcy antytalibskiej opozycji, cieszącego się zaufaniem Zachodu[2]. Wyeliminowanie Masuda było elementem przygotowań do przewidywanego przez Al-Kaidę (jak się okazało – słusznie) odwetu wojsk USA w Afganistanie będącego odpowiedzią na atak na Stany Zjednoczone.

Osama bin Laden i przywódca talibów mułła Mohammad Omar nie mieli chyba wątpliwości co do tego, że podobnie jak afgańscy mudżahedini zniszczyli armię radziecką po dziesięciu latach wojny, ich bojownicy również poradzą sobie z siłami Stanów Zjednoczonych, jeśli dojdzie do inwazji. Autor artykułu zwraca uwagę na to, że

[1] Trwająca od maja 2021 r. ofensywa talibów nasiliła się na przełomie lipca i sierpnia 2021 r. Żołnierze Afgańskiej Armii Narodowej prawie bez walki oddawali kolejne duże miasta Afganistanu. W dniu 15 sierpnia talibowie zajęli Kabul. Tempo, w jakim to nastąpiło, było zaskoczeniem dla wielu obserwatorów. Prezydent Aszraf Ghani uciekł do Zjednoczonych Emiratów Arabskich. Tysiące ludzi, wśród których byli współpracownicy wojsk NATO, członkowie ich rodzin, przedstawiciele afgańskiej administracji, organizacji międzynarodowych i sił bezpieczeństwa, okupowało lotnisko w Kabulu, usiłując dostać się na pokład samolotów państw zachodnich, które podjęły się spóźnionej ewakuacji. Dla wielu z tych osób pozostanie w Afganistanie oznacza wyrok śmierci z rąk talibów.

[2] Zabójstwa Ahmeda Szacha Masuda dokonało dwóch młodych Marokańczyków posługujących się belgijskimi paszportami. Podając się za dziennikarzy, przybyli do Doliny Pandższeru (Panczsziru) w północno-wschodnim Afganistanie, stanowiącej bazę Masuda i dowodzonych przez niego bojowników, przez pięć lat bezskutecznie atakowanej przez talibów. W kamerze mieli ukrytą bombę, która wybuchła w momencie, gdy jeden z zamachowców nagrywał wywiad prowadzony przez drugiego rzekomego dziennikarza. Masud zmarł po kilku godzinach w wyniku odniesionych obrażeń.

prognoza Al-Kaidy okazała się w pełni słuszna, jednak dla administracji Białego Domu wysłanie wojsk do Afganistanu nie było tak oczywiste w pierwszym momencie po ataku. Poruszył też kwestię teorii spiskowych dotyczących ataku z 11 września 2001 r., które przez kilkanaście lat propagowano w mediach, filmach i publikacjach książkowych. Wywarły one duży wpływ na świadomość społeczeństwa amerykańskiego, którego znaczna część przyjęła alternatywną wersję wydarzeń.

Przy pisaniu artykułu autor posłużył się metodą historyczną, pozwalającą ukazać chronologiczny przebieg zdarzeń, które doprowadziły do przeprowadzenia czterech zamachów w dniu 11 września 2001 r. W pracy autor wykorzystał ponadto metodę behawioralną, polegającą na analizie zachowania poszczególnych uczestników antyamerykańskiego spisku, zarówno w momencie przygotowań do zamachów, jak i uprowadzenia samolotów. W artykule przedstawiono także skutki ataku terrorystycznego na USA – podano liczbę ofiar i wysokość strat materialnych.

Przygotowania do zamachu

Pomysłodawcą przeprowadzenia spektakularnego ataku terrorystycznego w USA był urodzony w Kuwejcie Chalid Szejk Mohammad[3], wuj Ramziego Jusufa[4], który odpowiadał za zamach bombowy na World Trade Center (WTC) w 1993 r.[5] Dwa lata później obaj obmyślili plan przeprowadzenia zamachów bombowych na 12 amerykańskich samolotów lecących z Azji do USA[6]. W 1996 r. Mohammad poznał w Afganistanie Osamę bin Ladena, któremu przedstawił różne pomysły na dokonanie ataków na Stany Zjednoczone, w tym operację lotniczą. W ciągu trzech kolejnych lat Al-Kaida analizowała możliwości zaatakowania USA. Jeden z planów ataku, autorstwa Chalida Szejka Mohammada, przewidywał porwanie dwóch grup samolotów: pięciu lecących ze

[3] Chalid Szejk Mohammad został aresztowany w marcu 2003 r. w Pakistanie. Obecnie przebywa w amerykańskim więzieniu. W 2019 r. Mohammad, chcąc uniknąć grożącej mu kary śmierci, złożył rodzinom ofiar ofertę współpracy. Obiecał, że będzie zeznawał na ich korzyść w procesie przeciwko Arabii Saudyjskiej. Jego proces jeszcze się nie zakończył.

[4] Ramzi Jusuf został aresztowany w lutym 1995 r. w Pakistanie. W 1998 r. amerykański sąd skazał go na karę dożywotniego więzienia za zamach na WTC z 26 lutego 1993 r. i podłożenie ładunku wybuchowego w samolocie lot nr 435 Philippines Airlines 11 grudnia 1994 r.

[5] W dniu 26 lutego 1993 r. w podziemnym garażu WTC eksplodował samochód ciężarowy wypełniony materiałem wybuchowym. Zginęło sześć osób, a kilkaset zostało rannych. Po zamachu Ramzi Jusuf wyjechał z USA.

[6] W ramach przygotowań do tej operacji (krypt. „Bojinka") 11 grudnia 1994 r. Ramzi Jusuf umieścił skonstruowany przez siebie ładunek wybuchowy w samolocie lecącym z Manili do Tokio. W wyniku eksplozji zginęła jedna osoba, a dziesięć zostało rannych. Samolot został poważnie uszkodzony, ale dzięki doświadczeniu załogi oraz niewielkiej odległości od Okinawy bezpiecznie wylądował. Ładunek użyty w tym ataku był kilkakrotnie słabszy od tych, które planowano wykorzystać w operacji „Bojinka". Atak na samoloty został pokrzyżowany przez przypadkowy pożar w pokoju hotelowym wynajmowanym przez terrorystów.

wschodniego wybrzeża USA i pięciu lecących z Azji do USA. Dziewięć z nich miało się rozbić o wybrane wcześniej cele, m.in. budynki CIA, FBI oraz elektrownie jądrowe. Mohammad zamierzał siąść za sterami dziesiątego samolotu, zabić wszystkich mężczyzn na pokładzie, a następnie wygłosić oświadczenie potępiające politykę USA na Bliskim Wschodzie, wylądować w bliżej nieokreślonym miejscu i uwolnić kobiety i dzieci. Tę ostatnią część planu Osama bin Laden stanowczo odrzucił, jednak wiosną 1999 r. wydał zezwolenie na przeprowadzenie takiej operacji. Jeszcze w tym samym roku w Kandaharze spotkali się szef Al-Kaidy, Chalid Szejk Mohammad i Muhammad Atef alias Abu Hafs al-Masri[7]. Celem tajnego spotkania było wybranie obiektów ataku mających symboliczne znaczenie dla USA, których zniszczenie spowodowałoby nie tylko jak największe szkody materialne, lecz przede wszystkim wizerunkowe. Nikt poza nimi nie brał udziału w naradzie, ale w gronie najbliższych współpracowników Osamy bin Ladena mówiło się o „operacji samoloty"[8].

Przywódca Al-Kaidy snuł wizję, że atak na tego typu cele mógłby doprowadzić do rozpadu państwa federalnego. Nic zatem dziwnego, że chciał zniszczyć Biały Dom i Kapitol. Na liście celów znalazł się także budynek Pentagonu. Gdyby udało się zniszczyć te obiekty, rozpad USA wcale nie byłby aż tak nierealną fantazją. Chalid Szejk Mohammad zaproponował ponadto wieżowce WTC, których jego siostrzeniec Ramzi Jusuf nie zdołał zburzyć w 1993 r. Dyskutowano też o wieżowcach Sears Tower w Chicago i Library Tower w Los Angeles. Bin Laden uznał, że ataki na te cele będzie można przeprowadzić później. Jak wspomniano, Bin Laden brał pod uwagę taką możliwość, że w odwecie Stany Zjednoczone wcześniej czy później zechcą uderzyć na Afganistan, gdzie wykrwawią się, podobnie jak ZSRR w latach 80. XX w. Nie wykluczał również, że po atakach USA ostatecznie wycofają wszystkie swoje siły z Bliskiego Wschodu, podobnie jak uczyniły to w Somalii po nieudanej próbie pojmania Mohammada Faraha Aidida na początku października 1993 r. W tej operacji zginęło 19 amerykańskich żołnierzy.

W 2001 r. Al-Kaida nie dysponowała dużą ilością pieniędzy, za to w jej szeregach było wielu młodych ludzi gotowych umrzeć męczeńską śmiercią. Gdyby plan obejmował tylko wysadzenie w powietrzu porwanych samolotów, nie byłoby potrzeby angażowania ludzi mających przeszkolenie w pilotowaniu samolotów. Tymczasem koncepcja ataku była bardziej skomplikowana, a do jego przeprowadzenia była potrzebna zdyscyplinowana grupa osób, z których część potrafiłaby pilotować samoloty. Bin Laden przydzielił Mohammadowi czterech swoich najbardziej niezawodnych ludzi. W grupie tej było dwóch Saudyjczyków: Nawaf al-Hazmi, Chalid al-Mihdar i dwóch Jemeńczyków: Zuhail Abdu Anam Said al-Szarabi alias Abu Bara i Taufik bin Attasz alias Challad. Do grupy dołączyli: Jemeńczyk Ramzi bin asz-Szibh (Asz-Szajba), Egipcjanin Muhammad Ata as-Sajjid, Libańczyk Zijad Dżarrah i Emiratczyk Marwan asz-Szihhi, którzy pod

[7] Były egipski policjant, członek Egipskiego Islamskiego Dżihadu, jeden z dowódców Al-Kaidy należący do najbardziej zaufanych doradców Osamy bin Ladena. Zginął podczas amerykańskich nalotów w Afganistanie w listopadzie 2001 r.

[8] S. Coll, *Rodzina Bin Ladenów. Arabskie losy w amerykańskim stuleciu*, Warszawa 2015, s. 435–436.

koniec 1999 r. przybyli z Niemiec do Afganistanu na spotkanie z Bin Ladenem. Poinformował on ich, że zostaną męczennikami, a do tego czasu nakazał im wrócić do Niemiec, a następnie lecieć do USA i tam zapisać się do szkół lotniczych[9]. Plany operacji z użyciem samolotów obejmowały dwa zespoły, z których każdy miał przeprowadzić atak dotkliwy dla wroga. Grupa z Niemiec zgłosiła kradzież lub zaginięcie paszportów, aby nie zwrócono uwagi na ich pobyt w Afganistanie. Później nazwano ją „komórką hamburską". Jej członkowie pochodzili z dobrze sytuowanych rodzin, studiowali nauki techniczne w Europie. Dżarrah i Asz-Szihhi byli inżynierami, Muhammad Ata architektem (w latach 1992–1999 studiował urbanistykę w Hamburgu), dzięki czemu łatwo mogli wmieszać się w amerykańskie społeczeństwo podczas szkoleń na pilotów. Od tej trójki odstawał pochodzący z niemajętnej rodziny i bez konkretnego zawodu Asz-Szibh, który jednak dobrze znał *Koran*. Natomiast żaden z nich nie miał za sobą wychowania w medresie, które przed 11 września 2001 r. często uznawano za źródło muzułmańskiego terroryzmu. Wszyscy uczęszczali do świeckich szkół, a Dżarrah przed przystąpieniem do grupy nie był nawet praktykującym muzułmaninem[10]. Grupie przewodził Muhammad Ata. Po skończeniu studiów wynajął w Hamburgu mieszkanie przy Marienstrasse 54. To właśnie tutaj zbierali się przyszli zamachowcy. Typowe dla komórki hamburskiej było prowadzenie działań w sposób niezauważalny dla osób z zewnątrz. Żaden z późniejszych zamachowców nie zwrócił na siebie uwagi jako fanatyczny wyznawca islamu. Mimo że Federalny Urząd Kryminalny chciał wszcząć śledztwo wobec członków grupy Aty, których przesłuchiwano w związku z podejrzanymi incydentami, Prokuratura Generalna nie wyraziła zgody na ich zatrzymanie, ponieważ nie było uzasadnienia dla żadnych działań prawnych lub wydania nakazu aresztowania. Muhammad Ata żył więc normalnie, nie ukrywał się, dużo podróżował i nawiązywał kontakty od Hamburga po Afganistan, co ułatwiło mu przeprowadzenie 11 września ataku terrorystycznego na wielką skalę[11].

Wspomniani wyżej Saudyjczycy, Nawaf al-Hazmi i Chalid al-Mihdar, nie mieli problemów z uzyskaniem amerykańskich wiz i z Kuala Lumpur przez Bangkok polecieli do Los Angeles, gdzie przybyli 15 stycznia 2000 r. Jemeńczycy, Abu Bara i Challad, nie otrzymali natomiast amerykańskich wiz (Challad był mózgiem ataku na niszczyciel USS „Cole" z 12 października 2000 r.[12]). Saudyjczykom, którzy w USA mieli zapisać się

[9] L. Wright, *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, s. 432–435.

[10] K. Armstrong, *Pola krwi. Religia i przemoc*, Warszawa 2017, s. 532–533.

[11] W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm*, Warszawa 2009, s. 150; A. Lichtenberg, B. Dudek, *Zamachy 11 września: historia „Grupy Hamburskiej"*, https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [dostęp: 12 IX 2011].

[12] W burtę okrętu zacumowanego w porcie w Adenie uderzyła łódź motorowa wypełniona materiałami wybuchowymi. Eksplozja spowodowała dziurę o średnicy 12 m i wiele innych poważnych uszkodzeń. Zginęło 17 marynarzy, a 39 zostało rannych. Atak na USS „Cole" nastąpił po podobnym, ale nieudanym, ataku na niszczyciel USS „The Sulivans", który cumował u wybrzeży Jemenu. Doszło do niego 3 stycznia 2000 r. Wówczas łódź wyładowana materiałami wybuchowymi zatonęła przed osiągnięciem celu.

do szkoły lotniczej, pomocy udzielił mieszkający w San Diego saudyjski stypendysta Omar Bajumi. Trzej członkowie grupy hamburskiej przybyli do USA w maju i czerwcu 2000 r., przy czym najpierw przyleciał jedynie Marwan asz-Szihhi, a następnie Muhammad Ata razem z Zijadem Dżarrahem. Ramzi bin asz-Szibh nie otrzymał amerykańskiej wizy, został więc łącznikiem między zamachowcami w USA i Al-Kaidą (obecnie przebywa w amerykańskim więzieniu). Asz-Szihhi i Dżarrah udawali ochroniarzy Aty, który z kolei wcielił się w rolę członka saudyjskiej rodziny królewskiej. Cała trójka udała się na Florydę i tam, w mieście Wenecja, pobierała lekcje pilotażu. Przyszli terroryści spędzili wiele godzin na symulatorze lotu Boeingiem 727 oraz latali małymi samolotami na Florydzie i w innych stanach. Największe postępy czynił Dżarrah, który w sierpniu 2000 r. uzyskał licencję na pilotowanie małych samolotów. Pod koniec tego roku rozpoczął szkolenie w zakresie pilotowania dużych odrzutowców. Opłaty za szkolenie wnosił Pakistańczyk Ali Abdul Aziz Ali alias Amar al-Baluczi za pośrednictwem Emirates Bank International. Pieniądze wpływały do Sun Trust Banku, w którym Muhammad Ata, Asz-Szihhi i Dżarrah założyli konta.

Pod koniec stycznia 2001 r. cała trójka musiała wylatać jeszcze więcej godzin, odbyć więcej ćwiczeń na symulatorach lotu wielkich samolotów pasażerskich (Boeing 747 i 767), a także poznać sposoby zabezpieczeń na lotniskach. Pobyt w USA przerywali wyjazdami do Europy, Afryki i na Bliski Wschód. Dżarrah sześć razy opuszczał Stany Zjednoczone, częściej niż jakikolwiek inny zamachowiec. Odwiedzał m.in. swoją dziewczynę w Niemczech. Muhammad Ata, Asz-Szihhi i Dżarrah latali również jako pasażerowie na liniach amerykańskich, co umożliwiło im poznanie stanu zabezpieczeń lotnisk. Podczas jednego z takich lotów rozpoznawczych z Nowego Jorku do Kaliforni Asz-Szihhi i Dżarrah wzbudzili zainteresowanie pracowników ochrony lotniska, ale nie zostali zatrzymani[13].

Z dużymi trudnościami przebiegało natomiast szkolenie lotnicze saudyjskich przyjaciół: Nawafa al-Hazmiego i Chalida al-Mihdara. W 1995 r. razem walczyli na Bałkanach po stronie bośniackich muzułmanów, a potem w Afganistanie wspierali talibów walczących z Sojuszem Północnym Ahmeda Szaha Masuda. W San Diego, gdzie zamieszkali od stycznia 2000 r., uczęszczali do meczetu, którego imamem był Anwar al-Awlaki[14]. W San Diego pobierali też lekcje latania, ale z powodu słabej znajomości języka angielskiego nie radzili sobie podczas zajęć praktycznych. Instruktor Rick Garza udzielił im sześciu lekcji na ziemi, zanim pozwolił im polecieć ze sobą jednosilnikowym samolotem Cessna. Mimo że Garza uznał ich za całkowicie niezdolnych do nauki latania, Saudyjczycy byli zainteresowani wyłącznie lataniem dużymi

[13] P.L. Bergen, *Osama bin Laden. Portret z bliska*, Warszawa 2007, s. 319.

[14] Anwar al-Awlaki był obywatelem USA jemeńskiego pochodzenia. W Stanach Zjednoczonych uległ religijnemu radykalizmowi i, według niektórych opinii, udzielał duchowego wsparcia sprawcom zamachów z 11 września. Swoje nauki popularyzował na stronie internetowej www.anwar-awlaki.com. Po wydaleniu z USA udał się do Jemenu. Tam został duchowym przywódcą Organizacji Al-Kaidy na Półwyspie Arabskim. Zginął 30 września 2001 r. w wyniku nalotu amerykańskiego samolotu bezzałogowego.

samolotami pasażerskimi. Zaoferowali dodatkowe pieniądze za taki kurs, co wzbudziło podejrzenia instruktora, który jednak nie poinformował o tym władz. Było jasne, że żaden z nich nie opanuje w sposób dostateczny umiejętności pilotowania[15]. W dniu 10 czerwca 2000 r. Al-Mihdar poleciał do Jemenu, aby odwiedzić żonę, co rozgniewało Chalida Szejka Mohammada, który nie chciał, aby Al-Hazmi został sam w Kalifornii. Mohammad zamierzał nawet odsunąć Al-Mihdara od przygotowywanej operacji, ale podobno nie zgodził się na to Bin Laden. Saudyjczyk wrócił do USA. We wrześniu Al-Mihdar wraz z Al-Hazmim zmienili adres. Przeprowadzili się do domu informatora FBI Abdusattara Szejka, który nie powiadomił służby o zamieszkaniu w jego domu osób podejrzanych. Po ataku na USS „Cole" 12 października 2000 r. premier Jemenu Abdul Karim al-Irjani poinformował, że Al-Mihdar był jednym z głównych strategów zamachu i w tym czasie przebywał w Jemenie[16]. Pod koniec 2000 r. Al-Mihdar udał się do Arabii Saudyjskiej, a na początku 2001 r. do Afganistanu, gdzie przebywał kilka miesięcy. Tu prawdopodobnie spotkał się z Bin Ladenem. Wyznaczono go na organizatora i koordynatora grupy porywaczy, którzy mieli sterroryzować załogi samolotów i pasażerów. W czerwcu 2001 r. Al-Mihdar wrócił do Arabii Saudyjskiej i najprawdopodobniej w tym kraju zebrał pozostałych zamachowców oraz przygotował ich do podróży do USA. Do Stanów Zjednoczonych zamachowcy przylatywali parami. Al-Mihdar bez problemu uzyskał amerykańską wizę w konsulacie USA w Dżuddzie i 4 lipca 2001 r. wylądował w Nowym Jorku[17].

Gdy Al-Mihdar przebywał na Bliskim Wschodzie, w grudniu 2000 r. Al-Hazmi spotkał się ze swoim rodakiem Hanim Handżurem. Był to jedyny z przyszłych terrorystów, który przebywał w USA bez związku z zamachem. Po raz pierwszy przybył on do USA w 1991 r. na kilkumiesięczny kurs języka angielskiego. Po powrocie do Arabii Saudyjskiej, gdzie mieszkał pięć lat, złożył podanie o pracę w Saudi Arabian Airlines, ale został odrzucony z powodu słabych ocen. Linia lotnicza zaproponowała, że rozważy jego podanie, jeśli uzyska licencję pilota komercyjnego w Stanach Zjednoczonych. Wrócił więc do USA. Licencję pilota odebrał (ze słabą oceną) w kwietniu 1999 r., po trzech latach szkolenia. Jego podanie w Saudi Arabian Airlines zostało ponownie odrzucone z powodu niskich ocen otrzymanych na egzaminie przed przyjęciem do pracy. Pod koniec 1999 r. miał poinformować rodzinę, że udaje się do ZEA w poszukiwaniu pracy. W rzeczywistości wyjechał do Afganistanu, ale w grudniu 2000 r. był już w USA. Zamieszkał w domu Abdusattara Szejka w San Diego. Tam ponownie rozpoczął trening latania, okazał się jednak kiepskim pilotem, a słaba znajomość specjalistycznego języka angielskiego w dziedzinie lotnictwa uniemożliwiła mu uzyskanie certyfikatu pilota zawodowego. Mimo to rozpoczął zaawansowane szkolenie na symulatorze lotu

[15] J. Elsässer, *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007, s. 232.

[16] *Piecing together the terrorist jigsaw*, „The Guardian", 15 X 2001 r., https://www.theguardian.com/world/2001/oct/15/worlddispatch.brianwhitaker [dostęp: 17 I 2001].

[17] L. Wright, *Wyniosłe wieże…*, s. 478.

w Mesa w stanie Arizona, dokąd przybył razem z Al-Hazmim. Na początku kwietnia 2001 r. obaj zamieszkali w Falls Church w Wirginii, w metropolii Waszyngtonu. W tym czasie nowym imamem meczetu Dar al-Hidżra w Waszyngtonie został wspomniany Al-Awlaki[18]. Tu dołączyli do nich rodacy: Madżid Moked i Ahmed al-Ghamdi, którzy przylecieli z Arabii Saudyjskiej. Wszyscy czterej udali się do Patterson w stanie Wirginia i wynajęli tam mieszkanie. Z Wirginii latali do różnych miast, sprawdzając systemy bezpieczeństwa na lotniskach. Kilkakrotnie podróżowali też do Las Vegas, aby się zabawić. W Patterson dołączył do nich Al-Mihdar, który wrócił z Bliskiego Wschodu. W lipcu Handżur, na podstawie poświadczenia fałszywego adresu zamieszkania, uzyskał amerykańskie prawo jazdy. Pod koniec czerwca 2001 r. do Nowego Jorku przybyli kolejni dwaj Saudyjczycy: Abdul Aziz al-Omari i Salem al-Hazmi. Przez kilka dni obaj przebywali w Patterson z innymi przyszłymi porywaczami. Tam Al-Omari i Al-Mihdar nabyli fałszywe dokumenty tożsamości. Kupili je podobno w All Services Plus, w hrabstwie Passaic w stanie New Jersey, firmie, która zajmowała się sprzedażą fałszywek[19]. Według innych opinii fałszywe dokumenty sprzedał im Muhammad al-Atris[20], obywatel USA pochodzenia egipskiego. Stał on na czele grupy przestępczej zajmującej się produkcją i sprzedażą fałszywych amerykańskich dokumentów tożsamości[21]. Po fałszywe dokumenty Al-Omari udał się na Florydę, tam wynajął samodzielne mieszkanie, w którym przebywał do września. W tym czasie na Florydzie przebywali już inni Saudyjczycy: Satam as-Sukami oraz bracia Walid i Wail asz-Szihri. As-Sukami i Walid asz-Szihri należeli do dziewięciu osób, które otworzyły konta w banku SunTrust z depozytem gotówkowym[22]. Z tych kont wypłacano pieniądze na bieżące wydatki. W maju 2001 r. na Florydę przylecieli Mohand asz-Szihri, Hamza al-Ghamdi i Ahmed al-Nami[23], a w końcu czerwca Emiratczyk Fajez Banihammad i Saudyjczyk Said al-Ghamdi. Dwóch Al-Ghamdich: Hamza i Ahmed było braćmi, Said al-Ghamdi natomiast nie był z nimi spokrewniony. Wszyscy trzej wywodzili się z tego samego plemienia w saudyjskiej prowincji Baha, do którego należał również Ahmed al-Haznawi. W 2000 r. trzech Al-Ghamdich walczyło w Czeczenii. Byli też bardzo pobożni[24]. Said przyleciał do Miami na Florydzie z Wailem asz-Szihrim. Sprzeczne są natomiast informacje dotyczące dziewiętnastego zamachowca – Salema al-Hazmi, brata Nawafa. Według FBI oraz zgodnie z informacjami zawartymi w raporcie Komisji 11 Września po raz pierwszy miał on przybyć do USA 29 czerwca 2001 r., chociaż istniały liczne, niepotwierdzone doniesienia, że wcześniej wraz z Satamem as-Sukamim mieszkał w San Antonio w Teksasie.

[18] https://en.wikipedia.org/wiki/Hani_Hanjour [dostęp: 1 VI 2021].

[19] https://en.wikipedia.org/wiki/Abdulaziz_al-Omari [dostęp: 1 VI 2021].

[20] Muhammad al-Atris został aresztowany w sierpniu 2002 r. na lotnisku Johna Kennedy'ego. Podczas przeszukania jego mieszkania znaleziono 75 fałszywych dokumentów.

[21] K. Izak, *Fałszywe dokumenty w rękach terrorystów*, „Człowiek i Dokumenty" 2014, nr 32, s. 10.

[22] https://en.wikipedia.org/wiki/Satam_al-Suqami [dostęp: 1 VI 2021].

[23] https://en.wikipedia.org/wiki/Ahmed_al-Nami [dostęp: 1 VI 2021].

[24] https://en.wikipedia.org/wiki/Ahmed_al-Ghamdi [dostęp: 1 VI 2021].

Al-Hazmi, podobnie jak inni Saudyjczycy, skorzystał z programu Visa Express, aby wjechać do USA. Potem przeniósł się do Paterson w stanie New Jersey i tam zamieszkał z Hanim Handżurem. Obaj należeli do piątki porywaczy, którzy złożyli wnioski o wydanie dokumentów tożsamości w Arlington w Wirginii, mimo że Al-Hazmi miał już dowód osobisty wydany w New Jersey[25].

Do końca czerwca 2001 r. wszyscy uczestnicy ataku przebywali już na terenie USA. Wśród nich było 15 Saudyjczyków, dwóch obywateli ZEA, Libańczyk i Egipcjanin. Trzech spośród tej czwórki tworzyło komórkę hamburską: Marwan asz-Szihhi, Zijad Dżarrah i Muhammad Ata, która stanowiła trzon całej operacji. Ata miał nią kierować. W dniu 7 lipca 2001 r. udał się on przez Zurych do Hiszpanii. Przebywał w różnych miejscowościach na terenie prowincji Tarragona w północno-wschodniej części kraju, gdzie odbyło się spotkanie „na szczycie". Z całą pewnością uczestniczył w nim Ramzi bin asz-Szibh, członek komórki hamburskiej, który nie otrzymał wizy do USA i pozostał łącznikiem Al-Kaidy[26]. To spotkanie pomogli zorganizować Imad ad-Din Barakat Jarkas alias Abu Dahdah, urodzony w Syrii, i Marokańczyk Amar al-Azizi. Sugeruje się również, że w spotkaniu wzięli udział Chalid Szejk Mohammad i Said Behadżi, a później dołączyli do nich Marwan asz-Szihhi i dwie inne osoby, prawdopodobnie bracia Wail i Walid asz-Szihri, którzy 16 lipca zatrzymali się w hotelu w Salou na Costa Dorada. Podczas spotkania Asz-Szibh przekazał instrukcje od Osamy bin Ladena, w tym jego apel o jak najszybsze przeprowadzenie operacji lotniczej oraz utrzymanie do końca w tajemnicy jej celów. Lider Al-Kaidy niepokoił się o bezpieczeństwo operacji, realnym zagrożeniem bowiem było przebywanie w USA dużej liczby uczestników planowanego ataku. Muhammad Ata poinformował, że do Stanów Zjednoczonych bez problemów dotarli już wszyscy uczestnicy akcji, którzy mieli sterroryzować załogi i pasażerów

[25] https://en.wikipedia.org/wiki/Salem_al-Hazmi [dostęp: 1 VI 2021].

[26] Śledztwo przeprowadzone po 11 września wykazało, że do komórki hamburskiej należeli lub mogli należeć również Marokańczycy: Said Behadżi, Zakarija as-Sabar, Abdelghani Mzudi i Munir al-Motassadek. Ten ostatni był jedynym członkiem tej komórki, który został skazany w Niemczech na karę pozbawienia wolności. W styczniu 2007 r. Motassadek usłyszał wyrok 15 lat więzienia za członkostwo w organizacji terrorystycznej i pomoc w zamordowaniu 246 osób. Właśnie tylu ludzi leciało czterema samolotami amerykańskich linii lotniczych 11 września 2001 r. W październiku 2018 r. Motassadek opuścił zakład karny w Hamburgu i został deportowany do Maroka bez prawa powrotu do Niemiec w ciągu 46 lat. Abdelghani Mzudi został aresztowany razem z Motassadekiem, ale w 2004 r. został uniewinniony. Pozostałych dwóch Marokańczyków po 11 września wyjechało z Niemiec i udało się do Afganistanu. Według niemieckiego prawa komórka hamburska nie była samodzielną organizacją terrorystyczną, gdyż ani pod względem finansowym, ani personalnym nie była w stanie dokonać zamachów w USA (tak brzmiała wówczas argumentacja). Zdaniem Federalnego Urzędu Ochrony Konstytucji zamachy nie były planowane w Hamburgu, lecz w Afganistanie. Zob. *Zamachy 11 września: historia „Grupy Hamburskiej"*, Deutsche Welle, 11 IX 2011 r., https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [dostęp: 12 IX 2011]; N. Werkhäuser, *Hamburg: pomocnik zamachowców z 11 września wydalony do Maroka*, Deutsche Welle, 15 X 2018 r., https://www.dw.com/pl/hamburg-pomocnik-zamachowców-z-11-września-wydalony-do-maroka/a-45895869 [dostęp: 16 X 2018]; *The 9/11 Commission Report*, https://govinfo.library.unt.edu/911/report/911Report.pdf, s. 160–164 [dostęp: 6 VI 2021].

porwanych samolotów. Stwierdził, że potrzebuje jeszcze od pięciu do sześciu tygodni, aby dopracować szczegóły operacji. Bin asz-Szibh wręczył mu ostateczną listę celów wyznaczoną przez Bin Ladena. Były to symbole Ameryki: Kapitol Stanów Zjednoczonych, Pentagon i World Trade Center. Twin Towers były dwoma najbardziej rozpoznawalnymi budynkami na świecie i ukształtowały panoramę Nowego Jorku. Jeśli któryś z pilotów-porywaczy nie będzie w stanie dolecieć do wskazanego celu, miał rozbić samolot. Muhammad Ata opowiedział o problemach, które miał z Zijadem Dżarrahem. Podejrzewał, że może on zrezygnować z przygotowań do ataku. Gdyby faktycznie doszło do takiej sytuacji, miał go zastąpić Zacarias Mussawi, który był szkolony jako kolejny pilot[27].

Francuski obywatel Zacarias Mussawi alias Abu Chalid as-Sahrawi od końca lutego do końca maja 2001 r. zaliczył ok. 60 godzin pilotażu w Norman w stanie Oklahoma. Mimo to nigdy nie leciał samodzielnie i z nieznanych przyczyn opuścił dalsze szkolenie. W tej samej szkole pilotażu przebywali również Muhammad Ata i Marwan asz-Szihhi. Z Oklahomy Mussawi wyjechał do Minnesoty, aby kontynuować szkolenie w Eagan, na które otrzymał pieniądze z Düsseldorfu i Hamburga przesłane przez Bin asz-Szibha. W dniu 13 sierpnia zapłacił 6800 dolarów za szkolenie na symulatorach lotu Boeingiem 747 w Pan-Am International Flight Academy. Wzbudził jednak podejrzenia instruktora Clarence'a Prevosta, który 15 sierpnia skontaktował się z biurem terenowym FBI, gdyż zaniepokoiły go pytania kursanta. Mussawi zadawał pytania na temat tras lotniczych wokół Nowego Jorku i dociekał, czy podczas lotu można otworzyć drzwi kokpitu. FBI szybko ustaliło, że Mussawi jest islamskim radykałem, który przebywał wcześniej w Pakistanie, a prawdopodobnie również w Afganistanie. Podejrzewano, że może on w przyszłości zostać porywaczem samobójcą. Ponieważ był obywatelem francuskim, któremu skończył się już termin ważności wizy, urząd imigracyjny wydał nakaz jego zatrzymania. W dniu 16 sierpnia Mussawi został aresztowany w Eagan i oskarżony o naruszenie przepisów imigracyjnych[28]. Po 11 września wysunięto hipotezę, że Mussawi przygotowywał się prawdopodobnie do drugiej serii ataków Al-Kaidy, która miała nastąpić na zachodnim wybrzeżu USA[29]. Był to jedyny z uczestników przygotowywanego ataku, który został aresztowany przed 11 września. Nazwano go później dwudziestym porywaczem. Tego samego określenia używano w stosunku do Ramziego bin asz-Szibha, ale niesłusznie, ponieważ ten nigdy nie dotarł do Stanów Zjednoczonych.

Po powrocie z Hiszpanii Muhammad Ata spotkał się 25 lipca z Dżarrahem, którego odwiózł na lotnisko w Miami, skąd miał on odlecieć do Niemiec. Następnego dnia Ata linią lotniczą Continental Airlines podróżował do Newark w Stanie New Jersey. Celem podróży było prawdopodobnie spotkanie z przebywającymi tam uczestnikami ataku. Wrócił na Florydę 30 lipca. W sierpniu ponownie podróżował samolotem do New Jersey i dwukrotnie do Las Vegas w celach obserwacyjnych, niezależnie od innych członków grupy. Co miesiąc spotykał się z Nawafem al-Hazmim, aby omawiać

[27] https://en.wikipedia.org/wiki/Mohamed_Atta [dostęp: 1 VI 2021].

[28] https://en.wikipedia.org/wiki/Zacarias_Moussaoui [dostęp: 1 VI 2021].

[29] L. Wright, *Wyniosłe wieże*…, s. 490.

stan przygotowań do operacji. W dniu 10 września Muhammad Ata odebrał Abdula Aziza al-Omariego z hotelu Milner w Bostonie w stanie Massachusetts (zameldowali się w nim również inni porywacze) i obaj terroryści wynajętym samochodem udali się do hotelu Comfort Inn w Portland w stanie Maine, gdzie spędzili ostatnią noc. Rano wsiedli na pokład samolotu lecącego z Portland do Bostonu. Przed godziną siódmą na lotnisku Logan w Bostonie Ata odebrał telefon od Marwana asz-Szihhi najprawdopodobniej z informacją, że i on wraz z towarzyszącymi mu osobami są już w tym samym porcie lotniczym[30]. Operacja weszła w fazę finałową.

Przebieg ataku

Boeing 767 American Airlines, lot nr 11 z Bostonu do Los Angeles

O godz. 7.59 samolot Boeing 767 American Airlines odbywający lot nr 11 wystartował z Bostonu do Los Angeles. Na jego pokładzie znajdowało się 81 pasażerów, w tym Muhammad Ata, Abdul Aziz al-Omari, bracia Wail i Walid asz-Szihri oraz Satam as-Sukami. Piętnaście minut po starcie, kiedy przystępowano do wydawania pasażerom napojów, rozpoczęła się operacja porwania samolotu. Prawdopodobnie terroryści zagrozili spowodowaniem eksplozji ładunku wybuchowego. W tym czasie piloci przestali reagować na sygnały kontroli ruchu lotniczego Zostali zmuszeni do opuszczenia kokpitu, a miejsce za sterami zajął Ata. Samolot zaczął zbaczać z zaplanowanej trasy. O godz. 8.18 dwóm stewardesom, Betty Ong i Madeline Sweeney, udało się z tylnej części samolotu nawiązać kilkuminutowy kontakt za pomocą radiotelefonu SBC Communications z biurem American Airlines i obsługą lotów na lotnisku Logan w Bostonie. Kobiety poinformowały o porwaniu samolotu, przekazały numery miejsc w pierwszej klasie, które zajęli porywacze po wejściu na pokład samolotu (w kolejności: 2A, 2B, 9A, 9C i 9B). Na tej podstawie szybko ustalono ich tożsamość. Przekazały też informację o zranieniu nożem pasażera, stewarda i stewardesy. Sprawcami byli bracia Asz-Szihri[31]. Dokładnie o godzinie 8.23 Muhammad Ata chciał z kokpitu podjąć próbę rozmowy z pasażerami, ale wcisnął niewłaściwy przycisk i tym samym wysłał wiadomość do służby kontroli ruchu lotniczego. Powiedział: (…) *mają trochę samolotów, stójcie tylko cicho, a nikomu nic się nie stanie. Wracamy na lotnisko*. Minutę później dorzucił: *Niech nikt się nie rusza. Wszystko będzie w porządku. Jeśli ktokolwiek się poruszy, zagrozi sobie i samolotowi. Po prostu tylko stójcie cicho*[32]. Służba kontroli ruchu lotniczego uzyskała potwierdzenie, że samolot został porwany, i poinformowała o tym fakcie Federalną Agencję Lotnictwa. O godz. 8.33 Muhammad Ata zakomunikował: *Proszę wszystkich,*

[30] https://en.wikipedia.org/wiki/Mohamed_Atta [dostęp: 1 VI 2021].

[31] https://pl.melayukini.net/wiki/Betty_Ong [dostęp: 1 VI 2021]; https://pl.melayukini.net/wiki/Wail_al-Shehri [dostęp: 1 VI 2021].

[32] https://en.wikipedia.org/wiki/Mohamed_Atta [dostęp: 1 VI 2021].

by się nie ruszali. Wracamy na lotnisko, nie próbujcie wykonywać jakichkolwiek głupich ruchów[33]. Pięć minut później bostońska Służba Kontroli Ruchu Lotniczego poinformowała NORAD[34], który z kolei wezwał dwa samoloty F-15 Eagle z bazy Otis, aby przejęły kontrolę nad lotem. Rozkaz startu myśliwców F-15 wydano jednak za późno. Z analizy czasu informowania kontrolerów wynika, że nie podjęto właściwych decyzji w odpowiednim czasie, NORAD bowiem został poinformowany o 8.38, a więc 20 minut po pierwszym sygnale dotyczącym porwania samolotu przekazanym przez stewardesę. Samolot był już nad nowojorskim Manhattanem[35]. O godz. 8:46 przerażona Sweeney powiedziała przez telefon do menadżera Michaela Woodwarda: *Widzę wodę. Widzę budynki. Widzę budynki! Lecimy nisko. Lecimy bardzo, bardzo nisko. Lecimy zbyt nisko. O mój Boże, lecimy zbyt nisko. O mój Boże!*[36] W tym momencie samolot pilotowany przez Atę uderzył w północną wieżę WTC z prędkością ok. 750 km/h (w zbiornikach znajdowało się ok. 40 tys. litrów paliwa)[37]. Samolot wbił się między 93. a 99. piętrem budynku. Ze względu na ogromne zniszczenia wieży ludzie nie mogli uciec z pięter, które były powyżej 92. piętra. Z powodu zablokowania wszystkich schodów i wind 1344 osoby zostały uwięzione. Setki osób zostało zabitych od siły uderzenia, inne zginęły od ognia bądź dymu, a jeszcze inne poniosły śmierć, wyskakując z okien budynku. Pierwsze doniesienia mówiły o nieszczęśliwym wypadku, jednak narracja zmieniła się z chwilą, gdy drugi samolot, lot 175, rozbił się o południową wieżę WTC[38].

---

[33] Tamże.

[34] North American Aerospace Defense Command (Dowództwo Obrony Północnoamerykańskiej Przestrzeni Powietrznej i Kosmicznej) – jednostka organizacyjna istniejąca od 12 maja 1958 r., w skład której wchodzą dwa kraje: USA i Kanada, https://pl.wikipedia.org/wiki/North_American_Aerospace_Defense_Command [dostęp: 23 VIII 2021] – przyp. red.

[35] https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks#American_Airlines_Flight_11:_One_World_Trade_Center,_North_Tower [dostęp: 3 VI 2021]; National Commission on Terrorist Attacks Upon the United States, *We have some planes*, https://www.9-11commission.gov/report/911Report_Ch1.htm [dostęp: 3 VI 2021].

[36] https://pl.melayukini.net/wiki/Madeline_Amy_Sweeney [dostęp: 1 VI 2021].

[37] Lot z Portland do Bostonu był opóźniony, dlatego bagaż Muhammada Aty nie dotarł na czas na lot nr 11. Służby odzyskały go później na lotnisku Logan. W bagażu znajdowały się m.in.: mundury lotnicze, instrukcje lotu, a także list pożegnalny, będący swego rodzaju instrukcją męczennika. Dokument składał się z trzech części: wskazówek dotyczących ostatniej nocy życia męczennika, czasu przed wejściem na pokład samolotu i lotu nim do momentu męczeństwa. Były to instrukcje i wskazówki poparte cytatami z *Koranu* dla przyszłych zamachowców samobójców. Wszystko zostało sporządzone w kontekście przygotowania duchowego. Interesujący jest fragment „testamentu" Aty: *Ci, którzy będą obmywać moje ciało, powinni być dobrymi muzułmanami. Ten, kto będzie obmywać moje ciało wokół genitaliów, powinien założyć rękawiczki, by ich nie dotykać.* Terrorysta nie zdawał sobie sprawy z tego, że jego ciało zostanie unicestwione w wybuchu. Zob. P.L. Williams, *Al-Kaida – bractwo terroru*, Warszawa 2002, s. 168–175.

[38] https://pl.wikipedia.org/wiki/Katastrofa_lotu_American_Airlines_11 [dostęp: 1 VI 2021].

Boeing 767 United Airlines, lot nr 175 z Bostonu do Los Angeles

W dniu 9 września z Florydy do Bostonu odlecieli Marwan asz-Szihhi, Fajez Banihammad Mohand asz-Szihri i Satam as-Sukami. Następnego dnia wynajęli pokój w hotelu Milner w Bostonie. As-Sukami dzielił więc pokój z porywaczami innego samolotu, ponieważ on sam wszedł na pokład samolotu odbywającego lot nr 11[39]. Bracia Hamza i Ahmed al-Ghamdi przylecieli z Florydy do Bostonu już 7 września. Zameldowali się w hotelu Days, w którym przebywali do dnia ataku. Rano 11 września przyjechali taksówką na lotnisko Logan. Kilka minut przed godziną siódmą już na lotnisku Marwan asz-Szihhi wykonał telefon do Aty, z którym rozmawiał ok. trzy minuty. Około godz. 7.30 porywacze: Asz-Szihhi, Banihammad, Asz-Szihri oraz bracia Al-Ghamdi zajęli miejsca w samolocie Boeing 767 United Airlines, mającym odbyć lot nr 175 do Los Angeles. Na pokładzie znajdowało się 46 pasażerów i dziewięciu członków załogi. Po ok. 30 minutach lotu, między godziną 8.42 a 8.46, samolot został porwany. Bracia Al-Ghamdi zepchnęli pasażerów i załogę na tył samolotu, grożąc eksplozją ładunku wybuchowego, a Banihammad i Szihri zabili pilotów – Victora Saraciniego i Michaela Horroksa. Umożliwiło to Asz-Szihhiemu przejęcie kontroli nad samolotem. Jedna ze stewardes została pchnięta nożem. Pilotowany przez Asz-Szihhiego samolot omal nie zderzył się z samolotem Delta Airlines lot 2315. Kilku pasażerów zatelefonowało do swoich bliskich, informując ich o porwaniu. Jednocześnie dowiedzieli się o samolocie, który uderzył w północną wieżę WTC. O godz. 9.03 ich samolot – lecący z prędkością 950 km/h, a więc szybciej niż samolot pilotowany przez Muhammada Atę – wbił się w pobliżu południowo-wschodniego narożnika południowej wieży, między piętrami 77. a 85. W zbiornikach miał ok. 38 tys. litrów paliwa. Uderzenie w budynek w takim miejscu spowodowało, że południowa wieża zawaliła się wcześniej niż północna, która runęła o godz. 10.28[40]. Szacuje się, że w budynku w chwili katastrofy zginęło lub uwięzionych w nim zostało 637 osób. W momencie zderzenia od samolotu oderwała się część kadłuba i podwozia, która spadła na 47-piętrowy budynek WTC 7 (bliźniacze wieże to WTC 1 i WTC 2), co spowodowało jego pożar, a o godz. 17.20 jego zawalenie[41].

Boeing 757 American Airlines, lot nr 77 z Waszyngtonu do Los Angeles

W dniu 10 września wszyscy porywacze samolotu Boeing 757 American Airlines odbywającego lot nr 77 do Los Angeles, tj. Hani Handżur, Chalid al-Mihdar, Madżid Moked oraz bracia Nawaf i Salem al-Hazmi, zameldowali się w hotelu Marriott Residence Inn w Herndon w stanie Wirginia, położonym niedaleko międzynarodowego lotniska Dulles w Waszyngtonie. W tym samym czasie w hotelu przebywał Saleh ibn Abdul Rahman Husajen, prominentny przedstawiciel władz Arabii Saudyjskiej, jednak nie ma dowo-

[39] https://pl.melayukini.net/wiki/Satam_al-Suqami [dostęp: 1 VI 2021].

[40] https://pl.melayukini.net/wiki/Marwan_al-Shehhi [dostęp: 4 VI 2021]; https://pl.melayukini.net/wiki/Hamza_al-Ghamdi [dostęp: 4 VI 2021].

[41] https://pl.xcv.wiki/wiki/United_Airlines_Flight_175 [dostęp: 4 VI 2021].

dów na to, że spotkał się on z którymś z przyszłych porywaczy lub nawet o nich wiedział. Następnego dnia ok. godz. 6.20 cała grupa opuściła hotel i udała się na wymienione lotnisko. O godz. 7.20 po kontroli bezpieczeństwa Al-Mihdar i Moked zostali poddani ponownej kontroli, ponieważ wykrywacz metalu zasygnalizował obecność metalowego przedmiotu. Jednak obaj bez problemów weszli na pokład samolotu, podobnie jak trzej pozostali członkowie grupy. O godz. 7.50 zajęli miejsca w samolocie. Byli oni uzbrojeni w plastikowe noże i przecinaki do tapet. Oprócz nich na pokładzie znajdowało się 53 pasażerów i sześciu członków załogi. Samolot wystartował o godz. 8.20 z 10-minutowym opóźnieniem. Dokładnie 30 minut później piloci ostatni raz skomunikowali się drogą radiową z kontrolerami ruchu lotniczego. W ciągu następnych czterech minut samolot musiał znaleźć się już w rękach porywaczy, ponieważ zboczył z wyznaczonego kierunku lotu. Za sterami samolotu usiadł Hani Handżur. W odróżnieniu od porwań pozostałych samolotów w przypadku lotu nr 77 nie było informacji o groźbie wywołania eksplozji i ataku przy użyciu ostrych narzędzi. Piloci Charles Burlingame i David Charlesbois zostali zmuszeni do zajęcia miejsc w tyle samolotu. Używając interkomu pokładowego, Handżur ogłosił, że samolot został porwany. Pasażerka Barbara Olson przez telefon poinformowała swojego męża Theodora Olsona, prokuratora generalnego USA, o porwaniu samolotu. O godz. 9.37 samolot wbił się zachodnią fasadę Pentagonu. Zginęły 64 osoby znajdujące się w samolocie i 125 osób przebywających w budynku[42].

Boeing 757 United Airlines, lot nr 93 z Newarku do San Francisco

W dniu 7 września Zijad Dżarrah, Ahmed al-Haznawi, Ahmed al-Nami i Said al-Ghamdi jako pierwsi opuścili Florydę. Przylecieli do Newarku koło Nowego Jorku. Nie wiadomo, czym się zajmowali do chwili porwania samolotu. Dnia 10 września Dżarrah napisał list do narzeczonej w Niemczech, którego jednak nie otrzymała. Przesyłka wróciła do USA i została przejęta przez FBI. Był to list terrorysty samobójcy, zawierający m.in. zwroty: *Zrobiłem, co musiałem. To wielki zaszczyt, zobaczysz wynik i wszyscy będą świętować*[43]. Dnia 11 września między godziną 7.39 a 7.48 wszyscy porywacze weszli na pokład samolotu Boeing 757 United Airlines, majacego odbyć lot nr 93 z Newarku do San Francisco. Zajęli miejsca w klasie biznes z przodu samolotu. Oprócz nich na pokładzie znajdowało się 33 pasażerów i siedmioro członków załogi. Samolot miał wystartować o godz. 8.00, ale z powodu opóźnień innych lotów wystartował dopiero o godz. 8.42. O godz. 9.24 załoga została powiadomiona o dwóch samolotach, które rozbiły się o WTC, i ostrzeżona przed próbą wtargnięcia do kokpitu. Dwie minuty później pilot poprosił o potwierdzenie tej informacji. W tym czasie jeden z porywaczy, prawdopodobnie Al-Ghamdi, zaatakował jedną ze stewardes, a Al-Haznawi pasażera i pokazał tekturową atrapę bomby, którą przymocował do ciała. O godz. 9.28 stewardesa

[42] https://pl.melayukini.net/wiki/Hani_Hanjour [dostęp: 4 VI 2021]; https://pl.melayukini.net/wiki/Nawaf_al-Hazmi [dostęp: 4 VI 2021].

[43] https://pl.melayukini.net/wiki/Ziad_Jarrah [dostęp: 4 VI 2021].

została zmuszona do otwarcia drzwi kokpitu. Tam Al-Ghamdi i Al-Namni podcięli gardła pilotom, Jasonowi Dahlowi i LeRoyowi Homerowi, oraz zabili stewardesę. Kontroler ruchu lotniczego usłyszał krzyk zabijanej kobiety i głos terrorysty krzyczącego „Allah Akbar!". Gdy samolot zaczął gwałtownie opadać, za sterami zasiadł Dżarrah, który wyrównał lot i zawrócił maszynę w kierunku Waszyngtonu. Pasażerów zmuszono do zajęcia miejsc w tylnej części samolotu. O godz. 9.32 jeden z porywaczy nakazał im zachować spokój. Dżarrah wydawał pasażerom polecenia z kokpitu, ponieważ jednak nie przełączył odpowiedniego guzika, jego głos nie był słyszany na pokładzie samolotu, lecz w kontroli ruchu powietrznego. O godz. 9.31 przekazał komunikat: *Panie i panowie, mówi kapitan. Proszę zająć miejsca. Pozostańcie w pozycji siedzącej. Mamy bombę na pokładzie. Więc usiądźcie.* Osiem minut później powtórzył: *Mówi kapitan. Chciałbym, żebyście wszyscy pozostali na miejscach. Na pokładzie jest bomba. Wracamy na lotnisko, aby spełniono nasze żądania. Proszę zachować ciszę*[44]. Nie zabroniono natomiast pasażerom korzystania z telefonów komórkowych. Dzięki temu dowiedzieli się od swoich rodzin o ataku na WTC. Pasażer Jeremy Glick przekazał rodzinie, że porywacze są Arabami i zawiązali sobie na głowach czerwone opaski. On i inni pasażerowie doszli do wniosku, że ich samolot również może posłużyć do ataku na jakiś ważny obiekt. W wyniku głosowania podjęli decyzję o próbie odbicia samolotu z rąk terrorystów. W tej decyzji utwierdził ich najprawdopodobniej widok ciał pilotów, które leżały przed kokpitem. Zdecydowano się zaatakować przy użyciu broni sporządzonej ze sztućców znajdujących się w pokładowej kuchni samolotu oraz naczyń z wrzątkiem. Atak pasażerów spowodował, że porywacze stracili panowanie nad sytuacją. Zijad Dżarrah miał poważne kłopoty ze sterowaniem Boeingiem, jednak usiłował utrudnić pasażerom przedostanie się pod drzwi kokpitu, kładąc maszynę raz na lewe, raz na prawe skrzydło. To powodowało, że pasażerowie tracili równowagę w wąskich przejściach wnętrza samolotu, mimo to zdołali przejść na przód maszyny. Najprawdopodobniej używając wózka do rozwożenia posiłków, staranowali jednego z terrorystów stojącego przed drzwiami kokpitu. Pasażerom udało się go obezwładnić lub zabić. W tym czasie trzej pozostali porywacze zamknęli się w kokpicie. Nie byli przygotowani na taki obrót sytuacji. Gdy pasażerowie zaczęli wyważać drzwi do kabiny pilotów, Dżarrah najprawdopodobniej podjął decyzję o rozbiciu samolotu o ziemię. Z niewiadomych przyczyn przedłużał moment katastrofy. W chwili gdy zwiększył prędkość lotu, pasażerom udało się wyważyć drzwi. Wdali się oni w bójkę z terrorystami. Samolot odwrócił się podwoziem do góry i o godz. 10.03 (według innych źródeł o 10.06 lub 10.10) z prędkością 930 km/h roztrzaskał się o ziemię. Katastrofa nastąpiła niedaleko Shanksville w Pensylwanii[45]. Ponad 40-minutowe opóźnienie lotu nr 93 sprawiło, że pasażerowie dowiedzieli się o wcześniejszych atakach, czego terroryści nie wzięli pod uwagę. Opór pasażerów ich zaskoczył. Celem

[44] Tamże.

[45] https://pl.wikipedia.org/wiki/Katastrofa_lotu_United_Airlines_93 [dostęp: 4 VI 2021]; https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks [dostęp: 4 VI 2021].

ataku był Biały Dom lub Kapitol. Ten drugi obiekt wydaje się jednak bardziej prawdopodobny, ponieważ jego zniszczenia zażyczył sobie Osama bin Laden.

Skutki ataku

W wydarzeniach z 11 września zginęło 2996 osób, w tym 19 terrorystów, a 6291 zostało rannych[46]. Wśród ofiar śmiertelnych było sześcioro Polaków. W akcji ratunkowej zginęło 343 strażaków. Większość ratowników, strażaków i policjantów, którzy jako pierwsi ruszyli z pomocą i przeżyli, zaczęła chorować na nowotwory z powodu wdychania szkodliwych substancji. U niektórych osób objawy pojawiły się dopiero po 10 latach, a nawet później. Do 2017 r. śmierć w wyniku chorób związanych ze służbą w okolicy strefy zero poniosło 142 funkcjonariuszy[47]. W mediach o ataku z 11 września zaczęto pisać i mówić jako o megaterroryzmie, ponieważ to zdarzenie było dotychczas najbardziej skutecznym atakiem jakiejkolwiek organizacji terrorystycznej. Stany Zjednoczone i duża część świata były w szoku. W USA w okresie kilkunastu dni po 11 września sprzedaż broni i amunicji do użytku osobistego wzrosła o 10 proc., w ciągu pół roku sprzedano o 450 tys. sztuk bronii więcej niż w analogicznym okresie sprzed ataku. Rozbudzono patriotyczne nastroje. W dniu ataku sprzedaż flag Stanów Zjednoczonych w sklepach sieci Walmart wzrosła o 2 tys. proc., a następnego dnia o dalsze 4 tys. proc. Na początku października 80 proc. Amerykanów miało wywieszone flagi przed domami. Kiedy prezydent George W. Bush 12 września ogłosił „totalną walkę dobra ze złem", tłum skandujący hasło „Zabić wszystkich Arabów!" otoczył jeden z największych, meczetów w Chicago, odwiedzany głównie przez Arabów. W całych Stanach Zjednoczonych nasiliły się antymuzułmańskie nastroje, akty nienawiści i agresji skierowane w stronę obcych kulturowo mieszkańców. Policja radziła zamknąć na tydzień szkoły muzułmańskie, a wyznawcom islamu zalecała, aby nie brali udziału w piątkowych modlitwach ze względu na bezpieczeństwo. Ofiarami tych ataków nienawiści, także śmiertelnymi, byli zarówno muzułmanie, jak i hindusi i sikhowie[48].

Zamachy wyrządziły olbrzymie straty materialne. Wyjątkowo duże koszty poniosły towarzystwa ubezpieczeniowe i reasekuracyjne, linie lotnicze oraz producenci samolotów, a także branża turystyczna. Ogromne szkody związane ze zniszczeniem nowojorskiego World Trade Center oraz dezorganizacją systemu finansowego musiały być pokryte przez towarzystwa asekuracyjne, zaangażowane w działalność na intratnym rynku amerykańskim. Duże odszkodowania należały się również liniom lotniczym, których samoloty zostały porwane, a następnie zniszczone podczas ataków

[46] https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [dostęp: 7 VI 2021].

[47] *Nieśli pomoc po ataku na WTC, po latach ciężko zachorowali. Śmierć strażaków - ojca i syna - w wyniku nowotworów*, Polsat News, 19 VIII 2017 r., https://www.polsatnews.pl/wiadomosc/2017-08-19/niesli-pomoc-po-ataku-na-wtc-smierc-strazakow-w-wyniku-nowotworow/ [dostęp: 6 VI 2021].

[48] D. Streatfeild, *Świat po 11 września*, Warszawa 2011, s. 42–44.

terrorystycznych. Szwajcarskie towarzystwo reasekuracyjne Swiss Re oceniło, że łączne straty sektora ubezpieczeniowego, mające związek z wrześniowym atakiem, wyniosły 90 mld dolarów, z czego 19 mld dolarów to koszty bezpośrednie. Zabezpieczając się na przyszłość, sektor ubezpieczeniowy zrewidował dotychczasową politykę i podniósł znacznie stawki. Wzrosły one od 20 do 80 proc., najwięcej w tych przypadkach, w których występuje szczególnie duże ryzyko. Dla linii lotniczych porwanie i zniszczenie kilku samolotów oznaczało gwałtowny spadek zainteresowania podróżami. Obawy przed nowymi atakami terrorystycznymi sprawiły, że ruch pasażerski wyraźnie się zmniejszył, co dla przewoźników oznaczało znaczne ograniczenie wpływów finansowych. Jeszcze dotkliwszym ciosem okazało się podwyższenie stawek ubezpieczeniowych, co bardzo zwiększyło koszty transportu lotniczego. Ponieważ komunikacja lotnicza już wcześniej borykała się ze skutkami ogólnego załamania koniunktury w gospodarce światowej, wydarzenia z 11 września pogrążyły ten sektor usług w kryzysie najgłębszym od czasów II wojny światowej. Łączne straty szacowano na 12–13 mld dolarów. W tych warunkach towarzystwa lotnicze musiały zrezygnować z części połączeń, wycofując z eksploatacji setki samolotów i redukując personel. Obniżono też ceny biletów, w niektórych przypadkach aż o 80 proc. Dwie firmy przeżywające od dłuższego czasu trudności finansowe – Swissair i Sabena – musiały ogłosić upadłość. Po 11 września ogólna liczba lotów w USA, łącznie z prywatnymi, zmniejszyła się o 22,7 proc. Europejskie linie lotnicze odnotowały w 2001 r. spadek ruchu pasażerskiego o 5 proc., a rok po ataku terrorystycznym był on mniejszy o 11 proc. Na lotniskach krajowych i międzynarodowych na całym świecie obsłużono o 3 proc. mniej pasażerów. Zmalał również ruch towarowy. Kryzys w przewozach powietrznych odbił się na sytuacji producentów samolotów. Linie lotnicze bowiem w dużym stopniu ograniczyły zamówienia, zwłaszcza na maszyny Boeing oraz Airbus. Spadek zainteresowania podróżami odczuła cała branża turystyczna, od organizatorów wycieczek przez hotele i gastronomię po różnego rodzaju firmy handlowe i usługowe. Jednym z przykładów było załamanie koniunktury w handlu artykułami luksusowymi, który odbywał się w zasadzie w portach lotniczych. W konsekwencji zmalała też produkcja takich artykułów[49].

Najważniejsze były jednak skutki o charakterze międzynarodowym. Przeprowadzając ataki na WTC i Pentagon, Al-Kaida wpłynęła na światową politykę, skłoniła bowiem Waszyngton do ogłoszenia wojny z terroryzmem. W przemówieniu do narodu 20 września 2001 r. prezydent George W. Bush ujawnił plany tej wojny. Stany Zjednoczone domagały się od swojego społeczeństwa, od swoich sojuszników i wszystkich narodów bezwarunkowego poparcia dla wojny z terroryzmem, a zasada „z nami albo przeciw nam" spowodowała potępienie neutralnych państw i uznanie ich za wrogów Stanów Zjednoczonych. W samej Ameryce sprzeciw wobec tej wojny traktowano jako zdradę tych, którzy zginęli na Manhattanie, w Waszyngtonie i w Pensylwanii, a także zdradę

[49] A. Krzemirski, *Rocznica 11 września. Olbrzymie odszkodowania i strach przed podróżami*, Parkiet, 11 IX 2002 r., https://www.parkiet.com/artykul/260530.html [dostęp: 6 VI 2021].

narodu i wartości cywilizacji[50]. Jednocześnie Waszyngton opracował listę celów strategicznych. Wśród nich rozpatrywano możliwość ataku na Irak, chociaż nic nie wskazywało na zaangażowanie tego kraju w ten akt terrorystyczny. Ostatecznie przeważyła umiarkowana linia postępowania sekretarza stanu Colina Powella i po odmowie talibów wydania Osamy bin Ladena, 7 października 2001 r. salwą 50 pocisków wystrzelonych z amerykańskich okrętów na Morzu Arabskim rozpoczęła się amerykańska operacja Enduring Freedom (Trwała Wolność). Jeden z pocisków trafił w Kandaharze w rezydencję mułły Mohammada Omara, przywódcy talibów, zabijając jego ojczyma i 10-letniego syna. Inny spadł na małą wioskę Kuram, zabijając 100 cywilów, a kolejny zniszczył meczet na przedmieściach Dżalalabadu. Do 9 listopada walczące z talibami siły afgańskiego Sojuszu Północnego, wspierane przez siły amerykańskie, uzyskały kontrolę nad strategicznym miastem Mazar-i-Szarif – stolicą prowincji Balch w północnym Afganistanie. W ten sposób położono kres władzy talibów. Dwa dni później miasto Herat, znajdujące się na zachodzie kraju, poddało się niemal bez strzału. Dnia 12 listopada siły koalicyjne weszły do Kabulu, gdzie witały je wiwatujące tłumy przeciwników talibów. Wbrew wszelkim oczekiwaniom pierwszy etap odwetowej wojny przeciwko talibom okazał się niezaprzeczalnym sukcesem armii amerykańskiej. Podczas gdy wieszczono nowy Wietnam lub remake klęski radzieckiej z lat 80. XX w., armia amerykańska, dzięki swojemu lotnictwu i siłom specjalnym oraz pomocy oddziałów wrogich talibom, w ciągu kilku tygodni rozbiła Islamski Emirat Afganistanu. Al-Kaida musiała zrezygnować ze swoich struktur zwartej organizacji w Afganistanie i od tego momentu pozostawała strukturą sieciową oraz ideologią polityczną. Amerykanom nie udało się schwytać w Afganistanie Osamy bin Ladena, który dla wielu muzułmanów stał się symbolem walki z USA i żywą legendą.

Dalszym ciągiem amerykańskiej wojny z terroryzmem była inwazja na Irak 20 marca 2003 r. Podwójne zagrożenie terroryzmem i bronią masowego rażenia było jedynie pretekstem do wyeliminowania wroga, który od dawna był na celowniku Stanów Zjednoczonych, szczególnie tzw. neokonserwatystów, polityków skupionych wokół wiceprezydenta Dicka Cheneya i zastępcy sekretarza obrony Paula Wolfowitza. Cheney podjął starą koncepcję wojny prewencyjnej Reagana i uczynił z niej główny element nowej strategii, aby doprowadzić do zmiany rządu w Iraku. Prewencja została zastąpiona odstraszaniem. Od tego czasu teoretyczne pojęcie wojny prewencyjnej przemieszało się w praktyce z wojną z terroryzmem. Był to sposób narzucenia amerykańskiej supremacji na kolejne dziesięciolecia i przekształcenia Stanów Zjednoczonych w hegemoniczne mocarstwo, m.in. przez obalenie reżimu w Iraku i planowanie wprowadzenia tam demokracji na wzór USA. W dłuższej perspektywie miało to wpłynąć na zmiany systemu rządów w innych krajach nad Zatoką Perską i przyczynić się do rozwiązania konfliktu palestyńsko-izraelskiego. Dalszy ciąg wydarzeń jest powszechnie znany. W dniu 20 marca 2003 r. siły koalicji, głównie amerykańskie i brytyjskie (przy

[50] *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, P. Scraton (red.), Warszawa 2003, s. 14–15.

udziale Australijczyków i Polaków), szybko obaliły rząd Saddama Husajna, który został zatrzymany kilka miesięcy później. Siły amerykańskie, które utknęły na długie lata zarówno w Afganistanie, jak i w Iraku, nie rozwiązały żadnych problemów, przyczyniły się za to do rozwoju islamskiego terroryzmu na niespotykaną skalę. Ponadto inwazja na Irak okazała się jedną z najbardziej spektakularnych, śmiercionośnych pomyłek strategicznych w dziejach wojskowości.

Atak terrorystyczny na USA stał się impulsem do reformy amerykańskich służb specjalnych, największej od 1947 r. Waszyngton podjął decyzję dotyczącą konieczności stworzenia systemu efektywnie przeciwdziałającego zagrożeniom o charakterze terrorystycznym oraz skutecznie ostrzegającego o ich wystąpieniu. Wiązało się to ze wzmocnieniem struktur mających uprawnienia operacyjno-rozpoznawcze, zwiększeniem zakresu ich zadań oraz usprawnieniem ich zdolności do koordynacji. Zdaniem niektórych ekspertów i agentów FBI to właśnie brak współpracy między tą służbą a CIA, która nie przekazywała jej ważnych informacji, nie pozwolił na wykrycie terrorystycznego spisku w USA, zanim doszło do największego w historii zamachu. Bez odpowiedzi pozostaje natomiast pytanie, czy w innych okolicznościach udałoby się zapobiec atakowi. Wydaje się, że raczej nie. Amerykańskie służby specjalne miały zbyt mało informacji, aby można je było powiązać w logiczny ciąg prowadzący do zamachowców.

Oprócz reformy służb wprowadzono też nowe regulacje prawne. Zostały one zawarte w dokumencie z 26 października 2001 r., znanym powszechnie pod nazwą *USA Patriot Act*[51]. Ta ustawa zezwoliła rządowi na dostęp do informacji prywatnych, nawet jeśli nic nie dowodziło zaangażowania się danej osoby w działalność terrorystyczną, przy wszystkich możliwych nadużyciach, które z tego wynikały. Na terytorium kraju wprowadzono liczne środki bezpieczeństwa, ze szczególnie ścisłymi kontrolami na lotniskach i w budynkach publicznych. Zaostrzono kontrolę granic, dotyczącą zwłaszcza osób z krajów objętych obowiązkiem wizowym. Imigranci uznani za osoby podejrzane byli aresztowani. Dokonano centralizacji aparatu zarządzania walką z terroryzmem. Przystąpiono do reformy Wspólnoty Wywiadów (Intelligence Community), skłóconej wewnętrznymi walkami o wpływy, kompetencje i zakres działania. Waszyngton przyznał wymiarowi sprawiedliwości najwyższe prerogatywy. Trudno ocenić, w jakim stopniu działania podjęte na podstawie tych decyzji pomogły w zlikwidowaniu zagrożenia terrorystycznego. Z pewnością w pewnym stopniu przyczyniły się do ograniczenia wolności obywatelskich i praw człowieka, czego symbolem stało się internowanie więźniów podejrzewanych o działalność terrorystyczną w amerykańskiej bazie wojskowej w Guantanamo. Na arenie międzynarodowej nowy kierunek w polityce zagranicznej USA został wypaczony sympatiami i doraźnymi celami neokonserwatystów, którzy wpisali Irak na czarną listę krajów wspierających Al-Kaidę (mimo że nie było na to żadnych dowodów), pominęli natomiast Arabię Saudyjską i Pakistan, o których

[51] M. Szymańska, *Eksplozja terroryzmu w USA a przekształcenia w amerykańskich służbach specjalnych po 11 września 2001 r.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 186.

wiadomo, że wspierały wiele organizacji terrorystycznych, z Al-Kaidą włącznie[52]. Wiele kontrowersji w Stanach Zjednoczonych wywołało utajnienie 28 stron (z 838) przywoływanego już raportu Kongresu USA z 2002 r. poświęconego zamachom z 11 września. Arabia Saudyjska stanowczo odrzucała oskarżenia, że miała cokolwiek wspólnego z atakami na Nowy Jork i Waszyngton. Podstawą takich zarzutów, wysuwanych przez część rodzin ofiar i amerykańskich polityków, było właśnie utajnienie fragmentu raportu Kongresu USA. Spekulowano, że są tam dowody wskazujące na związki Arabii Saudyjskiej z zamachami, i nie wynikały one tylko z tego, że 15 z 19 terrorystów było Saudyjczykami, którzy należeli do Al-Kaidy dowodzonej przez innego bogatego Saudyjczyka – Osamę bin Ladena. Po odtajnieniu dokumentu w lipcu 2016 r. zwracano uwagę, że nie było w nim żadnych informacji wskazujących na powiązania władz saudyjskich z zamachowcami. Jednocześnie były senator z Florydy Bob Graham, który współprzewodniczył śledztwu Kongresu, uznał, że z ujawnionych stron jasno wynika, że Arabia Saudyjska była głównym źródłem finansowania zamachów. Tak więc wątpliwości w sprawie roli Arabii Saudyjskiej w ataku z 11 września 2001 r. pozostały i dały podstawę do roszczeń o odszkodowania wysuwanych przez rodziny ofiar pod adresem Rijadu[53].

Teorie spiskowe na temat ataku z 11 września 2001 roku

Duża część zwolenników teorii spiskowych dotyczących wydarzeń z 11 września sugeruje, że stał za nimi ówczesny rząd USA, a zamachy zostały zaplanowane i zorganizowane przez służby specjalne. W sondażu przeprowadzonym w 2006 r., w piątą rocznicę zamachów, ponad jedna trzecia respondentów stwierdziła, że waszyngtońska administracja pomogła zrealizować te ataki lub rozmyślnie nie uczyniła nic, aby im zapobiec. Z kolei w telefonicznym sondażu przeprowadzonym w tym samym roku połowa Amerykanów odpowiedziała, że dla prezydenta George'a W. Busha zamachy z 11 września były pretekstem do wojny z Irakiem. Dwa lata później jeszcze bardziej wzrosła liczba osób uznających alternatywną wersję wydarzeń z 11 września. Aż 46 proc. Amerykanów nie wierzyło w wersję wypadków podawaną przez rząd, a niemal połowa społeczeństwa amerykańskiego, w tym wielu naukowców i polityków, domagała się ponownego śledztwa w sprawie zamachów[54]. Nic zatem dziwnego, że urósł w siłę ruch

[52] G. Chaliand, A. Blin, *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020, s. 372–373.

[53] *USA: Kongres ujawnił tajną część raportu o zamachach z 11 września*, „Dziennik Gazeta Prawna", 15 VII 2016 r., https://www.gazetaprawna.pl/wiadomosci/artykuly/960454,usa-kongres-ujawnil-tajna-czesc-raportu-o-zamachach-z-11-wrzesnia.html [dostęp: 16 VII 2016]; *Rodziny ofiar zamachów na WTC z 11 września pozywają Arabię Saudyjską*, Bankier.pl, 21 III 2017 r., https://www.bankier.pl/wiadomosc/Rodziny-ofiar-zamachow-na-WTC-z-11-wrzesnia-pozywaja-Arabie-Saudyjska-3668756.html [dostęp: 22 III 2017].

[54] *Spisek World Trade Center*, Laif, 9 V 2008 r., https://web.archive.org/web/20090615224350/http://laif.co.uk/art,spisek_world_trade_center,1496.html [dostęp: 9 VI 2021].

na rzecz prawdy o zamachu na Amerykę – 9/11 Truth Movement, który wspierał produkcję filmów dokumentalnych demaskujących domniemane kłamstwa i zaniedbania Waszyngtonu oraz publikację książek, często autorstwa uznanych autorytetów. Jednak żywiołem dla tego ruchu okazał się Internet, w którym rozpowszechniano informacje, że rząd jest współodpowiedzialny lub wprost odpowiedzialny za zamachy. Szczególną rolę odgrywały w nim rodziny ofiar, które nie mogły zrozumieć, (…) *dlaczego prezydent Bush po informacji o uderzeniu samolotu w drugą wieżę WTC siedział bezczynnie, z bezmyślną miną wśród sześciolatków w szkole na Florydzie*[55].

W 2014 r. 2300 architektów i inżynierów zrzeszonych w organizacji Architects & Engineers for 9/11 Truth – AE911Truth (Architekci i Inżynierowie na rzecz Prawdy o 9/11) domagało się ponownego i niezależnego dochodzenia w sprawie zawalenia się trzech budynków WTC. Obecnie ta organizacja liczy już 3300 członków[56]. We wrześniu 2019 r. zespół naukowców z University of Alaska Fairbanks opublikował wyniki czteroletnich badań dotyczących zachowania się konstrukcji budynku WTC 7 w chwili katastrofy. Na podstawie m.in. przeprowadzonych symulacji komputerowych stwierdzono, że przyczyną zawalenia się 47-piętrowego budynku nie mógł być pożar, a jedynie niemal jednoczesne uszkodzenie wszystkich kolumn wewnątrz budynku. W przypadku budynków WTC 1 i WTC 2 pożar spowodowany rozbiciem się samolotów nie trwał długo i nie spowodował długotrwałego wzrostu temperatury, ponieważ całe paliwo pochodzące ze zbiorników samolotów wypaliło się od razu po katastrofie. Symulacje komputerowe miały pokazać, że temperatura pożarów wynosiła ponad 1000°C, a stal i żelazo stosowane w tego typu konstrukcjach zaczynają się topić dopiero w temperaturze ok. 1500°C. Według teorii spiskowej Twin Towers i WTC 7 zostały zniszczone na skutek zastosowania kontrolowanych detonacji ładunków wybuchowych. W oficjalnym raporcie National Institute of Standards and Technology unikano jakiejkolwiek dyskusji na temat możliwości podłożenia ładunków wybuchowych, gdyż zostało to arbitralnie wykluczone już na wstępie dochodzenia[57].

Jeszcze więcej pytań powstało w związku z atakiem na Pentagon. Olbrzymi Boeing, który w niego uderzył, był pilotowany przez Haniego Handżura, nisko ocenionego przez instruktorów jako pilot nawet dwuosobowych samolotów. Tymczasem 11 września pilotował on wielki samolot, z niewiarygodnym wprost opanowaniem i dokładnością wbijając w budynek maszynę lecącą z prędkością prawie 1000 km/h na wysokości zaledwie kilku metrów nad ziemią. Nie znaleziono szczątków samolotu, a zniszczenia, które stwierdzono w budynku po wypadku, były zbyt małe w stosunku do wielkości samolotu. Chociaż wielu naocznych świadków opisywało katastrofę, władze nie potrafiły

[55] M.A. Velez, *11 września: władza spisków*, Wirtualna Polska, 7 IX 2006 r., https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [dostęp: 11 IX 2006].

[56] M. Kucharczyk, *Wybuch, który miał zatrzeć ślady wielkiego spisku. Ta teoria o zamachach na WTC wciąż ma się dobrze*, gazeta.pl, 11 IX 2020 r., https://wiadomosci.gazeta.pl/wiadomosci/7,114881,26286855,kontrolowany-wybuch-ktory-mial-zatrzec-slady-ta-teoria-o-zamachach.html [dostęp: 12 IX 2021].

[57] Tamże.

pokazać żadnego nagrania wideo, na którym byłoby widać sylwetkę nadlatującego samolotu, mimo że w okolicy Pentagonu było zainstalowanych kilkadziesiąt kamer. Wszystkie ciała ofiar, z wyjątkiem jednego, zostały zidentyfikowane dzięki analizie DNA. Niejasne było, w jaki sposób zachowały się szczątki ludzkie, skoro nie znaleziono żadnych istotnych fragmentów samolotu, ponieważ „wyparowały" z powodu wysokiej temperatury (informacja dotycząca szczątków samolotu znalazła się w oficjalnej wersji raportu Komisji 11 Września). Te wątpliwości były wywołane pojawieniem się teorii o pocisku rakietowym, który trafił w Pentagon. Był to zatem kolejny dowód na spisek neokonserwatystów, którego celem było sfabrykowanie pretekstu do inwazji na Irak[58].

Inne wersje spiskowe były oparte na rzekomej wcześniejszej wiedzy wybranych osób na temat ataku, do którego doszło 11 września. To zagadnienie, dotyczące korzystnych operacji finansowych przeprowadzanych przed atakiem, poruszono m.in. w filmie *Fahrenheit 9.11* Michaela Moore'a. Z kolei brytyjska telewizja BBC oraz agencja Reuters poinformowały o zawaleniu się budynku WTC 7 ponad 20 minut przed tym zdarzeniem, co, zdaniem zwolenników teorii spiskowych, miało świadczyć o wcześniejszej wiedzy na temat zamachów. Na serwisie YouTube można było znaleźć umieszczony tam fragment wiadomości BBC, kiedy spikerka informuje o zawaleniu się WTC 7, podczas gdy za jej plecami widać pokazywaną na żywo panoramę Manhattanu ze stojącym tam nadal budynkiem. Według BBC była to pomyłka reporterki, która dopiero co przybyła na miejsce wydarzeń, oraz wina nieprawidłowej informacji otrzymanej z agencji Reuters. Agencja Reuters wydała oświadczenie, że informacja o zawaleniu się budynku WTC 7 została podana przez miejscową agencję i bez weryfikacji przekazana dalej. Według innej teorii spiskowej o zamachu wcześniej mieli być rzekomo ostrzeżeni żydzi, ponieważ żaden z nich nie zginął w WTC, mimo że wielu ich tam pracowało. Ta teoria była poparta tym, że na liście ofiar znajdował się tylko jeden Izraelczyk. Tymczasem nie każdy żyd jest obywatelem Izraela, a w wyniku ataku na WTC zginęło ok. 400 amerykańskich żydów. W krajach muzułmańskich natomiast rozpowszechniona była teoria, że spisek został przygotowany przez Izrael, o czym miało świadczyć to, że 11 września 2001 r. 4 tys. żydów nie przyszło do pracy w WTC, ponieważ zostali ostrzeżeni za pomocą SMS-ów[59].

Według zeznań Colina Powella, ówczesnego sekretarza stanu, część tzw. jastrzębi z otoczenia prezydenta Busha od razu chciała wykorzystać te wydarzenia jako sposób rozwiązania problemu z Irakiem. Innymi słowy – 11 września miał się stać pretekstem do wojny z Saddamem Husajnem. Tu znajduje się sedno spiskowych teorii na temat ataku z 11 września. Paul Wolfowitz, Donald Rumsfeld, Dick Cheney, brat prezydenta Jeb Bush – wszyscy ci ludzie w 1997 r. współtworzyli Project for the New American

[58] P. Łepkowski, *11 września 2001 roku: Dzień, który zmienił świat*, „Rzeczpospolita", 11 IX 2020 r., https://www.rp.pl/Historia/309099993-11-wrzesnia-2001-roku-Dzien-ktory-zmienil-swiat.html [dostęp: 12 IX 2020].

[59] R. Nogacki, *World Trade Center – Czy Żydzi wiedzieli wcześniej?*, Nasza Witryna, 6 VI 2013, https://web.archive.org/web/20130606091550/http://www.naszawitryna.pl/przewodnia_sila_19.html [dostęp: 9 VI 2021].

Century – PNAC (Projekt na rzecz Nowego Wieku Ameryki) – organizację przygotowującą intelektualne zaplecze przyszłej neokonserwatywnej administracji. Jesienią 2000 r., w dobie kampanii wyborczej, twórcy projektu opublikowali raport pod tytułem *Rebuilding America's Defenses* (*Odbudowa amerykańskiej obronności*). Był to apel o wzmocnienie militarnej dominacji USA na świecie i o swego rodzaju remilitaryzację po latach rozluźnienia spowodowanego końcem zimnej wojny. Autorzy wyrazili opinię, że bez nowego Pearl Harbor taka remilitaryzacja będzie trudnym i powolnym procesem. Bez wojny niezdyscyplinowani Amerykanie nie będą chcieli utrzymywać globalnego imperium. W myśl tej logiki wojna jest konieczna i aby zmotywować do niej społeczeństwo, konieczne jest „drugie" Pearl Harbor. Wieże World Trade Center, ikony Ameryki, na „nowy" Pearl Harbor nadawały się znakomicie. Wojna w Iraku miała zaś stanowić milowy krok w zaprowadzaniu „Pax Americana" w roponośnej Zatoce Perskiej[60].

Najbardziej fantastyczne interpretacje wydarzeń z 11 września mają wielu zwolenników i odrzucają niektóre argumenty bardziej wyważonych „spiskologów". W żadne teorie spiskowe nie wierzyli szanowani politycy Thomas H. Kean i Lee H. Hamilton – przewodniczący i współprzewodniczący Komisji 11 Września, ale i oni nie byli usatysfakcjonowani postawą rządu. Dwa lata po wydaniu oficjalnego raportu Komisji wspólnie napisali książkę *Without Precedent: The Inside Story of the 9/11 Commission* (*Bez precedensu: Komisja 11 Września od środka*). W umiarkowanych słowach opowiedzieli w niej o bezustannym zmaganiu się z administracją Busha i o coraz to nowych przeszkodach, które uniemożliwiały Komisji prowadzenie niezależnego śledztwa. W raporcie Komisji piętnowano brak zdecydowanych działań Białego Domu wobec pojawiających się długo przed atakami informacji przekazywanych przez CIA, że podejrzani ludzie planują uprowadzenie samolotów pasażerskich. *System alarmował czerwonym światłem* – taki tytuł nosi rozdział raportu dotyczący zlekceważonych przez administrację znaków, że szykuje się poważny atak na Stany Zjednoczone. Natomiast po zamachach zaskakująco szybko ustalono, kto ich dokonał, jak i po co. Zadziwiająco sprawnie pozbyto się złomu z WTC. Wprost z nowojorskiego Manhattanu popłynął do chińskich hut. Amerykański filozof David Ray Griffin zauważył, że to właśnie oficjalna, propagowana przez rząd wersja wydarzeń z 11 września 2001 r. nosiła znamiona teorii spiskowej[61].

Zakończenie

Zarówno przed, jak i po roku 2001 w USA oraz innych rejonach świata dochodziło do zamachów terrorystycznych, jednak nigdy na taką skalę, jak w przypadku ataku z 11 września. Jego przyczyny tkwiły w szerzącym się islamskim fanatyzmie, którego przedstawiciele uzurpują sobie prawo do przedstawiania tylko siebie jako prawdziwie

[60] M.A. Velez, *11 września: władza spisków*, Wirtualna Polska, 7 IX 2006 r., https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [dostęp: 11 IX 2006].

[61] Tamże.

wierzących, a innych nazywają niewierzącymi, z którymi należy walczyć. Nałożyło się na to pospolite w świecie muzułmańskim przekonanie o zaangażowaniu się USA po stronie Izraela w nierozwiązanym konflikcie palestyńsko-izraelskim, atak na Irak w 1991 r. i sankcje nałożone na to państwo, wspieranie przez Waszyngton reżimów w państwach muzułmańskich oraz nurtujące świat (także obecnie) problemy społeczno-ekonomiczne i proces globalizacji, któremu muzułmanie starają się przeciwstawić, eksponując odrębność religijną i przywiązanie do tradycji. Stany Zjednoczone, najbogatszy i najpotężniejszy ekonomicznie kraj na świecie, są obwiniane przez wiele społeczności, w tym muzułmanów, za problemy ekonomiczne powstałe w różnych regionach globu. Z jednej strony z powodu ekspansji amerykańskich koncernów, a z drugiej, zdaniem niektórych, zbyt małej pomocy ekonomicznej i technologicznej dla ubogich regionów. Krytycy wychodzą z założenia, że problem biedy na świecie jest także problemem amerykańskim w tym sensie, że Stany Zjednoczone jako supermocarstwo powinny jeszcze bardziej niż dotychczas poczuwać się do współodpowiedzialności za losy współczesnego świata, choćby udzielając pomocy w rozwiązywaniu wspomnianych problemów społecznych i ekonomicznych[62]. Atak na WTC, symbol ekonomicznej potęgi Stanów Zjednoczonych, był rodzajem swoistej zemsty za brak dostatecznego zaangażowania się USA w pomoc dla ubogich regionów świata, przede wszystkim muzułmańskiego, a atak na Pentagon, symbol wojskowej potęgi USA, był zemstą za interwencje militarne na Bliskim Wschodzie.

Do powyższych uwag należy dołączyć wyjaśnienia Ajmana az-Zawahiriego, ideologa Al-Kaidy i zastępcy Osamy bin Ladena. W grudniu 2001 r. w arabskojęzycznej gazecie wydawanej w Londynie, „Asz-Szark al-Awsat' („Bliski Wschód"), opublikował on manifest pt. *Fursan taht rajat al-Nabi* (*Rycerze pod sztandarem proroka*). Stwierdził w nim m.in., że w latach 90. XX w. nie spełniły się nadzieje, które zrodził zwycięski dżihad w Afganistanie. Zwolennicy dżihadu ponieśli wówczas ostateczną klęskę w całym świecie muzułmańskim, gdyż nie zdołali zmobilizować u swego boku tysięcy muzułmanów w celu wspólnego obalania rządzących w krajach muzułmańskich, określanych mianem „bliskiego wroga". Zaradzić niepowodzeniu mogłaby jedynie radykalna zmiana strategii, czyli silny cios zadany Stanom Zjednoczonym. Zuchwałość i skala tego ataku miały przekonać rzesze niezdecydowanych muzułmanów o nieodpartej mocy sił dżihadu oraz słabości „wspaniałej Ameryki", protektorki „apostatów" z Bliskiego Wschodu i Afryki Północnej. Rozgłos w światowych mediach na temat ataku na USA miał zmobilizować muzułmanów, którzy przyłączą się do Al-Kaidy jako awangarda prowadząca za sobą tysiące braci w wierze do zwycięskiego dżihadu zarówno przeciwko „bliskiemu", jak i „dalekiemu wrogowi", czyli Zachodowi[63].

[62] Rzadko jednak precyzuje się, w jaki sposób należy to czynić. Najczęściej oczekuje się pomocy finansowej. Jeśli Stany Zjednoczone jej nie udzielały zgodnie z wyobrażeniami oczekujących, to często stawało się to przyczyną antyamerykańskich wystąpień.

[63] G. Kepel, *Fitna. Wojna w sercu islamu*, Warszawa 2006, s. 11–12.

Wydarzenia z 11 września 2001 r. wywarły negatywny wpływ na gospodarkę, przede wszystkim Stanów Zjednoczonych, ale nie tylko. W związku z zagrożeniem terrorystycznym zmniejszyła się na przykład liczba turystów w USA. Ucierpiały na tym przede wszystkim stany żyjące z turystyki, w tym Floryda, która – jak szacowano – tylko na przełomie roku 2001/2002 utraciła ok. 30 mld dolarów z powodu zmniejszenia liczby turystów. Miliardy dolarów straciły także linie lotnicze oraz instytucje ubezpieczeniowe. Te pierwsze z powodu zmniejszonej liczby pasażerów, te drugie zaś z powodu wypłaty odszkodowań. Pojawiły się liczne utrudnienia w transporcie międzynarodowym spowodowane zaostrzeniem środków bezpieczeństwa. Wzmożono kontrolę międzynarodowych przepływów finansowych w celu ustalenia i likwidacji źródeł finansowania organizacji terrorystycznych. Wydarzenia z 11 września uświadomiły wielu krajom, że nikt – nawet najpotężniejsze państwo – nie może czuć się bezpieczny, a więc jest konieczna ścisła współpraca międzynarodowa w celu zwalczania terroryzmu oraz rozwiazywania palących problemów współczesnego świata, konfliktów i napięć na arenie międzynarodowej.

Atak z 11 września 2001 r. stał sie punktem zwrotnym w walce z terroryzmem międzynarodowym. Pokazał nieznaną dotychczas skalę zagrożeń ze strony organizacji terrorystycznych, łącznie z możliwością użycia przez nie broni masowego rażenia. Reakcja na tego typu terroryzm musiała być adekwatna do potencjalnego niebezpieczeństwa. Wydarzenia z 11 września dokonały przełomu w polityce amerykańskiej. Stany Zjednoczone ogłosiły wojnę przeciwko terroryzmowi. Pierwszym aktem było uderzenie na Islamski Emirat Afganistanu, czyli siedzibę sojusznika Al-Kaidy. Amerykańska operacja Enduring Freedom była zgodna z Kartą Narodów Zjednoczonych, która nie ogranicza prawa do samoobrony, dopóki sprawy nie przejmie Rada Bezpieczeństwa. Udział innych państw, w tym Polski, w tej operacji był pomocą udzieloną USA, na co zezwoliła karta ONZ. We wrześniu 2002 r. przyjęto w USA doktrynę zezwalającą na przeprowadzenie uderzenia prewencyjnego w obliczu realnej groźby działań terrorystycznych lub posiadania broni masowego rażenia przez tzw. państwa rozbójnicze. Nowa doktryna została zastosowana w następnym roku przeciw Irakowi. Wojna z terroryzmem ujawniła jednak poważne różnice pomiędzy Europą a Stanami Zjednoczonymi. Chodziło nie tyle o różnice w potencjale wojskowym i związanym z tym innym sposobem prowadzenia działań wojennych, ile o odmienne postrzeganie roli instytucji oraz sił międzynarodowych, a także o różną ocenę scenariuszy możliwych działań i środków wykorzystywanych w ramach walki z terroryzmem.

Atak na Stany Zjednoczone był zaskoczeniem, wstrząsem i szokiem zarówno dla tego kraju, jak i całej społeczności międzynarodowej. Istniejące struktury i organizacje bezpieczeństwa międzynarodowego okazały się nieskuteczne. Siła militarna i cały arsenał najbardziej zaawansowanych rodzajów broni nie były w stanie zapewnić bezpieczeństwa wewnętrznego. Stany Zjednoczone i świat stanęły wobec nowych zagrożeń. Zainicjowano wiele przedsięwzięć mających na celu zapewnienie bezpieczeństwa i wyeliminowanie terroryzmu międzynarodowego. Walka z nim stała się głównym kierunkiem aktywności

społeczności międzynarodowej, doprowadziła do zmiany priorytetów w polityce zagranicznej USA, nasiliła tendencje do jednostronnych działań prewencyjnych.

Należy też pamiętać, że wojna z terroryzmem przysporzyła olbrzymich korzyści finansowych amerykańskiej branży wojskowo-przemysłowej. Już we wrześniu i październiku 2001 r. nastąpił wzrost cen akcji takich koncernów, jak Lockheed Martin, Northop Grumman i Rytheon. Producenci sprzętu wojskowego odnieśli niespodziewane korzyści, nie tylko dlatego, że Zachód podjął zdecydowane kroki przeciw państwom, organizacjom i osobom podejrzanym o terroryzm, lecz także na skutek uruchomienia pakietów pomocowych dla krajów rozwijających się. Dzięki pakietowi „naprawczemu" prezydenta Busha, mającemu pomóc w ożywieniu gospodarki, zyskała każda większa korporacja. Ze 100 mld dolarów wydanych z tego pakietu tylko w listopadzie 2001 r. 75 proc. zostało przeznaczone na subwencje pokrywające podatki przedsiębiorstw, zwłaszcza największych korporacji[64].

Sukces ataku z 11 września obrócił się przeciw Al-Kaidzie. Siłom USA nie udało się w Afganistanie wyeliminować kierownictwa tej organizacji, które wymknęło się do Pakistanu dzięki pomocy sprzymierzonych z nią Afgańczyków. Przechwycenie dokumentów i taśm wideo Al-Kaidy w należących do niej „bezpiecznych domach" pozwoliło lepiej poznać strukturę i zrozumieć dynamikę tej organizacji, a także udaremnić zamach w Singapurze w grudniu 2001 r. Siły amerykańskie doprowadziły do rozproszenia kierownictwa Al-Kaidy, zlikwidowały obozy szkoleniowe i w dużym stopniu zredukowały możliwości wzajemnego komunikowania się jej członków i dowódców z centralą, zajmującą się wsparciem logistycznym lokalnych operacji. Osamę bin Ladena udało się wyeliminować dopiero dziesięć lat później.

Atak islamskich terrorystów na Stany Zjednoczone ukazał prawdziwe oblicze społeczeństw krajów muzułmańskich. Widok walących się wież WTC był witany okrzykami radości milionów muzułmanów w Indonezji, Malezji, Bangladeszu, Indii, Egipcie, Sri Lance, Omanie, Jemenie, Sudanie, Bośni i Hercegowinie, Afganistanie, Pakistanie i Wielkiej Brytanii[65]. Wiwatujący mieszkańcy na ulicach arabskich miast stali się, w powszechnym odbiorze, symbolem nieskrywanej nienawiści do Stanów Zjednoczonych. Były to obrazy szokujące dla mieszkańców Zachodu, ale przedstawiały żywiołowy i autentyczny stosunek dużej części muzułmanów do tego kraju. Przyszłość pokazała, że podobną nienawiść do całej cywilizacji zachodniej żywią także ci wyznawcy, którzy mieszkają w Europie. Po 11 września 2001 r. znacznie wzrosło zainteresowanie islamem. Zaobserwowano, że wielu młodych ludzi w Europie (a także w Polsce) dokonywało konwersji na islam. Zaczęto zwracać większą uwagę na radykalny islam, którego ideologia dała początek istnieniu i aktywnej działalności ekstremistycznych organizacji w krajach muzułmańskich. Wiele z nich, łącznie z Al-Kaidą, przeprowadzało krwawe zamachy

[64] D. Whyte, *Interesy po staremu? Moralność wielkich korporacji i „wojna z terroryzmem"*, w: *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, P. Scraton (red.), Warszawa 2003, s. 193–194.

[65] P.L. Williams, *Al-Kaida – bractwo…*, s. 96–97.

terrorystyczne już przed 2001 r., lecz to właśnie ataki na Nowy Jork i Waszyngton wyznaczyły cezurę w najnowszych dziejach terroryzmu. Fundamentalistyczny nurt islamu skupił całą uwagę naukowców i mediów, zasypujących Zachód mniej lub bardziej rzetelnymi informacjami. Tylko do końca 2001 r. w literaturze angielskojęzycznej ukazało się ok. 800 książek poświęconych tej problematyce. Amerykański atak na Irak w 2003 r. i odrodzenie się ruchu talibów w Afganistanie pogłębiły te tendencje. Interwencja NATO w obu tych krajach przyczyniła się do wzrostu zagrożenia terrorystycznego w Europie, a jej mieszkańcy stali się celem islamskich ekstremistów w Afryce i Azji.

Bibliografia

11 września. Przyczyny i konsekwencje w opiniach intelektualistów, Scraton P. (red.), Warszawa 2003, Dialog.

Armstrong K., *Pola krwi. Religia i przemoc*, Warszawa 2017, Wydawnictwo W.A.B.

Bergen P.L., *Osama bin Laden. Portret z bliska*, Warszawa 2007, PIW.

Chaliand G., Blin A., *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020, PIW.

Coll S., *Rodzina Bin Ladenów. Arabskie losy w amerykańskim stuleciu*, Warszawa 2015, Kurhaus Publishing.

Dietl W., Hirschmann K., Tophoven R., *Terroryzm*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Elsässer J., *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007, MUZA.

Izak K., *Fałszywe dokumenty w rękach terrorystów*, „Człowiek i Dokumenty" 2014, nr 32, s. 7–20.

Kepel G., *Fitna. Wojna w sercu islamu*, Warszawa 2006, Dialog.

Streatfeild D., *Świat po 11 września*, Warszawa 2011, Oficyna Wydawnicza ŁośGraf.

Szymańska M., *Eksplozja terroryzmu w USA a przekształcenia w amerykańskich służbach specjalnych po 11 września 2001 r.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 186–210.

Whyte D., *Interesy po staremu? Moralność wielkich korporacji i „wojna z terroryzmem"*, w: *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, Scraton P. (red.), Warszawa 2003, Dialog, s. 187–194.

Williams P.L., *Al-Kaida – bractwo terroru*, Warszawa 2002, Studio Emka.

Wright L., *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, Wydawnictwo Czarne.

Źródła internetowe

https://en.wikipedia.org/wiki/Abdulaziz_al-Omari [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Ahmed_al-Nami [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Ahmed_al-Ghamdi [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Hani_Hanjour [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Mohamed_Atta [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Salem_al-Hazmi [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Satam_al-Suqami [dostęp: 1 VI 2021].

https://en.wikipedia.org/wiki/Zacarias_Moussaoui [dostęp: 1 VI 2021].

https://pl.melayukini.net/wiki/Betty_Ong [dostęp: 1 VI 2021].

https://pl.melayukini.net/wiki/Hamza_al-Ghamdi [dostęp: 4 VI 2021].

https://pl.melayukini.net/wiki/Hani_Hanjour [dostęp: 4 VI 2021].

https;//pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks [dostęp: 4 VI 2021].

https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks#American_Airlines_Flight_11:_One_World_Trade _Center,_North_Tower [dostęp: 3 VI 2021].

https://pl.melayukini.net/wiki/Madeline_Amy_Sweeney [dostęp: 1 VI 2021].

https://pl.melayukini.net/wiki/Marwan_al-Shehhi [dostęp: 4 VI 2021].

https://pl.melayukini.net/wiki/Nawaf_al-Hazmi [dostęp: 4 VI 2021].

https://pl.melayukini.net/wiki/Satam_al-Suqami [dostęp: 1 VI 2021].

https://pl.melayukini.net/wiki/Wail_al-Shehri [dostęp: 1 VI 2021].

https://pl.melayukini.net/wiki/Ziad_Jarrah [dostęp: 4 VI 2021].

https://pl.wikipedia.org/wiki/Katastrofa_lotu_American_Airlines_11 [dostęp: 1 VI 2021].

https://pl.wikipedia.org/wiki/Katastrofa_lotu_United_Airlines_93 [dostęp: 4 VI 2021].

https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [dostęp: 7 VI 2021].

https://pl.xcv.wiki/wiki/United_Airlines_Flight_175 [dostęp: 4 VI 2021].

Krzemirski A., *Rocznica 11 września. Olbrzymie odszkodowania i strach przed podróżami*, Parkiet, 11 IX 2002 r., https://www.parkiet.com/artykul/260530.html [dostęp: 6 VI 2021].

Kucharczyk M., *Wybuch, który miał zatrzeć ślady wielkiego spisku. Ta teoria o zamachach na WTC wciąż ma się dobrze*, gazeta.pl, 11 IX 2020 r., https://wiadomosci.gazeta.pl/wia-

domosci/7,114881,26286855,kontrolowany-wybuch-ktory-mial-zatrzec-slady-ta-teoria--o-zamachach.html [dostęp: 12 IX 2020].

Lichtenberg A., Dudek B., *Zamachy 11 września: historia „Grupy Hamburskiej"*, https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [dostęp: 12 IX 2011].

Łepkowski P., *11 września 2001 roku: Dzień, który zmienił świat*, „Rzeczpospolita", 11 IX 2020 r., https://www.rp.pl/Historia/309099993-11-wrzesnia-2001-roku-Dzien-ktory-zmienil--swiat.html [dostęp: 12 IX 2020].

Nieśli pomoc po ataku na WTC, po latach ciężko zachorowali. Śmierć strażaków - ojca i syna - w wyniku nowotworów, Polsat News, 19 VIII 2017 r., https://www.polsatnews.pl/wiadomosc/2017-08-19/niesli-pomoc-po-ataku-na-wtc-smierc-strazakow-w-wyniku-nowotworow/ [dostęp: 6 VI 2021].

Nogacki R., *World Trade Center – Czy Żydzi wiedzieli wcześniej?*, Nasza Witryna, 6 VI 2013 r., https://web.archive.org/web/20130606091550/http://www.naszawitryna.pl/przewodnia_sila_19.html [dostęp: 9 VI 2021].

Piecing together the terrorist jigsaw, „The Guardian", 15 X 2001 r., https://www.theguardian.com/world/2001/oct/15/worlddispatch.brianwhitaker [dostęp: 17 I 2001].

Rodziny ofiar zamachów na WTC z 11 września pozywają Arabię Saudyjską, Bankier.pl, 21 III 2017 r., https://www.bankier.pl/wiadomosc/Rodziny-ofiar-zamachow-na-WTC-z-11-wrzesnia-pozywaja-Arabie-Saudyjska-3668756.html [dostęp: 22 III 2017].

Spisek World Trade Center, Laif, 9 V 2008 r., https://web.archive.org/web/20090615224350/http://laif.co.uk/art,spisek_world_trade_center,1496.html [dostęp: 9 VI 2021].

USA: Kongres ujawnił tajną część raportu o zamachach z 11 września, „Dziennik Gazeta Prawna", 15 VII 2016 r., https://www.gazetaprawna.pl/wiadomosci/artykuly/960454,usa-kongres--ujawnil-tajna-czesc-raportu-o-zamachach-z-11-wrzesnia.html [dostęp: 16 VII 2016].

Velez M.A., *11 września: władza spisków*, Wirtualna Polska, 7 IX 2006 r., https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [dostęp: 11 IX 2006].

Werkhäuser N., *Hamburg: pomocnik zamachowców z 11 września wydalony do Maroka*, Deutsche Welle, 15 X 2018 r., https://www.dw.com/pl/hamburg-pomocnik-zamachowców-z--11-września-wydalony-do-maroka/a-45895869 [dostęp: 16 X 2018].

We have some planes, National Commission on Terrorist Attacks Upon the United States, https://www.9-11commission.gov/report/911Report_Ch1.htm [dostęp: 3 VI 2021].

The 9/11 Commission Report, https://govinfo.library.unt.edu/911/report/911Report.pdf, [dostęp: 6 VI 2021].

Abstrakt

Serię ataków terrorystycznych z 11 września 2001 r. w USA, największych w historii świata, przeprowadziło 19 osób. Wśród nich było 15 Saudyjczyków, dwóch obywateli Zjednoczonych Emiratów Arabskich, Libańczyk i Egipcjanin. Trzech spośród tej czwórki tworzyło komórkę hamburską, która stanowiła trzon całej operacji. Kierował nią Egipcjanin Muhammad Ata as-Sajjid. Pilotował on samolot Boeing 767 American Airlines, lot nr 11, który pierwszy uderzył w północną wieżę WTC. Marwan asz-Szihhi był pilotem Boeinga 767 United Airlines, lot nr 175, który rozbił się o południową wieżę WTC. Hani Handżur zasiadł za sterami samolotu Boeing 757 American Airlines odbywającego lot nr 77. Celem ataku był Pentagon. Pilotowi czwartego samolotu – Boeinga 757 United Airlines, lot nr 93 – Zijadowi Dżarrahowi nie udało się osiągnąć celu, prawdopodobnie Kapitolu, ponieważ pasażerowie przystąpili do odbicia samolotu z rąk terrorystów. Maszyna spadła na ziemię w Pensylwanii. W wydarzeniach z 11 września ogółem zginęło 2996 osób, w tym 19 terrorystów, a 6291 zostało rannych[66]. Wśród ofiar śmiertelnych było sześcioro Polaków. W akcji ratunkowej zginęło 343 strażaków.

Zamachy wyrządziły olbrzymie straty materialne. Duże koszty poniosły zwłaszcza towarzystwa ubezpieczeniowe i reasekuracyjne, linie lotnicze oraz producenci samolotów, a także branża turystyczna. Ogromne straty związane ze zniszczeniem nowojorskiego World Trade Center oraz dezorganizacją systemu finansowego musiały zostać pokryte przez towarzystwa asekuracyjne, zaangażowane w działalność na rynku amerykańskim.

Atak terrorystyczny na USA stał się impulsem do największej od 1947 r. reformy amerykańskich służb specjalnych. Waszyngton podjął decyzję dotyczącą konieczności stworzenia systemu efektywnie przeciwdziałającego zagrożeniom o charakterze terrorystycznym oraz skutecznie ostrzegającego w przypadku ich wystąpienia. Wiązało się to ze wzmocnieniem struktur mających uprawnienia operacyjno-rozpoznawcze, zwiększeniem zakresu ich zadań oraz usprawnieniem ich zdolności do koordynacji działań. Większość regulacji prawnych została zawarta w dokumencie znanym powszechnie pod nazwą *USA Patriot Act* z 26 października 2001 r. Najważniejsze były jednak skutki o charakterze międzynarodowym. Atakami na WTC i Pentagon Al-Kaida wpłynęła na światową politykę przez skłonienie Waszyngtonu do wypowiedzenia „wojny z terroryzmem". W jej ramach siły amerykańskie, wspierając Sojusz Północny, doprowadziły do upadku Islamskiego Emiratu Afganistanu, a następnie wkroczyły do Iraku, co jednak w dłuższej perspektywie okazało się jedną z najbardziej spektakularnych pomyłek strategicznych w dziejach wojskowości.

Atak z 11 września 2001 r. spowodował również, że pojawiło się wiele teorii spiskowych. Ich propagowanie w mediach, filmach dokumentalnych przyczyniło się do

[66] https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [dostęp: 7 VI 2021].

spadku zaufania do amerykańskiego rządu. W sprawie WTC 7 do dzisiaj prężnie działa organizacja o nazwie Architekci i Inżynierowie na rzecz Prawdy o 9/11, która szczyci się, że skupia 3,3 tys. architektów i inżynierów z całych Stanów Zjednoczonych. Celem tych osób jest ujawnienie „prawdy", czyli tego, że bliźniacze wieże nie zawaliły się z powodu uderzenia samolotów pilotowanych przez terrorystów, tak samo jak WTC 7, która nie uległa zniszczeniu na skutek oderwania się fragmentu drugiego samolotu. W ich ocenie szkody spowodowane przez samoloty były dalece niewystarczające, aby doprowadzić do takiej katastrofy. Wierzą, że ktoś musiał podłożyć ładunki wybuchowe.

Słowa kluczowe: Al-Kaida, atak terrorystyczny, komórka hamburska, Pentagon**,** WTC**.**

Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA

Abstract

The series of terrorist attacks on 11 September 2001 in the USA, the largest in the history of the world, was carried out by 19 people. Among them were 15 Saudis, two UAE nationals, a Lebanese and an Egyptian. Three of the four formed the Hamburg cell, which was the backbone of the entire plot. It was led by the Egyptian Muhammad Atta el-Sayed. He flew Boeing 767 aircraft American Airlines Flight 11, which first struck the North Tower of the WTC. Marwan al-Shehhi was the pilot of Boeing 767 aircraft United Airlines Flight 175, which crashed into the South Tower of the WTC. Hani Hanjour sat at the controls of the Boeing 757 aircraft American Airlines flight 77. It was the third machine to target the Pentagon. The pilot of the fourth plane - Boeing 757 aircraft United Airlines Flight 93 - Ziad Jarrah failed to reach his destination, possibly the Capitol, because the passengers decided to take over the control of the plane from the terrorists. The machine crashed in Pennsylvania. In the events of 9/11, a total of 2,996 people were killed, including 19 terrorists, and 6,291 were injured . Six Poles were among the fatalities. 343 firefighters died in the rescue operation.

The attacks caused enormous material losses. Particularly high costs were incurred by insurance and reinsurance companies, airlines and aircraft manufacturers, as well as the tourism industry. The huge losses related to the destruction of the New York City World Trade Center and the disruption of the financial system had to be covered by insurance companies involved in the operations on the American market.

The terrorist attack on the USA was the impetus for the largest reform of the American secret services since 1947. Washington made a decision regarding the need to create a system that would effectively counteract terrorist threats and effectively warn

in the event of their occurrence. This was related to the strengthening of structures with operational and reconnaissance powers, increasing the scope of their tasks and improving their ability to coordinate. Most of the legal regulations were expressed in the document commonly known as the USA Patriot Act of 26 October 2001. The most critical, however, were the international repercussions. By the attacks on the WTC and the Pentagon, al-Qaeda influenced world politics by prompting Washington to declare a "war on terror". Within its framework, American forces, supporting the so-called Northern Alliance led to the collapse of the Islamic Emirate of Afghanistan, and then entered Iraq, which in the long run turned out to be one of the most spectacular and deadly strategic mistakes in the history of the military.

At the same time the September 11 attacks sparked many conspiracy theories. Their propagation in the media, in documentaries, as well as in articles, contributed to undermining trust in the American government. An organization called Architects and Engineers for 9/11 Truth which boasts 3.3 thousand architects and engineers from all over the United States, is still very active in researching the case of 7 WTC. Its mission is to establish the truth that the twin towers did not collapse due to the impact of terrorist-piloted planes, as well as the destruction of WTC 7 was not a result of the detachment of a fragment of the second plane. In the opinion of members of this organisation, the damage caused by the planes was far from sufficient to lead to such a catastrophe. They believe someone must have planted explosives.

Keywords: Al-Qaeda, terrorist attack, Hamburg cell, Pentagon, WTC.

II

RECENZJE

REVIEWS

KRZYSZTOF IZAK
ORCID: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.028.14305

Ewa Martusewicz-Pawlus, *Euroislam contra islamizm. Drogi i bezdroża bezpieczeństwa obywateli Unii Europejskiej*[1]

W 2020 r. nakładem wydawnictwa Difin ukazała się interesująca monografia dr Ewy Martusewicz-Pawlus pod wyżej wymienionym tytułem. Nieduża objętościowo publikacja zawiera teoretyczne rozważania oraz wyniki badań autorki dotyczące problematyki muzułmańskich imigrantów w Niemczech oraz relacji przybyszów ze społeczeństwem kraju przyjmującego, z uwzględnieniem sytuacji w Polsce. W notce biograficznej na tylnej stronie okładki można przeczytać, że Martusewicz-Pawlus, która na stałe mieszka w Niemczech, jest m.in. autorką artykułów poświęconych religijności niemieckiej i polskiej młodzieży.

Na wstępie swojej książki badaczka definiuje pojęcie „euroislam", które do narracji naukowej zostało wprowadzone w 1991 r. przez Bassama Tibiego, niemieckiego badacza pochodzenia syryjskiego, autora książki zatytułowanej *Fundamentalizm religijny*. Do Tibiego autorka odwołuje się wiele razy. W jego ujęciu euroislam jest „zsekularyzowaną formą islamu" (o ile w ogóle islam można laicyzować). *Jej istota polega na dostosowaniu obowiązków i zasad islamu wyznawanych przez muzułmanów żyjących na obszarze Europy do wartości nowoczesnej kultury europejskiej. Głównym założeniem koncepcji euroislamu jest odrzucenie dwóch integralnych elementów islamu, jakimi są dżihad i szariat*[2]. Autorka stawia kontrowersyjną tezę, że obecna sytuacja, w jakiej znalazła się Unia Europejska, wymusza na jej krajach realizowanie koncepcji euroislamu, m.in. przez wspieranie działalności liberalnych muzułmanów, promujących islam w duchu poszanowania konstytucji i praw człowieka. Rozważania teoretyczne, oparte głównie na publikacjach niemieckojęzycznych, autorka uzupełniła wynikami

[1] E. Martusewicz-Pawlus, *Euroislam contra islamizm. Drogi i bezdroża bezpieczeństwa obywateli Unii Europejskiej*, Warszawa 2020, Difin, 211 s.

[2] B. Tibi, *Fundamentalizm religijny*, Warszawa 1997, s. 164.

badań ankietowych oraz dziesięcioma wywiadami eksperckimi przeprowadzonymi w Niemczech i Polsce. Głównym celem publikacji jest wykazanie, że do harmonijnej koegzystencji muzułmanów ze społeczeństwami Zachodu może doprowadzić jedynie realizowanie koncepcji euroislamu. Tymczasem zdaniem autora recenzji ten cel jest niemożliwy do osiągnięcia, ponieważ jego podstawą są przesłanki z lat 90. XX w., które nie przystają do obecnej rzeczywistości i obserwowanej islamizacji Europy.

Książka składa się z czterech rozdziałów, z których każdy jest zakończony wnioskami. Recenzja połowy publikacji stwarza jednak duże problemy, gdyż własnych myśli i spostrzeżeń autorki jest w tej części niewiele. Martusewicz-Pawlus opiera się głównie na pracach innych badaczy, cytuje ich tezy i wnioski, niekiedy kontrowersyjne, ale rzadko się do nich ustosunkowuje.

W rozdziale pierwszym autorka analizuje zderzenie cywilizacji na kontynencie europejskim. Punktem wyjścia do tych rozważań są słynne prace Samuela P. Huntingtona – artykuł pt. *Zderzenie cywilizacji?*, opublikowany w 1993 r. na łamach magazynu „Foreign Affairs"[3], oraz książka pt. *Zderzenie cywilizacji i nowy kształt ładu światowego*[4]. W tej drugiej publikacji autor wyodrębnił na świecie dziewięć cywilizacji: japońską, chińską, buddyjską, hinduistyczną, islamską, prawosławną, zachodnią, latynoamerykańską i afrykańską (z wyłączeniem Afryki Północnej, której kraje należą do cywilizacji islamskiej). Ważną rolę w tych cywilizacjach odgrywają państwa-ośrodki, odpowiadające za powstanie i utrzymanie nowego ładu światowego. W przypadku cywilizacji zachodniej są to Stany Zjednoczone w Ameryce Północnej oraz Francja i Niemcy w Europie. W cywilizacji islamskiej taką rolę odgrywa Turcja, a w mniejszym stopniu Arabia Saudyjska. Autorka definiuje pojęcia z zakresu współczesnej cywilizacji i kultury, ale nie ukazuje ich historycznego kontekstu. A przecież współczesne cywilizacje czerpią z myśli i osiągnięć starożytnych przodków – cywilizacji Mezopotamii, Egiptu, Anatolii, egejskiej, grecko-hellenistycznej, rzymskiej, Chin, Indii czy Indochin. Wyznacznikiem każdej z nich był rozwój miast i pisma. W obrębie jednej cywilizacji mogło rozwijać się wiele kultur.

Martusewicz-Pawlus zajmuje krytyczne stanowisko wobec Huntingtonowskiej teorii zderzenia cywilizacji. Odwołuje się przy tym do publikacji, w których autorzy negują koncepcję Huntingtona, a mianowicie potraktowanie przez niego islamu jako monolitu i wspólnej kultury, rozciągającej się od Nigerii po Indonezję, oraz jego przekonania o istnieniu konfliktów międzycywilizacyjnych, w tym przede wszystkim między cywilizacją zachodnią a islamem. Tymczasem większość konfliktów rozgrywa się wewnątrz cywilizacji islamskiej. Biorąc pod uwagę narastającą falę migracji do Europy, wzrastającą liczebność populacji muzułmanów w UE oraz nasilenie konfliktów między diasporą muzułmańską a społecznościami państw przyjmujących, autorka recenzowanej książki stoi jednak na stanowisku, że wizja Huntingtona (zmarł w 2008 r.) przynajmniej częściowo

[3] S.P. Huntington, *The Clash of Civilization?*, „Foreign Affairs" 1993, nr 3, https://www.foreignaffairs.com/system/files/c0007.pdf [dostęp: 26 II 2021].

[4] S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2008.

wytrzymuje próbę krytyki. Martusewicz-Pawlus zwraca uwagę na związki cywilizacji islamu i cywilizacji zachodniej. Wyróżnia trzy fale ekspansji islamskiej. Pisze: *Pierwsza fala podbojów arabskich w Afryce, zapoczątkowana w 711 roku, doprowadziła muzułmanów do Ceuty. Jeszcze w tym samym roku doszło do decydującego starcia pod Jerez de la Frontera, w którym Tarik ibn Zijad pokonał wojska Wizygotów i położył podwaliny nowego kalifatu Al-Andalus, zapewniając muzułmanom kilkusetletnie panowanie na terenach dzisiejszej Hiszpanii* (s. 36). O ile do drugiego zdania tego cytatu nie można mieć zastrzeżeń, to pierwsze mija się z prawdą. Pierwsza fala podbojów arabskich w Afryce została zapoczątkowana w 640 r. wyprawą wojsk Amra ibn al-Asa do Egiptu. W 706 r. Arabowie zdobyli Tanger i dotarli do Oceanu Atlantyckiego, a trzy lata później opanowali Ceutę (starożytne Septem). Tak więc do 711 r. arabski podbój północnego wybrzeża Afryki, a dokładniej terytoriów ograniczonych na południu limesem rzymskim, praktycznie się zakończył i rozpoczął się podbój Półwyspu Iberyjskiego. W tym miejscu warto zwrócić uwagę na pewien istotny element w islamskim podboju Afryki. Nie ma o tym wzmianki w omawianej książce, a miało to duże znaczenie dla współczesnego oblicza islamu w Afryce, do którego odwołują się Tibi i cytująca go autorka. Otóż w X–XII w. na islam przechodzili władcy królestw Sahelu oraz członkowie tamtejszych elit. Byli oni gwarantami tradycyjnych kultów. Lud przyjmował islam dopiero w XIX w., podczas walk różnych dżihadystycznych ruchów, w tym bractw sufickich. Nieprawdziwe jest również inne stwierdzenie zawarte w książce: *Konstantynopol przemianowano na Stambuł i ustanowiono nową stolicą Imperium Osmańskiego, które w szczytowym okresie swojego rozwoju obejmowało trzy kontynenty: Azję Południowo-Wschodnią, Afrykę Północną oraz Europę Południowo-Wschodnią* (s. 36). W Azji Imperium Osmańskie nie sięgało dalej na wschód niż poza tereny obecnego Iraku.

Charakteryzując islam i jego specyfikę, autorka podaje nieaktualne dane statystyczne dotyczące liczby wyznawców islamu w najludniejszych krajach muzułmańskich. Opiera się na pracy Heinza Halma[5] i wymienia (s. 39): Indonezję (prawie 200 mln muzułmanów), Pakistan (174 mln), Indie (160 mln), Bangladesz (145 mln), Egipt (78 mln) oraz Turcję i Iran (po 73 mln). Należy jednak pamiętać, że książka Halma została wydana pięć lat przed publikacją autorki. Według danych Wikipedii bardziej aktualne dane statystyczne dla tych krajów przedstawiają się następująco: Indonezja – ponad 230 mln muzułmanów, Pakistan – ok. 200 mln, Indie – ponad 190 mln, Bangladesz – ponad 150 mln, Egipt – ok. 90 mln, a Turcja i Iran przekroczyły liczbę 82 mln muzułmanów. To są dane z lat 2017–2020. Niezbyt poprawne jest również podanie za Halmem liczby muzułmanów zamieszkujących obszary byłych republik Związku Radzieckiego (70 mln). Powinno się raczej wyodrębnić państwa Azji Centralnej i podać populację wyznawców islamu zamieszkujących Kazachstan (ok. 14 mln), Kirgistan (ponad 5 mln), Tadżykistan (8 mln), Turkmenistan (ok. 6 mln), Uzbekistan (ponad 30 mln) oraz Azerbejdżan (ok. 9 mln) na Zakaukaziu i osobno wymienić przybliżoną liczbę muzułmanów zamieszkujących Federację Rosyjską (ok. 15–20 mln). Następnie

[5] H. Halm, *Der Islam. Geschichte und Gegenwart*, München 2015.

autorka stwierdza: *Europejskie kraje o największej populacji muzułmańskiej to Niemcy, gdzie w 2010 r. według Pew Research Center mieszkało 4,8 miliona muzułmanów, co stanowiło 5,8% społeczeństwa niemieckiego. Na drugim miejscu znajduje się Francja, gdzie według powyższego ośrodka badawczego mieszka 4,7 milionów muzułmanów.* Tymczasem to Francja była i jest krajem o największej liczbie muzułmanów. W 2003 r. Nicolas Sarkozy, ówczesny minister spraw wewnętrznych, szacował liczbę muzułmanów we Francji na 5–6 mln[6]. Takie dane podaje się też obecnie. W dalszej części rozdziału autorka nadal powołuje się na książkę Halma i przedstawia mało wiarygodne informacje. Na str. 44 pisze: *Według H. Halma żądanie wprowadzenia kary śmierci za odstąpienie od wiary stanowi jedno z głównych dążeń islamistycznych, realizowane jest jednak tylko w niektórych krajach, takich jak Iran, Sudan czy Pakistan*. Przede wszystkim karanie śmiercią za apostazję (arab. *ridda*) owszem jest jednym z głównych dążeń islamistycznych, czyli upolitycznionego islamu, jest jednak głęboko zakorzenione w historii islamu i jest jednym z jego nakazów. Ponadto jest więcej krajów, w których za apostazję można stracić życie zgodnie z obowiązującym prawem. Są to: Afganistan, Arabia Saudyjska, Gambia, Jemen, Komory, Malawi i Mauretania, nie wspominając już o tym, że w całym świecie muzułmańskim *ridda* oznacza wykluczenie społeczne i potencjalne zagrożenie honorowym zabójstwem. Przesłanką pozwalającą stwierdzić, że Halm jest mało wiarygodnym badaczem, jest kolejne odniesienie do jego książki znajdujące się w recenzowanej publikacji: *W pracy niemieckiego uczonego H. Halma modlitwa nie stanowi ani mówionego, ani myślanego tekstu, jest natomiast tylko konkretną sekwencją ruchów ciała w następującej kolejności: stanie prosto, skłon tułowia, klęknięcie przy jednoczesnym podwójnym dotknięciu czołem podłogi. Sekwencja ta nazywa się rak'a, czyli pokłon. Liczba pokłonów podczas pięciokrotnej w ciągu dnia modlitwy jest różna. Modlitwa zakończona zostaje zwrotem głowy w prawo, później w lewo*. Trzeba przyznać, że trudno o bardziej niedorzeczne stwierdzenie. Można przypuszczać, że zarówno autorka książki, jak i badacz, na którego się powołuje, nigdy nie byli w meczecie podczas piątkowej modlitwy zgromadzeniowej. Zresztą wiele takich modlitw odbywa się na ulicach niemieckich miast. Otóż po pierwsze, każda z pięciu muzułmańskich modlitw jest sekwencją pozycji wymienionych przez Halma, jednak każdej z nich towarzyszą werbalne treści wymawiane po cichu przez modlącego się muzułmanina i nie ma od tego żadnego odstępstwa. W niniejszej recenzji nie ma miejsca na dokładniejszy opis muzułmańskiej modlitwy, jednak należy podkreślić, że każda z nich zaczyna się cichą recytacją pierwszej sury *Koranu – Al-Fatiha*. Po drugie, zakończenie modlitwy zwrotem głowy w prawo, a później w lewo nie towarzyszy każdej ceremonii modlitewnej, lecz odbywa się podczas modlitwy zgromadzeniowej. Muzułmanin, w pozycji siedzącej (często na piętach), zwraca głowę najpierw w kierunku towarzysza po prawej stronie i wymawia formułę: *As-salam alejkum wa rahmatu Llahi wa barakatuhu* (Niech pokój, miłosierdzie i błogosławieństwo Allaha będzie z tobą). Tę samą frazę wymawia, gdy zwraca głowę w lewą stronę. Po trzecie, tureccy muzułmanie, którzy w Niemczech

[6] J. Laurence, J. Vaïsse, *Intégrer l'Islam. La France et ses musulmans: Enjeux et réussites*, Paris 2006, s. 38.

stanowią większość, modlą się na głos. Autorowi recenzji trudno więc zrozumieć, dlaczego przypisano muzułmanom „milczącą" modlitwę. „Głośna" modlitwa tureckich muzułmanów jest często uznawana przez ortodoksyjnych i konserwatywnych arabskich muzułmanów za herezję. Z tego powodu Turcy i Arabowie mają swoje własne meczety. W Warszawie również istnieje rozdział muzułmańskich miejsc kultu.

Omawiając krąg kultury zachodniej, autorka wymienia jego charakterystyczne cechy. Kulturę europejską osadza w historycznym kontekście. Cywilizacja zachodnia formowała się, czerpiąc z myśli i osiągnięć starożytnej cywilizacji grecko-hellenistycznej i rzymskiej. Zabrakło jednak szerszego odniesienia do tego kontekstu. Autorka wspomina: *Jeśli Grecy wymyślili rządy prawa, to Rzymianom cywilizacja zachodnia zawdzięcza rozwój prawodawstwa* (s. 58). Jednak to Grekom świat zachodni zawdzięcza całą spuściznę filozoficzną. W ostatnim podrozdziale Martusewicz-Pawlus zwraca uwagę czytelnika na relacje świata islamu z Zachodem oraz sytuację Europy w obliczu konfliktu wartości. Dane statystyczne zgromadzone w 2013 r. przez wspomniany Pew Research Center wskazują, że mieszkańcy 31 krajów z przeważającą populacją muzułmańską (na 57 państw zrzeszonych w Organizacji Współpracy Islamskiej) opowiedzieli się za demokracją, ale przewagę mieli zwolennicy wprowadzenia szariatu jako obowiązującego prawa. Wskazuje to na ewidentny konflikt między wartościami demokratycznymi w społeczeństwach zachodnich i państwach muzułmańskich. Podobny rozdźwięk obserwuje się wśród europejskich społeczności muzułmańskich, które akceptują demokrację, ale większość z nich uważa szariat za konieczny. Autorka wskazuje teoretyczną możliwość rozwiązania tego dysonansu przez wprowadzenie zasady idżtihadu, czyli indywidualnego wysiłku umysłowego w celu samodzielnego formułowania opinii prawnych dostosowanych do rzeczywistych warunków. *Dzięki takiemu zabiegowi możliwe jest dostosowanie praw islamu do nowych warunków w sytuacji, w której Koran i sunna nie zawierają konkretnych wskazówek* (s. 65). Swój wywód opiera na publikacji niemieckiej uczonej Naiki Foroutan[7]. Uznaje się jednak, że w XI w. bramy idżtihadu zastały zamknięte przez aszaryckiego teologa Abol-Ma'alego Abd al Malika Dżowajniego. Oznaczało to zakaz stosowania twórczej interpretacji prawa. Wciąż jednak jest ona wykorzystywana w nurcie usulickim szyizmu[8]. Jest to jeden z czynników pozwalających uznać islam za nieprzystający do kultury świata zachodniego, a dialog między tymi kulturami za skomplikowany. Mimo to, jak konstatuje autorka, obie społeczności koegzystują w Europie od dziesiątków lat. Trzeba jednak zauważyć, że wywołuje to coraz więcej konfliktów i napięć. We wnioskach kończących rozdział pierwszy autorka wyraża nadzieję na pozytywne zakończenie procesu dostosowania

[7] N. Foroutan, *Kulturdialoge zwischen dem Westen und der islamischen Welt. Eine Strategie zur Regulierung von Zivilisationskonflikten*, Wiesbaden 2004.

[8] Usulici zdominowali szyizm ze względu na entuzjastyczne wsparcie dla stosowania idżtihadu w tworzeniu muzułmańskiego ustawodawstwa. Do dziś w prawie szyickim przyjmuje się zasadę, że cokolwiek jest nakazane przez rozum, jest też nakazane przez religię. W nurcie usulickim każdorazowo po śmierci głównego mudżtahida (znawcy idżtihadu) jest wymagany powrót do źródeł prawa muzułmańskiego i podejmowanie przez uczonych trudu jego nowych interpretacji.

islamu do wartości europejskich, co jest jedyną szansą na zgodne współżycie i współdziałanie przedstawicieli odmiennych kręgów kulturowych na terenie UE. Tymczasem, zdaniem recenzenta, proces dostosowania nie następuje (poza nielicznymi wyjątkami), obserwuje się natomiast pogłębiającą się przepaść między rdzennymi Europejczykami a muzułmańskimi imigrantami i ich potomkami.

Rozdział drugi nosi tytuł *Islamizm jako zagrożenie bezpieczeństwa europejskiego*. Na jego wstępie znajdują się informacje, podane za Pew Research Center, na temat liczby muzułmanów w Europie na koniec 2016 r. (26 mln) oraz szacowanego wzrostu tej liczby do 2050 r. Wspomniany ośrodek prognozuje, że wyniesie on 11,2 proc. (2,9 mln). Według autora recenzji jest to prognoza bardzo niedoszacowana, gdyż w ciągu kolejnych 30 lat liczba muzułmanów w Europie ulegnie przynajmniej podwojeniu. Obecnie przewiduje się, że już w 2030 r. muzułmanie będą stanowić 26,4 proc. ludności świata, z przeciętną wieku tylko 24 lata[9]. Będzie więc rosła presja z ich strony na zewnętrzne granice UE. Ponadto według niemieckiego demografa prof. Gunnara Heinsohna do 2050 r. mogą zaistnieć w Niemczech islamskie większości, ponieważ nasilającej się migracji muzułmanów będzie towarzyszyć wzrost emigracji etnicznych Niemców[10]. Jednocześnie nie można oddzielić zagadnień dotyczących migracji i bezpieczeństwa. Są one nierozłączne, zarówno na płaszczyźnie „bezpieczeństwa twardego", czyli konieczności utrzymania suwerenności państw, ich integralności terytorialnej i eliminowania zagrożenia terrorystycznego, jak i „bezpieczeństwa miękkiego", rozpatrywanego w sensie demograficznym, kulturowym. Terroryzm islamski stanowi więc tylko jedno z możliwych zagrożeń bezpieczeństwa państw Europy, jednak równie istotne jest bezpieczeństwo kulturowe. Martusewicz-Pawlus pisze: *Incydenty zwiastujące starcie cywilizacji były bagatelizowane w Europie w przeszłości, czemu sprzyjała polityka poprawności politycznej i wielokulturowości, w wyniku której nie zadbano o asymilację imigrantów wywodzących się z odmiennych kręgów cywilizacyjno-kulturowych* (s. 70). Autorka niesłusznie używa czasu przeszłego, gdyż poprawność polityczna i zmowa milczenia nadal towarzyszą polityce dotyczącej problematyki imigranckiej i muzułmańskiej w UE. Martusewicz-Pawlus wychodzi z założenia, że to islamizm jest zagrożeniem kulturowym Europy. Przedstawia argumenty za i przeciw w kwestii oddzielania islamu od islamizmu, czyli upolitycznionej formy islamu. Cytuje przy tym stanowiska różnych autorów. W końcu konkluduje, że rozróżnienie kategorii pojęciowych „islam" oraz „islamizm" jest zasadne, między innymi dlatego, że jest pomocne w procesie analizy celów politycznych dżihadystów. Wiązanie dżihadu z islamizmem, a nie z islamem to po prostu przeniesienie źródła przemocy z religii – islamu, na ideologię – islamizm. Takie stanowisko to kolejny przejaw poprawności politycznej, gdyż islam to religia wszechogarniająca, która obejmuje wszystkie dziedziny życia: duchowego, społecznego, ekonomicznego, politycznego,

[9] R. Muhammad, *The Global Halal Market – Stats & Trends*, HalalFocus, 16 I 2015 r., http://halalfocus.net/the-global-halal-market-stats-trends/ [dostęp: 17 V 2017].

[10] U. Ulfkotte, *Niemcy jako Mekka. Cicha islamizacja Europy*, Wrocław 2019, s. 95.

gospodarczego, zarówno w czasach pokoju, jak i wojny. Towarzyszy muzułmaninowi od narodzin do śmierci. Islamizmowi, a nie islamowi poprawni politycznie autorzy przypisują szariat, dżihad i da'wę (misję szerzenia islamu), przy czym zapominają, że te zjawiska od początku są związane z tą religią. Dżihad był podstawowym sposobem krzewienia islamu. Błędem jest doszukiwanie się jego źródeł w dziełach XX-wiecznych „islamistycznych" ideologów. Ci muzułmańscy myśliciele jedynie przypomnieli o dżihadzie jako zapomnianej powinności muzułmanów[11]. Autorka słusznie zauważa, że w Niemczech dokonuje się proces islamizacji. W imię wolności wyznania lekceważy się zapisy niemieckiej konstytucji bądź stawia się je niżej niż prawa mniejszości muzułmańskiej. Jako przykład podaje wyrok sądu, w którym niemiecka sędzia przyjęła możliwość bicia żony (Marokanki) przez jej marokańskiego męża i oddaliła jej pozew o rozwód. Uznała, że zawierając związek małżeński z muzułmaninem, powódka musiała mieć świadomość, w jaki sposób muzułmańskie prawo reguluje stosunki między kobietami a mężczyznami. Innym przykładem potwierdzającym rozszerzanie się wpływów islamu w Niemczech jest przejmowanie opustoszałych kościołów i tworzenie w nich sal modlitewnych. Autorka książki nie ukazała pełnej wagi tego zjawiska, które jest problemem systemowym, zagrażającym tożsamości, kulturze i integralności kraju. Niemcy niemal w każdej dziedzinie życia ustępują pola mniejszościom muzułmańskim, które coraz bardziej się rozzuchwalają i domagają się kolejnych ustępstw i przywilejów. To wszystko dzieje się za zgodą władz landowych i federalnych, przy pełnym poparciu mediów, które nie widzą problemu, a niewygodne fakty przemilczają. Osoby, które głośno starają się mówić o zagrożeniu, nazywa się islamofobami i rasistami. Martusewicz-Pawlus stwierdza, że zaistniała konieczność wyznaczenia granic tolerancji w polityce Niemiec wobec muzułmanów, jednak te granice już dawno zostały przekroczone. Najlepszym tego dowodem jest liczebne rozrastanie się społeczeństwa równoległego.

Kolejne podrozdziały książki zostały poświęcone ogólnym zagadnieniom dotyczącym terroryzmu i terroryzmu islamskiego jako przykładom zagrożeń bezpieczeństwa publicznego. Opierając się na danych statystycznych Global Terrorism Index z 2016 r., autorka pisze: *Przedstawiona statystyka wskazuje, iż problem terroryzmu nie dotyczy jedynie obszarów dotkniętych konfliktami terytorialnymi, narodowościowymi czy ideologicznymi. Co więcej, terroryzm zdaje się stosunkowo powoli, ale skutecznie przemieszczać na obszary europejskie* (s. 93). Przecież terroryzm jest obecny w Europie od dawna, a w Niemczech, gdzie mieszka autorka, od lat 70. XX w. Trzy strony dalej wyraża ona opinię, że teoria polityczna islamu była obiektem zainteresowań naukowych, szczególnie po zwycięstwie rewolucji islamskiej w Iranie w 1979 r. Następnie nastąpił spadek

[11] Malik ibn Anas (zm. w 795 r.), twórca jednej ze szkół prawa (arab. *mazhab*) – szkoły malikickiej, definiował dżihad jako walkę zbrojną. Opisywał, jak powinien działać bojownik na rzecz islamu, jak dzielić łupy zdobyte w walce i jak interpretować śmierć w boju. Abdullah ibn al-Mubarak w pracy *Kitab al-dżihad* (*Księga dżihadu*), którą napisał w latach 90. VIII w., rozbudował idee dżihadu. Oparł je na przekazach pierwszych muzułmanów (hadisach) dotyczących dżihadu za życia proroka Muhammada.

tego zainteresowania, zwłaszcza po śmierci ajatollaha Chomeiniego. Tymczasem dla genezy i rozwoju ruchu dżihadystycznego największe znaczenie miała wojna w Afganistanie w latach 1979–1989 przeciwko radzieckiej okupacji. To w wyniku tego konfliktu i na skutek jego następstw powstały Al-Kaida i światowy ruch dżihadystyczny, a islamscy ideolodzy napisali wiele dzieł motywujących muzułmanów do walki. Ten wątek jest istotny dla zrozumienia współczesnego dżihadu, który zostaje omówiony na kilku kolejnych stronach książki. Zawarte są tam między innymi sprzeczne opinie różnych autorów na temat radykalizacji. Dla jednych to wykluczenie społeczne wzmacnia procesy radykalizacji, a marginalizowanie muzułmanów ma być skutkiem strachu i niechęci wobec nich ze strony społeczności niemieckiej. Inni autorzy, na których powołuje się autorka, stwierdzają, że nierówności społeczne czy religijne odniesienia nie w pełni tłumaczą proces radykalizacji. Najbardziej trafne, zdaniem recenzenta, jest sformułowanie: *Niezależnie od swojej pozycji społecznej młodzież muzułmańska ma identyczną skłonność do zostania radykałami* (s. 106), a co najważniejsze: (…) *w kontekście użycia przemocy przynależność religijna dystansuje zarówno pochodzenie społeczne, jak i osiągnięcia w nauce młodego muzułmanina* (s. 107). A więc to islam motywuje jego wyznawców do przemocy. Badania własne autorki doprowadziły ją do konkluzji, że (…) *dalszy napływ imigrantów z krajów muzułmańskich na terytorium Unii Europejskiej stanowi zagrożenie poczucia bezpieczeństwa Europejczyków* (s. 107). Na końcu rozdziału formułuje alarmujące wnioski, przy czym zwraca uwagę na niepokojące rozmiary i tempo islamizacji kontynentu europejskiego oraz wymienia najbardziej wyraziste przykłady tego procesu. Nie sposób jednak zgodzić się z następującą opinią: *Badania autorskie potwierdziły, że sytuacja powyższa dotyczy w szczególności Niemiec, które ze względu na swoją przeszłość i moralne obciążenie związane z II wojną światową cały czas są krajem bardzo tolerancyjnym* (s. 110). Martusewicz-Pawlus przeprowadziła swoje badania tylko w Niemczech i w Polsce, a proces islamizacji, postępujący z większą lub mniejszą siłą, obserwuje się również w innych krajach – Francji, Belgii, Holandii czy Wielkiej Brytanii. Próbuje się go usprawiedliwić moralnym obciążeniem tych państw za czasy kolonializmu. Takie tłumaczenie nie wytrzymuje jednak próby czasu i nie odpowiada realiom, gdyż proces islamizacji zachodzi również w Szwecji, kraju szeroko otwartym na imigrantów. Tam politycy nie motywują tego zjawiska koniecznością ubogacania szwedzkiej kultury, lecz wprost ją deprecjonują, stawiając niżej od kultury i obyczajowości imigrantów. Znamienne są przy tym słowa algierskiego pisarza Boualema Sansala. Stwierdził on, że islamiści, którzy wypowiedzieli wojnę Zachodowi, swoją pierwszą bitwę już wygrali. Przyczyny tego stanu rzeczy wskazuje również autorka omawianej książki. Są to: (…) *kurczowe trzymanie się sukcesów w walce z terrorystami, uspokajanie samych siebie poprzez teorie współczucia, poszukiwanie powodów terroryzmu, obwinianie samych siebie, błędna polityka, nieudana integracja, paniczne wykluczanie krytyków islamu z dyskursu publicznego* (s. 110).

Rozdział trzeci pt. *Strach przed islamem a poczucie bezpieczeństwa osobistego* w znacznej mierze jest oparty na wynikach badań ankietowych przeprowadzonych

przez Martusewicz-Pawlus w Niemczech i Polsce. Za Moniką Bobako[12] stwierdza ona, że pojawienie się kwestii islamskiej jest skrupulatnie wykorzystywane przez prawą stronę sceny politycznej do siania strachu w społeczeństwach i zbijania politycznego kapitału na szerzeniu islamofobii, która może się przejawiać także aktami przemocy skierowanymi w obcych. Według autorki polaryzację w społeczeństwach europejskich wzmacniają zamachy terrorystyczne dokonywane na terenie Europy pod sztandarem islamu. Jest to teza stereotypowa, ponieważ problem jest znacznie głębszy. Dotyka on przede wszystkim życia codziennego. Mieszkająca w Polsce Bobako nie widzi antagonizmów obecnych na ulicach zachodnioeuropejskich dzielnic zdominowanych przez muzułmanów, którzy coraz bardziej zawłaszczają przestrzeń publiczną, arogancko odnoszą się do etnicznych Europejczyków, ignorują przepisy prawa i zagrażają bezpieczeństwu publicznemu. Porównywanie przez tę autorkę islamofobii do antysemityzmu jest nieuprawnione. Po pierwsze dlatego, że Arabowie to też lud semicki i w tym wypadku powinno się raczej używać określeń „antyjudaizm" lub „antyżydowskość", a po drugie, antyżydowskość ma wymiar prawicowy, lewicowy i muzułmański. Ten ostatni jest obecnie najgroźniejszy. Ponadto dla lewicy mniejszości muzułmańskie w Europie stanowią obiekt szczególnego zainteresowania i troski. Każda, nawet najbardziej rzeczowa, krytyka islamu wywołuje bunt muzułmanów, zdenerwowanie polityków i protesty mediów. Według nich również sama islamizacja jest wymysłem islamofobów, gdyż islam jest religią absolutnie pokojową. Czyżby Martusewicz-Pawlus, która cytuje Bobako, zapomniała o aplauzie, jaki wywołały słowa kanclerz Angeli Merkel, która w 2015 r. ogłosiła, że islam przynależy do Niemiec. Nawet przy najlepszej woli nie można jednak dostrzec jakichkolwiek dawniejszych śladów islamu w Niemczech, poza przyjaznymi stosunkami z Turcją, łączącymi Niemcy od czasów cesarza Wilhelma I. Inna sprawa, że pogląd pani kanclerz nie podlega już krytyce, ponieważ islam tak głęboko przeniknął życie ludzi w Niemczech, jakby był oficjalną ideologią państwową. Uzyskał wpływ na wszystkie dziedziny życia niemieckiego społeczeństwa i politykę. Unia Chrześcijańsko-Demokratyczna (CDU), do której należy Merkel, jest przecież partią prawicową, ale tak przesiąkniętą islamem, że na oficjalnych partyjnych imprezach chadecji można niekiedy zobaczyć logo partii z islamskim półksiężycem, gdyż krzyż przestał być widoczny w przestrzeni publicznej jako symbol obrażający uczucia muzułmanów. Ponadto założenie, że (…) *podstawowa ludzka potrzeba identyfikacji z własnym dziedzictwem oraz ludźmi podobnymi do siebie nie musi być równoznaczna z nienawiścią skierowaną wobec innego* (s. 113), jest ważne z etycznego punktu widzenia, ale nie przystaje do islamu, który jest tolerancyjny tylko tam, gdzie muzułmanie nie są jeszcze zbyt liczni. Pokazują to również badania sondażowe przeprowadzone przez autorkę. Wynika z nich, że Niemcy o wiele częściej niż Polacy nie czują się bezpiecznie w swoim kraju. Interesujące jest spostrzeżenie, że większość Polaków postrzega dalszy napływ imigrantów z krajów muzułmańskich do UE jako zagrożenie bezpieczeństwa Europejczyków, podczas gdy tylko 22,5 proc. Niemców podziela ten pogląd.

[12] M. Bobako, *Islamofobia jako technologia władzy. Studium z antropologii politycznej*, Kraków 2017.

Bardzo ważne jest to, że od zakończenia drugiej wojny światowej do 1989 r. Polska była jednym z najbardziej narodowych krajów świata. Gwarancją jej bezpieczeństwa była jednoetniczność, jednoreligijność i jednokulturowość. We współczesnej rzeczywistości te czynniki niekorzystnie się zmieniają. Jednak o ile napływ Wietnamczyków czy Chińczyków, cechujących się dyscypliną i pracowitością, spotyka się z przychylnym lub neutralnym przyjęciem, o tyle imigrantów z krajów muzułmańskich już niekoniecznie. Przekłada się to na proces asymilacji lub integracji. Autorka konstatuje: *W świetle wyników powyższych badań z całą stanowczością podkreślić należy, że ani przynależność etniczna, ani religijna nie decyduje bezwarunkowo o wystąpieniu bądź braku zjawiska integracji* (s. 123). A jednak tak nie jest, o czym świadczą dzielnice i całe miejscowości zdominowane przez muzułmanów, istniejące również w Niemczech. Czyżby autorka tego nie dostrzegała? Warto zadać sobie pytanie, jaki procent muzułmanów zasymilował się lub zintegrował ze społecznościami krajów przyjmujących. Zdaniem recenzenta nie będzie to więcej niż 20 proc., co i tak może być zawyżonym szacunkiem. Jako przykład udanej integracji w Niemczech Martusewicz-Pawlus podaje społeczność alewitów, których większość nie boi się żyć na sposób zachodni. Religia jest dla nich ważna, ale nie ma tak opresyjnego charakteru. Warto zwrócić uwagę, że alewici to odłam religijny luźno związany z szyizmem i baktaszytami, bractwem mistycznym. Jego członkowie nie przestrzegali szariatu, dżihadu i ramadanu, mogli spożywać alkohol i wieprzowinę. Alewici zrównali pozycję kobiety i mężczyzny, przejęli od chrześcijaństwa spowiedź, celibat duchownych, rodzaj chrztu i odpuszczenie grzechów. Alewitami-baktaszytami są Kurdowie. Ich domy kultu to nie meczety, lecz cem-evi, gdzie w obrzędach, często przy muzyce, wspólnie uczestniczą kobiety i mężczyźni. Już z tego krótkiego opisu wynika, że alewici nie mogą stanowić przykładu udanej integracji muzułmanów w Niemczech. W Wielkiej Brytanii takim przykładem nie mogą być z kolei członkowie stowarzyszenia Ahmadija, na co zwracają uwagę niektórzy autorzy.

Przedstawiając wyniki kolejnych badań, autorka zauważa, że w społeczeństwach zachodnich islam nadal jest traktowany jako ciało obce. Należy przypomnieć, że islam zawsze był tak traktowany w Europie. Jak stwierdza badaczka, większą niechęć do niego wykazują społeczeństwa, które mają niewielki kontakt z muzułmanami lub nie mają go w ogóle. Negatywny stosunek do wyznawców islamu ma 70,3 proc. Polaków oraz 46 proc. Niemców. W przypadku naszych zachodnich sąsiadów to zjawisko ma jednak tendencję wzrostową. Zdecydowana większość Polaków (71,4 proc.) jest niechętna budowie meczetów, w przypadku Niemców jest to nieco ponad połowa (53,5 proc.). Zbliżone są już natomiast dane dotyczące pozytywnego (Polacy – 51,3 proc., Niemcy – 48,3 proc.) bądź negatywnego (Polacy – 45,3 proc., Niemcy – 48,3 proc.) postrzegania symboliki muzułmańskiej przez obie nacje. Autorka książki broni prawa do noszenia chust przez muzułmanki, ponieważ (…) *chusta pozwala na wyrażenie swojej indywidualności oraz kulturowej tożsamości, kontestuje także kulturę, która uprzedmiatawia kobietę, oceniając ją według fizycznej atrakcyjności, co w ocenie wielu muzułmanek jest domeną świata zachodniego* (s. 130). Jak więc wytłumaczyć to, że pomimo zakrywania ciała ponad 80 proc. egipskich kobiet doświadczyło molestowania w środkach

komunikacji miejskiej w Kairze? Dlaczego Iranki zdejmują muzułmańskie stroje, gdy wyjeżdżają za granicę, i zakładają modne, podkreślające kształty ubrania?

Nie sposób polemizować z twierdzeniem, że demograficzny obraz Europy zmieni się w przyszłości na korzyść mniejszości muzułmańskich. Z tego względu należy zadbać o rzeczowy i stały dyskurs o islamie. Utrudnia lub wręcz uniemożliwia go islamofobia, czyli *spiritus movens* prawicowego ekstremizmu. Wymieniając za Arminem Pfahlem-Traughberem[13] postawy islamofobiczne, autorka konkluduje, że trudno je jednoznacznie oddzielić od konstruktywnej krytyki islamu. Ponownie przedstawia opinię, że zarówno w Niemczech, jak i w Polsce islamofobia jest czynnikiem umożliwiającym przejmowanie dyskursu przez środowiska skrajnie prawicowe. Recenzent uważa jednak, że nawet konstruktywna krytyka islamu jest traktowana jako islamofobia. Nie od dziś wiadomo, że każda najmniejsza próba podważenia islamu jako religii pokoju, podejmowana również przez samych muzułmanów, wzbudza gwałtowne protesty muzułmańskich uczonych. Autorka przytacza słowa Piotra Ibrahima Kalwasa[14], bądź co bądź wyznawcy islamu, który stwierdził, że (…) *islamofobia to obrzydliwie tępe narzędzie do kneblowania wolnej myśli i wolnego słowa. Rodzaj pały do walenia w łeb oponentów, jak nie ma się nic sensownego do powiedzenia. Radykalnie ująłbym to tak: nie ma żadnej islamofobii, prócz tej wymyślonej przez muzułmanów na potrzeby dyskusji, w której nie mają nic sensownego do powiedzenia* (s. 139). Mimo podobnego, choć mniej kategorycznego, pojmowania islamofobii przez innych autorów Martusewicz-Pawlus opowiada się za definicją Bobako, która traktuje islamofobię jako niechęć, nienawiść do islamu opartą na stereotypach. Tymczasem to niedostateczna wiedza o islamie jako religii i poprawność polityczna mogą skłaniać, zdaniem recenzenta, do wysuwania takiego wniosku. Idąc tym tokiem myślenia, należy stwierdzić, że nawet gdyby zachowania muzułmanów były inne i nie wynikały z nakazów i zakazów religijnych, jak również inna byłaby idąca im w sukurs polityka władz państw zachodnich, traktujących niekiedy własnych obywateli jako obywateli drugiej kategorii, pojęcie „islamofobia" i tak pojawiłoby się w narracji. Jeśli są islamofile, to muszą być islamofobi. Jest to obiektywna przyczyna – jeśli ktoś jest za, to zawsze będzie ktoś, kto jest przeciw.

Autorka książki zwraca uwagę na politykę Prawa i Sprawiedliwości, polskiej partii, która wykorzystuje lęk przed obcymi do kreowania zagrożenia związanego z nielegalną imigracją, uchodźcami, straszenia obywateli przed nowym wrogiem, aby pozyskiwać elektorat. Tego rodzaju socjotechnika umacnia postawy nacjonalistyczne, ksenofobiczne, wrogie wobec świata islamu. W większości krajów Europy Zachodniej partie rządzące prezentują przeciwne stanowisko wobec imigrantów i realizują politykę otwartych drzwi. Jakie przynosi to skutki? Po krótkotrwałej aprobacie, wręcz poklasku,

[13] A. Pfahl-Traughber, *Islamfeindlichkeit, Islamophobie, Islamkritik – ein Wegweiser durch den Begriffsdschungel,* Bundeszentrale für politische Bildung, 17 VI 2019 r., https://www.bpb.de/politik/extremismus/rechtsextremismus/180774/ islamfeindlichkeit-islamophobie-islamkritik-ein-wegweiser--durch-den-begriffsdschungel [dostęp: 4 III 2021].

[14] J. Winiarski, P.I. Kalwas, *Archipelag islam. Czas Koranu, czas zmi*any, Nysa 2018.

społeczeństwa w 2015 r., kiedy Niemcy przyjęły ponad 1 mln imigrantów, a Szwecja ponad 160 tys. (stanowiło to rekord w przeliczeniu na 1 mln mieszkańców), sytuacja diametralnie się zmieniła. Wykorzystały to tamtejsze partie antyimigranckie, które rządzący i związane z nimi media nazywają islamofobicznymi lub wręcz rasistowskimi. Poparcie dla nich rośnie wprost proporcjonalnie do negatywnych, przestępczych zachowań imigrantów, którzy wciąż mogą liczyć na łagodne traktowanie. Jest oczywiste, że musi to budzić niechęć społeczeństwa do władz. Autorka zwraca uwagę na przejawy islamofobii, ale nie znajduje ich źródeł po stronie muzułmanów. Winne są partie populistyczne i media, które na przykład nie nadały odpowiedniego rezonansu wydarzeniom w Kolonii w noc sylwestrową z 2015 na 2016 r. Zdaniem Martusewicz-Pawlus: (…) *przemilczenie faktów związanych z molestowaniem seksualnym kobiet przez imigrantów z Afryki Północnej paradoksalnie wzmacniać może postawy antyimigranckie/antymuzułmańskie. W tym przypadku zaprzepaszczona bowiem zostaje szansa na rzetelną dyskusję o kwestiach dla islamu problematycznych, takich jak wymuszana przez doktrynę islamu wstrzemięźliwość seksualna wyznawców*. Autorka konkluduje: *Uchylanie się od tego rodzaju analizy pozwala środowiskom skrajnie prawicowym wykorzystać negatywne okoliczności do interpretacji właściwej dla swoich politycznych interesów* (s. 145). To pokrętny wniosek. Czy dyskusję toczącą się w mediach na temat tabuizacji seksu w islamie nie nazwano by islamofobią? Pozostaje zaproponować przeprowadzenie badań na temat relacji muzułmańskich gwałcicieli i ich ofiar. Okazałoby się, że gwałt mieści się w tradycji muzułmańskiej, a Europejki są traktowane przez wielu muzułmańskich imigrantów jako „mięso" lub prostytutki, co ma być dodatkowym usprawiedliwieniem dla wyznawców islamu, którzy wyładowują na nich swoje popędy seksualne. Jednym z wniosków kończących omawiany rozdział jest twierdzenie, że rozwiązywanie konfliktów przez dialog między przedstawicielami odmiennych kręgów kulturowych jest koniecznością. Ale taki dialog jest przecież prowadzony ze społecznościami muzułmańskimi od lat. W przeszłości z reguły przynosił on tymczasowe uspokojenie sytuacji, po czym konflikt wybuchał ze zdwojoną siłą. Ponownie można przywołać słowa Sansala, który stwierdził, że islamiści swoją pierwszą bitwę w Europie już wygrali[15].

Najbardziej interesujący jest rozdział czwarty pt. *Euroislam – teoria i praktyka*, w którym zostaje rozwinięta koncepcja euroislamu Bassama Tibiego. Na wstępie zamieszczono odniesienie do *Koranu*, w którym sury pokojowe współwystępują z surami nawołującymi do stosowania przemocy wobec niewiernych. W związku z tym autorka prezentuje pogląd, że nie ma jednego islamu, a więc za czyny dokonywane przez ekstremistów muzułmańskich nie należy obciążać odpowiedzialnością wszystkich

[15] W 2014 r. lord Richard Scott, emerytowany sędzia brytyjskiego Sądu Najwyższego, poradził Brytyjczykom, w jaki sposób mogą ustrzec swoje córki przed gwałtami ze strony wyznawców islamu. Zalecił im, aby zapobiegawczo przeszli na islam lub swoje córki wydali za mąż za muzułmanów. Tylko ten, kto zrealizuje ten drugi wariant, daje wyraźny sygnał, że nie jest „wrogiem islamu". Jeden z dwóch synów lorda przeszedł na islam, uczyniła to również jedna z jego dwóch córek, a spośród dwanaściorga jego wnuków muzułmanami jest siedmioro. Zob. U. Ulfkotte, *Niemcy jako Mekka*…, s. 165.

wyznawców tej religii. Islam, podobnie jak inne religie, może być praktykowany w sposób umiarkowany. Przykładem jest wspomniany Tibi, Syryjczyk i muzułmanin z urodzenia, Europejczyk z wyboru, zintegrowany ze społeczeństwem zachodnim. W tym kontekście istotne staje się rozróżnienie między pojęciem „integracja", oznaczającym harmonijną koegzystencję różnych grup etnicznych lub religijnych przy zachowaniu ich odrębności kulturowej, a pojęciem „asymilacja", które oznacza całościowe „wtopienie się" przybyszów w kulturę społeczeństwa przyjmującego. Synonimem pojęcia „asymilacja" jest „akulturacja". Ze względu na to, że asymilacja, wiążąca się z rezygnacją z własnych wartości kulturowych, może prowadzić do utraty tożsamości, jest ona negatywnie postrzegana w kontekście wydarzeń, jakie zaszły w Europie doświadczanej nacjonalizmami i próbami likwidacji przejawów obcych kultur. Na tej podstawie Martusewicz-Pawlus, podobnie jak Stanisław Kosmynka i Bassam Tibi, postuluje integrację wykorzystującą koncepcję euroislamu. Kosmynka euroislam określił jako „trzecią drogę", wykluczającą asymilację i wielokulturowość. Obu tych koncepcji nie udało się urzeczywistnić w odniesieniu do europejskich muzułmanów. Idee euroislamu mają pozostawać w zgodzie z demokracją liberalną, prawami człowieka i zasadami społeczeństwa obywatelskiego przez odrzucenie dżihadu, szariatu, hidżry (migracji) i da'wy. Według Tibiego istnieje możliwość nadania islamowi nowego tła kulturowego, zgodnie z wersetem 13 zamieszczonym w surze nr XLIX (*Al-Hudżurat – Komnaty*): *O ludzie! Oto stworzyliśmy was z mężczyzny i kobiety i uczyniliśmy was ludami i plemionami, abyście się wzajemnie znali*. Aby dowieść, jak słabo jest to umocowana koncepcja, wystarczy zacytować słowa z wersetu 51 sury V (*Al-Maida – Stół zastawiony*): *O wy, którzy wierzycie! Nie bierzcie sobie za przyjaciół żydów i chrześcijan; oni są przyjaciółmi jedni dla drugich*. Zdecydowana większość muzułmańskich autorytetów jest zdania, że muzułmanów obowiązuje zakaz integracji z „niewiernymi", niektórzy z nich uważają, że nawet kontakty z nimi są niedopuszczalne, jeśli nie zachodzi taka konieczność. Ponadto według Europejskiej Rady Fatw i Badań z siedzibą w Dublinie, wydającej orzeczenia o zgodności postępowania z normami religijnymi, to sam Allah ustanowił świętą wojnę. Na dowód tego są cytowane odpowiednie wersety z *Koranu*. Nie należy też zapominać o obowiązującej w islamie zasadzie *mansuch* – oznaczającej anulowanie lub zastąpienie wersetów z okresu mekkańskiego (zwanych popularnie pokojowymi) wersetami *nasich* – skrajnie sprzecznymi z tymi pierwszymi. Ta zasada przeczy idei istnienia różnych islamów. Nie można również zgodzić się z przytoczoną w książce tezą, cytowaną za Tibim, że islam nie wypracował żadnej teorii państwa, a kalifat jest jedynie imperialnym porządkiem. Czyż kalifat nie jest formą organizacji państwa? Było ich przecież wiele w historii islamu, jak chociażby kalifat Fatymidów, hiszpańskich Umajjadów, tunezyjskich Hafsydów czy Marynidów w Maroku. Istniał też sułtanat Sokoto, którego spadkobiercy wciąż żyją w tym nigeryjskim mieście i przewodzą tamtejszym muzułmanom, ciesząc się dużym szacunkiem.

Mimo przedstawionych danych statystycznych stawiających wyznawców islamu w niekorzystnym świetle (65 proc. muzułmańskich imigrantów pierwszej generacji przedkłada normy religijne nad prawa świeckie kraju, w którym mieszkają, w drugim

pokoleniu jest to ponad 60 proc., a 50 proc. muzułmanów deklaruje wrogość do Zachodu) autorka książki nie jest w stanie zaakceptować poglądu Piotra Ślusarczyka, publikującego w portalu Euroislam.pl, który twierdzi, że integracja imigrantów z państw muzułmańskich jest w Europie mrzonką. Martusewicz-Pawlus opowiada się za pokojowym dialogiem i potrzebą zainteresowania etnicznych Europejczyków problematyką islamu, aby ignorancja w tym zakresie nie stanowiła przeszkody w realizacji koncepcji euroislamu. W ślad za innymi autorami nie szczędzi też słów krytyki pod adresem Tarika Ramadana, szwajcarskiego uczonego (wnuka Hasana al-Banny, założyciela egipskiego Stowarzyszenia Braci Muzułmanów), który pod pojęciem „euroislamu" prezentuje raczej ortodoksyjny islam i jest nazywany kryptofundamentalistą, wyrażającym sprzeczne opinie w celu zadowolenia władz i społeczności europejskich oraz środowisk muzułmańskich. Niezależnie od tych opinii warto zwrócić uwagę, że w latach 70. XX w. proces integracji muzułmanów, na przykład we Francji, przebiegał w sposób bezkonfliktowy. Co prawda imamowie i misjonarze, którzy w tym czasie przybywali z państw muzułmańskich do Francji i innych krajów zachodniej Europy, angażowali się w głoszenie nauk o islamie, ale z trudem przekonywali imigracyjnych robotników do przestrzegania nakazów islamu, ponieważ nie znali ich życiowych problemów. Ówcześni imigranci bardziej dbali o zapewnienie bytu rodzinie niż o zaspokojenie potrzeb duchowych. Pierwsze pokolenie imigrantów troszczyło się również o wykształcenie swoich licznych dzieci wzrastających w kulturze europejskiej i w ten sposób spełniało założenia polityki integracji społecznej.

Martusewicz-Pawlus jest przekonana, że mimo przesłanek zmuszających do krytycznej oceny zjawiska integracji społeczności muzułmańskich to integracaja ta jest możliwa. Jej warunkiem jest przyjęcie koncepcji euroislamu. Takie stanowisko podtrzymuje nawet po samokrytyce złożonej przez Tibiego, który po zaobserwowaniu zjawisk towarzyszących fali imigracyjnej do Niemiec w 2015 r. zakwestionował możliwość realizacji euroislamu w tym kraju. Pociesza się on tym, że warunki panujące w innych krajach bardziej sprzyjają realizacji tej idei. Jego optymizm jest jednak nieuzasadniony, gdyż w wielu państwach Europy Zachodniej sytuacja związana z relacjami z mniejszościami muzułmańskimi jest taka sama jak w Niemczech, a we Francji nawet bardziej napięta. Skala negatywnych zjawisk zależy od liczebności diaspory muzułmańskiej. Nie zmienią tego stanu rzeczy pojedyncze, nagłaśniane inicjatywy promujące liberalny islam, ponieważ, jak autorka książki sama zauważa, 70 proc. muzułmanów w Niemczech w ogóle nie interesuje się polityką. Co jednak ważniejsze i bardziej niepokojące, tzw. islam zorganizowany, mający poparcie 10 proc. muzułmanów, rości sobie pretensje do reprezentowania całej diaspory. Martusewicz-Pawlus pozostaje pod tak silnym wpływem koncepcji euroislamu, że trudno uznać za logiczne podtrzymywanie przez nią tego przekonania, gdy jednocześnie stwierdza w swojej książce: *Projekty reformatorskie nawiązujące w swych założeniach do idei oraz zasad euroislamu nie cieszą się akceptacją środowisk muzułmańskich, często też narażone są na krytykę z różnych stron sceny politycznej* (s. 195). Kto więc ma realizować koncepcję euroislamu? W jednym z wniosków zawartych w zakończeniu autorka pisze:

Przeprowadzone badania literaturowe i empiryczne dowodzą słuszności twierdzenia, iż dostosowanie norm religijnych islamu do wartości i zasad obowiązujących w społeczeństwach zachodnich pozytywnie wpływa na poziom bezpieczeństwa obywateli państw Unii Europejskiej, w tym Niemiec i Polski (s. 198). Jeśli chodzi o Polskę z pewnością tak jest, co potwierdza przykład Tatarów. Poza tym diaspora muzułmańska w naszym kraju jest zbyt mała, aby postrzegać ją jako źródło stałego zagrożenia, w przeciwieństwie do innych państw UE. Należy zgodzić się z autorką, że jej badania stanowią użyteczny wkład w bardzo aktualny dyskurs o przyszłości UE. Wskazują ponadto kierunek dalszych badań w dziedzinie bezpieczeństwa obywateli Unii. Rzeczywistość często jednak odbiega od teoretycznych rozważań. Jeśli weźmie się pod uwagę przesłanki demograficzne, można przyjąć, że dla dziedzictwa kultury europejskiej przyszłość nie rysuje się w różowych barwach.

Jakkolwiek w wielu ważnych sprawach autor niniejszej recenzji nie zgadza się z autorką omawianej publikacji, to poleca jej książkę osobom zainteresowanym relacjami ze społecznościami muzułmańskimi w Europie oraz przyszłością naszego kontynentu stojącego przed poważnymi wyzwaniami. Uwagi zawarte w niniejszej recenzji wzbudzą zapewne wątpliwości wśród czytelników i stałych użytkowników portalu Euroislam.pl, w którym na bieżąco są omawiane zagadnienia dotyczące radykalnego islamu, imigracji muzułmanów, wielokulturowości i integracji mniejszości muzułmańskich.

ROBERT BORKOWSKI
ORCID: 0000-0001-7086-9455

DOI: 10.4467/20801335PBW.21.029.14306

Adam Kucharski, *Prawa epidemii: skąd się epidemie biorą i dlaczego wygasają?*[1]

Skutkiem utrzymującej się od ponad roku pandemii wywołanej przez koronawirusa SARS-CoV-2 jest pojawienie się w społeczeństwie wielu różnych poglądów na temat istniejącej sytuacji, wprowadzanych ze względu na nią obostrzeń ograniczających wolności i swobody obywatelskie oraz programów szczepień. Pojawiają się teorie spiskowe dotyczące zarówno genezy samej epidemii, jak i opracowywanych i wdrażanych szczepionek. W tych czarnych wizjach pandemia jest efektem rzekomej zmowy koncernów farmaceutycznych, Światowej Organizacji Zdrowia, służb specjalnych i elit politycznych. Odmienna polityka walki z epidemią prowadzona w różnych krajach jest dodatkową pożywką dla autorów spiskowych wizji rzeczywistości. Działania władz zależą jednak od wielu czynników, m.in.: od doboru ekspertów (osoby merytoryczne albo przypadkowe), od wyboru modelu rozwoju epidemii (są różne modele, które prowadzą do różnych konsekwencji), od stanu służby zdrowia (działająca efektywnie albo nieefektywnie), od ładu społecznego i kultury politycznej danego kraju (liberalne podejście albo autorytarne restrykcje), od rozsądku elit rządzących (totalny lockdown albo racjonalne, selektywne regulacje), a także od sprawności państwa (spójność decyzyjna albo rytualny chaos). Gorące spory toczą się zresztą wśród samych epidemiologów. W gronie najwybitniejszych ekspertów, którzy modelują rozwój pandemii COVID-19, istnieją ogromne różnice poglądów, a przecież prognozy tych specjalistów są podstawą scenariuszy dotyczących zwalczania choroby i przyjęcia strategii przez poszczególne rządy. Na przykład przewidywania wynikające z modelu prof. Johna P.A. Ioannidisa z Uniwersytetu Stanforda w porównaniu z modelem opracowanym przez IHME (Institute of Health Metrics and Evaluation) Uniwersytetu Waszyngtońskiego są

[1] Adam Kucharski, *Prawa epidemii: skąd się epidemie biorą i czemu wygasają?* (tytuł oryginału: *The Rules of Contagions: Why Things Spread – and Why They Stop*), tłum. J. Maksymowicz-Hamann, Warszawa 2020, Wydawnictwo Relacja, 316 s.

zupełnie inne i prowadzą do diametralnie różnych wniosków co do sposobów zwalczania epidemii.

Rosnąca złożoność współczesnego świata i niezrozumiała natura wielu szybko zachodzących zjawisk powodują, że potrzebne są nowe narzędzia poznawcze i nowe sposoby myślenia, które pomogą rozumieć i wyjaśniać zachodzące zdarzenia i procesy (np. współczesny terroryzm, pandemie, kryzysy finansowe czy rozprzestrzenianie się wiadomości w sieci) oraz prognozować ich rozwój. Wielu badaczy już od dawna sygnalizowało potrzebę zmiany sposobu postrzegania zjawisk społecznych. Mniej więcej od końca lat 80. XX w. ukazują się prace będące próbą wyjaśnienia nowych uwarunkowań, pojawiających się w coraz bardziej złożonym i szybko zmieniającym się współczesnym świecie. Wykorzystano w nich rozmaite podejścia poznawcze i metodologiczne, nierzadko były one zbliżone do modelowania zjawisk w perspektywie epidemiologicznej[2].

Wybuch pandemii COVID-19 i reorientacja nastrojów społecznych wywołały zrozumiały wzrost zainteresowania problematyką epidemiczną zarówno w środowiskach nauk społecznych, które podjęły badania nad społecznymi i psychicznymi skutkami tej pandemii, jak i w środkach masowego przekazu, które chętnie epatują zagrożeniem i sensacjami. Ta problematyka dominuje w prasie i w telewizji od ponad roku i skutecznie wypiera inne tematy dotychczas obecne w mediach. Na nową sytuację zareagował również światowy rynek wydawniczy, na którym pojawiła się znaczna liczba książek poruszających problematykę epidemiczną i wirusologiczną. Są to publikacje różnego rodzaju i jakości, od literatury medycznej przez rzetelne prace popularnonaukowe po książki dziennikarskie, sensacyjne oraz negacjonistyczne[3]. Rodzimy rynek czytelniczy jest pod tym względem wciąż ubogi, zaistniało na nim jedynie kilka pozycji z dziedziny nauk medycznych[4].

Publikacja Adama Kucharskiego niewątpliwie wychodzi naprzeciw oczekiwaniom czytelników niebędacych medykami. Autor jest profesorem, uznanym specjalistą z zakresu epidemiologii z Londyńskiej Szkoły Higieny i Medycyny Tropikalnej (London School of Hygiene and Tropical Medicine), uczelni o bogatych tradycjach badawczych i dużym wkładzie w poprawę stanu zdrowia publicznego na świecie, z poważnym dorobkiem badawczym w zakresie analizy dynamiki rozwoju groźnych chorób wirusowych, takich jak ebola i zika. Głównym obszarem dociekań naukowych autora jest matematyczne modelowanie przebiegu epidemii, co jest zadaniem trudnym. Prezentowane dotychczas modele rozwoju obecnej pandemii bardzo się różnią.

---

[2] J. Diamond, *Kryzysy. Punkty zwrotne dla krajów w okresie przemian*, Warszawa 2021; M. Gladwell, *Punkt przełomowy. O małych przyczynach wielkich zmian*, Kraków 2019; J. Harkin, *Trendologia. Niezbędny przewodnik po przełomowych ideach*, Kraków 2010; J. Naisbitt, *Megatrendy. Dziesięć nowych kierunków zmieniających nasze życie*, Warszawa 1997; F. Capra, *Punkt zwrotny*, Warszawa 1987.

[3] Zob. np. S. Bhagdi, K. Reiss, *Fałszywa pandemia. Krytyka naukowców i lekarzy*, Warszawa 2020.

[4] Por. L. Jabłoński, I.D. Karwal, *Podstawy epidemiologii – epidemie chorób zakaźnych*, Lublin 2002; R. Beaglehole, R. Bonita, T. Kjellstrom, *Podstawy epidemiologii*, Łódź 2002; J. Bzdęga, A. Gębska-Kuczerowska, *Epidemiologia w zdrowiu publicznym*, Lublin 2010; W. Jędrychowski, *Epidemiologia w medycynie klinicznej i zdrowiu publicznym*, Kraków 2010.

Znamienne, że od pewnego czasu w państwowych mediach głównego nurtu nie podaje się informacji dotyczących modelu tej pandemii. Nasza wiedza na temat jej dynamiki jest wciąż bardzo ograniczona i dalece niewystarczająca, wbrew buńczucznym i w istocie nieprawdziwym wypowiedziom części zbyt pewnych siebie ekspertów. Trzeba zatem, choćby na własny użytek, poszerzać wiedzę na temat mikrobiologii, zagrożeń i sposobów przeciwdziałania im oraz na temat praw rządzących zjawiskami epidemicznymi. Warto mieć na uwadze słowa Seneki, który radził, aby w odniesieniu do trudno zrozumiałych zjawisk prowadzących do życiowych dramatów stosować maksymę „nie płacz, nie przeklinaj, zrozum".

Dla uporządkowania terminologii w dyskursie publicznym trzeba przypomnieć, że pojęcie „epidemia" (gr. *epi* – na, *demos* – ludzie) jest używane w odniesieniu do występowania w określonym czasie i na określonym terenie przypadków zachorowań lub innych zjawisk determinujących stan zdrowia publicznego w skali znacznie przewyższającej dotychczasowy, czyli normalny, stan rzeczy. Występowanie takiego zjawiska w małej skali, tj. na niewielkim obszarze i w ograniczonym czasie, a także w formach izolowanych przestrzennie określa się terminem „ognisko epidemiczne". W polskiej materii ustawowej w odniesieniu do epidemii używa się terminu „choroba zakaźna" i mówi się o jej „rozprzestrzenianiu"[5]. Epidemia o bardzo dużym zasięgu w populacji i występująca na ogromnych obszarach globu jest nazywana „pandemią" (gr. *pan* – wszyscy, *demos* – ludzie). Natomiast w przypadku występowania aktywnych przypadków choroby zakaźnej wśród zwierząt (czy to domowych, czy dzikich) na skalę znacznie większą niż zwykle stosuje się termin „epizoocja" (łac. *epizootia*). W dyskursie publicznym i w mediach nagminnie i błędnie jest używane w tej sytuacji określenie „epidemia". Z kolei w odniesieniu do masowego rozprzestrzeniania się zachorowań w świecie roślin stosuje się termin „epifitoza" (gr. *epi* – na, *fito* – roślina).

Rozwój badań nad chorobami zakaźnymi i dynamiką ich rozprzestrzeniania się w populacjach zaowocował powstaniem nowej dyscypliny badawczej, jaką jest epidemiologia, która rozwija się od końca XIX w. Jest to nauka o rozpowszechnianiu się chorób i o czynnikach, które są warunkiem występowania zdarzeń i stanów determinujących zdrowie w określonych populacjach. To oznacza, że przedmiotem dociekań i analiz epidemiologicznych są nie tylko choroby, lecz także wszelkie zjawiska, procesy i zachowania ludzi, których skutkiem są zmiany stanu zdrowia publicznego. Do takich czynników należą np. palenie tytoniu, zażywanie substancji psychoaktywnych czy wypadki. Epidemiologia koncentruje się na konkretnych problemach zdrowotnych, takich jak epidemiologia wypadków komunikacyjnych, górskich, narciarskich, nad wodą itd. Zwykle są prowadzone proste badania opisowe, polegające na zestawieniu statystyk występowania wypadków i przedstawieniu tych zjawisk za pomocą przyjętych współczynników. Najczęściej jest to wskaźnik liczby przypadków na 100 tys. mieszkańców, co pozwala porównywać ze sobą różne populacje, zarówno w czasie, jak i w przestrzeni.

[5] Zob. *Ustawa z dnia 5 grudnia 2008 roku o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi* (t.j.: DzU z 2020 r. poz. 1845, ze zm.).

W analizach epidemiologicznych bierze się pod uwagę podstawowe kategorie zmiennych, jak: cechy demograficzne (wiek, płeć, grupa etniczna) i społeczne (stan cywilny, zawód, status społeczny), miejsce (kraj, region, województwo, miasto), czas zdarzeń (zmiany chwilowe dzienne oraz godzinowe, sezonowe, zmiany cykliczne), okoliczności towarzyszące (np. warunki meteorologiczne, przebyte lub współtowarzyszące choroby). W odniesieniu do sytuacji w społeczeństwie, państwie, regionie itp. stosuje się pojęcie „sytuacja epidemiczna", a wszelkie kwestie związane z aspektami badawczymi epidemii nazywamy „epidemiologicznymi". Zdarza się, że dziennikarze i politycy używają niepoprawnego sformułowania „sytuacja epidemiologiczna" zamiast właściwego – „sytuacja epidemiczna". Brak wiedzy i niechęć do przyswojenia pojęć z nowego obszaru zarządzania państwem były widoczne np. podczas wystąpienia jednego z polskich ministrów, który na konferencji prasowej oznajmił, że młodzież szkolna będzie bezpieczna, gdyż w razie wystąpienia przypadków zakażeń wirusem szkoła zostanie poddana „dezynsekcji".

Tym bardziej może cieszyć pojawienie się książki, której lektura sprzyja opanowaniu pojęć, aby w poprawny i precyzyjny sposób posługiwać się terminami wypracowanymi na gruncie nauk biologicznych i medycznych (mikrobiologia, bakteriologia, wirusologia, epidemiologia), a nie tworzonymi ad hoc w dyskursie medialnym. Pozycja jest obszerna, liczy 315 stron, została podzielona na osiem rozdziałów poświęconych kolejno: aspektom teoretycznym epidemiologii, zjawisku paniki towarzyszącej pandemii, zasadom zachowań międzyludzkich, zagadnieniom dotyczącym rozprzestrzeniania się chorób i przestępczości oraz czynnikom obniżania śmiertelności, wirusologii i zjawiskom społecznym o analogicznej dynamice rozprzestrzeniania się, jaką mają wirusy, zasadom tworzenia modeli epidemii, końcowym wnioskom na temat wielu aktualnych i na pozór niezwiązanych ze sobą zjawisk.

W rozdziale pt. *Teoria zdarzeń*, który otwiera książkę, autor omawia charakterystykę przebiegu typowych epidemii. Jako przykłady podaje zarówno choroby pandemiczne, jak i zjawisko rozprzestrzeniania się wirusów komputerowych, np. WannaCry, czy też rozwój rynku magnetowidów w latach 80. ubiegłego wieku (s. 13). W zwięzły sposób omawia genezę epidemiologii, przytacza pionierskie dokonania Ronalda Rossa w zwalczaniu malarii i jego matematyczny model choroby zakaźnej (s. 18–29). Warto przy okazji uzmysłowić sobie, że Europejczycy jeszcze niedawno byli zagrożeni chorobami poważniejszymi niż COVID-19, gdyż malaria zaniknęła na naszym kontynencie ostatecznie dopiero w 1975 r. W dalszej części wywodu Kucharski przedstawia koncepcję „odporności stadnej", wokół której toczyły się burzliwe dyskusje w 2020 r. Ten termin wprowadził do epidemiologii statystyk wojskowy kpt. Major Greenwood, aby określić zahamowanie transmisji choroby w wyniku uodpornienia dużego odsetka populacji (s. 32). Autor przytacza następnie dokonania Andersona McKendricka i Williama Kermacka, którzy opracowali tzw. model SIR (ang. *susceptible-infectious-recovered model*) przenoszenia choroby, polegający na wyodrębnieniu w populacji podatnych, zakażonych i ozdrowieńców (s. 28–33). Ten model wyjaśnia, dlaczego nie wszyscy chorują podczas epidemii. Ponadto zostaje opisana dynamika rozwoju

wydarzenia zależnego, ilustrowanego krzywą S, dobrze znaną w socjologii (s. 40). Przykładem wykorzystania modelu wydarzenia zależnego (inaczej zaraźliwego) było skuteczne prognozowanie w latach 60. XX w. sprzedaży kolorowych telewizorów. Lektura tego rozdziału nie wymaga ani specjalnego przygotowania, ani wiedzy matematycznej, a jedynie wytężonej uwagi, aby zrozumieć tok myślenia pionierów epidemiologii.

Rozdział drugi pod – mylącym w kontekście obecnej sytuacji – tytułem *Panika i pandemia* nie dotyczy reakcji współczesnych społeczeństw na zagrożenie COVID-19. Jest poświęcony rynkom finansowym, fluktuacjom giełdowym i wielkim aferom w nowożytnych dziejach Europy. To bardzo interesujący wykład z historii gospodarczej, w którym ukazano mechanizmy gry, spekulacji, hossy i bessy. Kucharski omawia m.in. gorączkę tulipanową w Holandii w latach 30. XVII w. oraz bańkę spekulacyjną brytyjskiej Kompanii Mórz Południowych z lat 1719–1720, w której ogromne straty poniósł Izaak Newton jako udziałowiec. W bańkach spekulacyjnych, analogicznie do epidemii, wyróżnia się cztery fazy: wybuch, wzrost, szczyt i spadek (s. 53). W książce są podane przykłady piramid finansowych i rynku dotcomów pod koniec lat 90. ubiegłego stulecia. Autor przywołuje mało znany fakt z 1998 r., kiedy analityk firmy AT&T obliczył, że Internet rozrasta się w tempie niemogącym zapewnić takiego wzrostu popytu na rynku, który uzasadniałby inwestowanie w dostawców Internetu, takich jak WorldCom. Tę analizę jednak zlekceważono. Dalszy rozwój podstaw teoretycznych epidemiologii, który zawdzięczamy londyńskiemu badaczowi Georgeʼowi MacDonaldowi, zaowocował ambitnymi planami Światowej Organizacji Zdrowia. W 1955 r. postanowiła ona wyeliminować najgroźniejsze choroby zakaźne, takie jak malaria i ospa. Nieco później matematyk Klaus Dietz opracował koncepcję współczynnika reprodukcji R, czyli wskaźnika, ile osób może zakazić jeden zarażony (s. 59–62). Wartość R zależy od iloczynu czasu zakażenia danej osoby (ang. *duration*), średniej liczby okazji do przekazania infekcji każdego dnia (ang. *opportunities*), prawdopodobieństwa, że nastąpi zakażenie kolejnej osoby (ang. *transmission*) oraz średniej podatności populacji (ang. *susceptibility*). Wzór na współczynnik reprodukcji można zatem określić akronimem DOTS (s. 63). Kiedy charakteryzowano dynamikę rozwoju epidemii malarii oraz HIV, zaproponowano wzór 20/80, oznaczający, że ok. 20 proc. chorych odpowiada za zakażenie 80 proc. dalszych przypadków. Jeszcze wyższy wskaźnik miała epidemia SARS w 2003 r. – 20/90. Mniejszą dynamikę miała z kolei dżuma – w tym przypadku wskaźnik wyniósł tylko 20/50 (s. 65). Kucharski przytacza też dokonania matematyka Paula Erdsa, który wraz z Alfredem Renyim opracował teorię analizy sieciowej umożliwiającej obserwację zjawisk długodystansowych powiązań (s. 67–68), a następnie prowadził badania dynamiki roznoszenia chorób wenerycznych. W związku z epidemią AIDS dziennikarz Randy Shilts wprowadził w 1987 r. w swej książce pojęcie „pacjent zerowy", które przyjęło się w nauce (s. 71). Kucharski wyjaśnia także (znany już fakt), dlaczego grypę z 1918 r. nazwano hiszpanką. Hiszpania, w przeciwieństwie do większości ówczesnych państw, nie wprowadziła cenzury wojskowej, dlatego doniesienia na temat rozwoju tej choroby były obecne w prasie. W związku z tym media innych krajów zaczęły sugerować, że to Hiszpania jest krajem najbardziej dotkniętym epidemią. Lektura tego interesującego

rozdziału musi prowadzić do smutnej refleksji na temat płytkiej wiedzy dziennikarzy, decydentów, a także przedstawicieli części środowiska lekarskiego (reprezentujących notabene różne specjalności medyczne, lecz nie epidemiologię), którzy występowali przed kamerami telewizyjnymi w roli ekspertów.

Tematyka trzeciego rozdziału pt. *Miara przyjaźni* koncentruje się wokół mechanizmów rozpowszechniania idei społecznych oraz teorii naukowych. Już na początku lat 60. XX w. amerykański matematyk William Goffman porównał przepływ informacji między ośrodkami naukowymi do epidemii, co można łatwo udowodnić na podstawie sieci cytowań prac naukowych (s. 87 i 89). Żeby zrozumieć koncepcje zaraźliwości – pisze autor – (…) *trzeba badać, jak ludzie wchodzą w interakcje, a więc mierzyć kontakty społeczne, co jest wszakże wyjątkowo trudnym zadaniem.* Kucharski omawia zjawiska superroznosicieli, hemofilii, odwrotnego skutku, efektu zaprzeczania i głębokiej agitacji, dając w ten sposób interesujący wykład z pogranicza socjologii i psychologii społecznej.

Rozdział czwarty, zatytułowany dość kolokwialnie *Co wisi w powietrzu*, stanowi krótki wywód na temat epidemii przemocy. Na przykładzie przestępczości w Chicago autor przedstawia zjawisko fal przemocy w walce gangów. Nawiązuje do pionierskich badań Johna Snowa, który analizował rozprzestrzenianie się cholery w Londynie w 1854 r. (s. 119–122). Ten badacz, na podstawie profilowania geograficznego, odkrył przyczynę epidemii, którą była skażona woda ze studni w dzielnicy Soho. Jego dokonania nie zyskały aprobaty przedstawicieli ówczesnego świata nauki, w którym obowiązywała teoria zatrutego powietrza. Kucharski wskazuje podobieństwa między cechami epidemii cholery i epidemii przemocy (s. 124). Te przemyślenia powinny zainteresować nie tylko kryminologów, lecz także osoby kierujące policją. Skala przestępczości chicagowskiej przytaczana przez autora robi przytłaczające wrażenie, w policyjnej bazie danych osób aresztowanych tylko w ciągu ośmiu lat znajdowało się dossier 462 tys. osób. W rozdziale została przybliżona także postać Florence Nightingale i jej dokonania analityczne, szczególnie w zakresie badań statystycznych (s. 132–134), przedstawiona historia zmagań o poprawę konstrukcji samochodów w USA, epidemia błonicy w Bangladeszu, rekrutacja do ISIS oraz opisane rozprzestrzenianie się zamieszek rasowych w Wielkiej Brytanii i omówiony amerykański kryzys opioidowy. Niezwykle interesujący jest przykład, w jaki sposób w RFN osiągnięto błyskawiczny spadek liczby kradzieży motocykli. Otóż wprowadzono obowiązek jazdy w kasku, co spowodowało, że złodzieje kręcący się na parkingach musieliby je nosić ze sobą (s. 155). Końcowy wniosek zawarty w tym rozdziale wydaje się trywialny: (…) *na błędy w prognozowaniu* – konstatuje profesor – *składa się albo zbyt mało danych liczbowych, albo błąd w konstruowaniu modelu* (s. 146).

Rozdział piąty pt. *Jak wirus* odnosi się do zagadnień dotyczących marketingu i reklamy, przepływu informacji na Facebooku, trollowania oraz zaraźliwości treści internetowych. Szacuje się, że ilość cyfrowych informacji na świecie podwaja się co dwa lata (s. 190). Nie od rzeczy będzie przypomnienie poglądu Stanisława Lema na Internet i większość jego zasobów, które wybitny pisarz i filozof określił lapidarnie jako śmieci

w sieci. Najciekawsza jest informacja o badaniach poświęconych stronom internetowym zawierającym ekstremistyczną propagandę, teorie spiskowe, pseudonaukowe wynurzenia i skrajnie prawicowe poglądy. Badania Johanna Albrighta z 2017 r. wykazały, że mimo pozornej amatorszczyzny w redagowaniu tych stron zawierały one niezwykle złożone narzędzia do śledzenia tożsamości osób, ich aktywności w przeglądarkach itp. Te strony były niezmiernie wpływowe nie ze względu na zawarte na nich treści, ale dane, jakie potajemnie zbierały (s. 193). Rzuca to nowe światło na fenomen utrzymywania się i rozwoju radykalnej prawicy w niektórych krajach. Te praktyki wskazują, że są zakulisowe ośrodki, którym zależy na istnieniu tego rodzaju ekstremy. W dalszej części rozdziału Kucharski rozprawia się ze stereotypem ukształtowanym w mediach, że Rosjanie mieli wpływ na wynik wyborów prezydenckich w Stanach Zjednoczonych w 2016 r. Przytacza wiele danych liczbowych i dowodzi, że na jeden post rosyjskiego autorstwa przypadało około 90 tys. innych. Jednocześnie rosyjskie wpływy na Twitterze należałoby w tamtej kampanii szacować na 0,75 proc. (s. 198–199). Autor krytycznie odnosi się do kategorii pojęciowej „fake news" wprowadzonej w 2016 r., gdyż sformułowanie to jest niejednoznaczne i oznacza zarówno fałszywe informacje, teorie spiskowe, dezinformację, jak i wiele innych zjawisk (s. 203). Interesująca jest również charakterystyka chińskiej polityki wobec Internetu i szczególnego rodzaju narzędzi cenzury. Oba te rozdziały mają największą objętość i stanowią ponad jedną trzecią całości wykładu na temat praw epidemii, a zarazem najważniejszą część książki.

Następny, bardzo zwięzły rozdział nosi tytuł *Jak przejąć Internet.* Jest poświęcony zjawiskom zachodzącym w sieci i skoncentrowany wokół Internetu rzeczy (Internet of Things, IoT), które to pojęcie jest słabo znane w polskim społeczeństwie. Na przykładzie tzw. ataku Mirai z 2016 r. autor pokazuje, jak łatwo rozprzestrzeniają się sztuczne infekcje (s. 212 i nast.). Czytelnik może poznać krótką historię wirusów komputerowych, poczynając od pierwszego wirusa Elk Cloner, zaprojektowanego dla żartu w 1982 r. przez ucznia z Pensylwanii. Kucharski stwierdza jednoznacznie, że genezą złośliwego oprogramowania były tajne projekty rządowe, lecz nie używa w swej pracy pojęć „cyberwojna" i „cyberatak" (s. 218). Podaje przykłady zarówno poważnych zagrożeń, takich jak zainfekowanie irańskiego programu jądrowego, jak i przywołuje zabawne w gruncie rzeczy przypadki awarii systemów wywołane banalnymi przyczynami.

Kolejny rozdział książki zatytułowany *Śledzenie epidemii* jest poświęcony m.in. zagadnieniom graficznego obrazowania procesów ewolucji i transmisji. Autor omawia zarówno drzewo genealogiczne brytyjskiej rodziny królewskiej, jak i drzewo ewolucyjne Darwina oraz drzewo filogenetyczne wirusa SARS, którego średni okres wylęgania oszacowano już w 2003 r. na 6,4 dnia. Metoda filogenetyczna, powszechnie stosowana w analizach z zakresu zdrowia publicznego, pozwala zarówno na wskazanie źródła epidemii, jak i ujawnienie, kiedy dana choroba dotarła w konkretne miejsce (s. 232). Można ją też wykorzystać w badaniach kulturoznawczych, np. w odniesieniu do genezy baśni i legend (dzięki temu stwierdzono, że niektóre opowieści są tak stare jak języki indoeuropejskie). W dalszej części tego rozdziału został poruszony problem bezpieczeństwa danych osobowych. Badania Latanyui Sweeny z połowy lat 90. XX w. wykazały, że same dane dotyczące

wieku, płci i kodu pocztowego umożliwiają zidentyfikowanie osoby (s. 245). Analiza dostępnych danych na temat tras taksówek na Manhattanie pozwoliła na identyfikację celebrytów i ustalenie, w jaki sposób spędzają wolny czas (s. 246). Dane konsumenckie z systemu GPS mogą zagrażać obronności. Autor podaje przykład udostępnienia informacji na temat tras biegowych i rowerowych przez komercyjne urządzenia, z których korzysta personel wojskowy podczas ćwiczeń.

Ostatni i najkrótszy rozdział książki zatytułowany *Kawałek brudu* jest poświęcony wyzwaniom i trudnościom w badaniach dotyczących pojawiających się epidemii. Została w nim poruszona problematyka *big data* (dużych zbiorów danych), w tym projekt GFT, a także bulwersujący projekt profilowania psychologicznego amerykańskich i brytyjskich wyborców przez Cambridge Analytica. Końcowy wniosek autora książki odnosi się do rozwoju nauki. Pisze on, że (…) *w epidemiologii najważniejsze chwile to nie te, kiedy mamy rację. To te, kiedy zdajemy sobie sprawę z tego, że się myliliśmy* (s. 263). Ta myśl jest zgodna z Popperowskim rozumieniem wiodącej roli falsyfikacji w procesie rozwoju wiedzy naukowej.

Lektury książki nie ułatwia niestety wykaz przypisów, który został zamieszczony na końcu publikacji (s. 263–307). Całości dopełnia suplement zatytułowany *Dodatkowe źródła.* Zawiera on spis literatury (s. 308–313) i jest przeznaczony dla najbardziej zainteresowanych czytelników. W książce znalazały się również podziękowania złożone najbliższym współpracownikom autora i pierwszym czytelnikom jego rozprawy, umieszczone, co rzecz dziwna, na końcu, a nie na początku publikacji (s. 314–315). Przekład Jowity Maksymowicz-Hamann jest doskonały, zawiera jednak błąd w nazwie nowojorskiej uczelni (s. 161). Otóż Columbia University w Nowym Jorku to nie Uniwersytet Kolumbijski, jak uznała tłumaczka. Takie tłumaczenie mogłoby być usprawiedliwione w odniesieniu do uniwersytetu w Bogocie. Uwagę zwracają estetyczna szata graficzna, dobrze zaprojektowana okładka i czytelne wykresy, dzięki czemu po *Prawa epidemii* sięga się z prawdziwą przyjemnością.

Na koniec lektury można odnieść wrażenie, że niektóre rozważania autora mają wiele wspólnego z memetyką, zwłaszcza jej rozumieniem zaproponowanym przez psychologa Stevena Pinkera, według którego memetyka miała być dziedziną wiedzy bliską epidemiologii. Zbliżoną perspektywę przyjął swego czasu Douglas Rushkoff, tworząc koncepcję mediów wiralnych odwołującą się do wirusologii (ang. *viral media* lub *media virus*)[6]. Metaforę wirusologiczną wykorzystał wcześniej William S. Burroughs w swej powieści oraz w eseju poświęconym rewolucji elektronicznej, w których przedstawił ideę rozwoju i oddziaływania języka jako wirusa[7]. Memetyka była koncepcją dotyczącą badania procesów replikacji memów, ich rozprzestrzeniania się i ewolucji. Nie chodzi tu rzecz jasna o obecne, potoczne rozumienie tego pojęcia związane z żartami rysunkowymi zamieszczanymi w Internecie. Termin „mem" został stworzony przez Richarda Dawkinsa i zdefiniowany jako jednostka przekazu kulturowego lub

[6] Por. D. Rushkoff, *Media Virus: Hidden Agendas in Popular Culture,* New York 1994.

[7] Por. W.S. Burroughs, *The Ticket that Exploded*, Paris 1962.

jednostka naśladownictwa będąca replikatorem kulturowym analogicznym do genu, który jest replikatorem w biologii[8]. Termin pochodzi od greckich słów *mimos, mimētēs* i *mimēsis* oznaczających naśladowcę, naśladowanie oraz naśladownictwo. Niemiecki biolog Richard Semon już w 1904 r. wprowadził do rozważań na temat ewolucji kultury zbliżone do memu pojęcie „mneme". W Polsce prace poświęcone memetyce pojawiły się w połowie lat 90. ubiegłego wieku[9]. W światowej społeczności akademickiej memetyka została jednak uznana za błędny paradygmat nauk o kulturze, czego dobitnym wyrazem było zaprzestanie w 2005 r. wydawania czołowego czasopisma na ten temat, zatytułowanego „Journal of Memetics".

Reasumując, czytelnik książki Kucharskiego otrzymuje interesujący wykład z podstaw epidemiologii i jej wykorzystywania do analizy różnych zjawisk, zachodzących zarówno w obszarze zdrowia publicznego, jak i życia społecznego, ekonomii, nowych mediów, popkultury. Jest on napisany barwnym językiem, przystępnie i zrozumiale. Lekturę można polecić wszystkim chcącym poszerzyć swoją wiedzę na tematy, które nie są przedmiotem nauczania nie tylko w szkołach niższego szczebla, lecz także na uczelniach (poza studiami medycznymi, i to w bardzo wąskim zakresie), a których znajomość może okazać się przydatna w czasach pandemii. Książkę powinni przeczytać zarówno wykładowcy każdej z dyscyplin nauk społecznych, jak i oficerowie służb specjalnych, aby lepiej rozumieć skomplikowaną naturę otaczającego nas świata. Można bowiem narzekać, złościć się na przeciwności, ale można też, za radą rzymskich stoików, podjąć wysiłek zrozumienia zawiłych procesów rządzących się w istocie prawami wielkich liczb. Książka Adama Kucharskiego to zrozumienie niewątpliwie ułatwia.

[8] R. Dawkins, *Samolubny gen*, Warszawa 1996.

[9] Zob. np. M. Biedrzycki, *Genetyka kultury*, Warszawa 1998; R. Boroch, *Przeciw memetyce*, „Hybris" 2011, nr 15, s. 62–99.

III

PRZEGLĄD PRAC KONKURSOWYCH

OVERVIEW OF THE WORKS

JACEK MICHAŁ WOJCIECHOWSKI
ORCID: 0000-0003-0520-3379

DOI: 10.4467/20801335PBW.21.030.14307

Typy uprzywilejowane przestępstwa korupcji wyborczej[1]

Ustanowienie wypadku mniejszej wagi (art. 250a § 3 kk) należy postrzegać jako swoiste novum w zakresie kryminalizacji korupcji wyborczej w polskim porządku prawnym. Do chwili wejścia w życie tzw. noweli antykorupcyjnej z 13 czerwca 2003 r.[2] ustawodawca nie korzystał z tego rodzaju instrumentów prawnych na gruncie normatywnej konstrukcji tego przestępstwa. Jakkolwiek instytucja wypadku mniejszej wagi była znana Kodeksowi karnemu z 1932 r.[3], to jednak nie znajdowała zastosowania do typów korupcji wyborczej (art. 121–123 kk), jak również innych czynów korupcyjnych występujących w tej kodyfikacji[4]. Warto zwrócić uwagę, że Kodeks karny z 1932 r., do którego rozwiązań nawiązywali twórcy noweli antykorupcyjnej z 13 czerwca 2003 r., nie przewidywał odmian rodzajowych przestępstwa korupcji wyborczej, chociaż statuował typy kwalifikowane korupcji w sektorze publicznym (art. 290 § 2 kk)[5].

---

[1] Artykuł jest zmodyfikowanym i zaktualizowanym fragmentem rozprawy doktorskiej (VI rozdział) pt. *Przestępstwo korupcji wyborczej w polskim prawie karnym (art. 250a kk)* (Uniwersytet Mikołaja Kopernika w Toruniu, Wydział Prawa i Administracji).

[2] *Ustawa z dnia 13 czerwca 2003 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (DzU z 2003 r. nr 111 poz. 1061).

[3] *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. – Kodeks karny* (DzU z 1932 r. nr 60 poz. 571).

[4] Zob. R. Żurowska, *Przestępstwo korupcji w sporcie*, Poznań 2010, s. 141; *Projekt kodeksu karnego oraz przepisów wprowadzających kodeks karny*, Warszawa 1968, s. 54. Zmiany w tym zakresie nastąpiły wraz z wejściem w życie Kodeksu karnego z 1969 r. (*Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny* – DzU z 1969 r. nr 13 poz. 94 – przyp red.), który mimo że nie przewidywał penalizacji korupcji wyborczej, to jednak wprowadzał instytucję wypadku mniejszej wagi na grunt przestępstwa korupcji w sektorze publicznym.

[5] Zob. art. 290 § 2 kk z 1932 r.: „Jeżeli sprawca uzależnia czynność urzędową od otrzymania dla siebie lub innej osoby korzyści majątkowej lub osobistej, albo przyjmuje korzyść taką lub jej obietnicę za czynność, która sprzeciwia się lub ma się sprzeciwiać ustawie, podlega karze więzienia do lat 10".

Jednym z głównych czynników implikujących możliwość zastosowania art. 250a § 3 kk będzie rodzaj i charakter naruszonego dobra, którym w przypadku art. 250a kk jest rzetelność głosowania w wyborach i referendach. Przedmiot ochrony jest tutaj tożsamy dla obu typów korupcji wyborczej, gdyż sprawcy tych czynów zabronionych atakują to samo dobro prawne, ale niejako z innej strony. W doktrynie wskazuje się, że charakter tego dobra powinien przemawiać przeciwko decyzji o utworzeniu typu uprzywilejowanego wypadku mniejszej wagi przestępstwa korupcji wyborczej (art. 250a § 3 kk)[6]. Należy zgodzić się z tym poglądem, gdyż popełnienie przestępstw z art. 250a § 1–2 kk bez względu na treść czy wartość korzyści w jednakowy sposób godzi w dobro prawne podlegające ochronie na podstawie art. 250a kk, poddając w wątpliwość ostateczny rezultat głosowania. Biorąc pod uwagę rolę, jaką w polskim porządku prawnym odgrywają wybory i referenda, decyzja legislacyjna o utworzeniu typu uprzywilejowanego z art. 250a § 3 kk może wydawać się pod tym względem kontrowersyjna.

Kolejnym istotnym czynnikiem determinującym możliwość przyjęcia kwalifikacji czynu jako wypadku mniejszej wagi jest rozmiar wyrządzonej lub grożącej szkody. W zależności od jej rodzaju przy dokonywaniu oceny należy kierować się jej wysokością (szkoda majątkowa) lub jej charakterem (szkoda niemajątkowa) bądź brać pod uwagę szkodę, która zagrażała określonemu dobru prawnemu w następstwie zachowania sprawcy[7]. Wskazany czynnik, z uwagi na zawarty w nim element kwantytatywny, determinuje konieczność ustalenia wielkości szkody. Im jest ona wyższa, tym wyższy jest jego poziom[8]. W piśmiennictwie są wyrażane poglądy, w świetle których lokalny wymiar wyborów przemawia za przyjęciem niższego stopnia społecznej szkodliwości czynu w porównaniu z wyborami przeprowadzanymi na szczeblu ogólnopaństwowym[9]. Polemizując z tym stanowiskiem, należy wskazać, że przy prawnokarnej ocenie danego zachowania na podstawie art. 250a § 3 kk okoliczności takie, jak rodzaj wyborów lub referendum, ich ranga czy popularność, jaką cieszą się one wśród osób uprawnionych do głosowania, nie powinny mieć znaczenia. Należy wskazać, że wypełnienie znamion sprzedajności oraz przekupstwa wyborczego w obrębie wyborów na szczeblu samorządowym (wyborów do rady gminy, rady powiatu oraz sejmiku województwa) w praktyce powinno być traktowane na równi z podejmowaniem tego rodzaju czynności w przypadku innych kategorii wyborów powszechnych przeprowadzanych na podstawie przepisów Kodeksu wyborczego

---

[6] J. Sobczak, *Przestępstwo korupcji wyborczej*, w: *Przemiany prawa wyborczego – doświadczenia nowych demokracji*, A. Sokala, Z. Witkowski (red.), Bydgoszcz 2007, s. 115. Zob. również: W. Kozielewicz, w: *Kodeks karny. Komentarz*, R. Stefański (red.), Warszawa 2020, s. 1685.

[7] M. Budyn-Kulik, w: *Kodeks karny. Komentarz*, M. Mozgawa (red.), Warszawa 2017, s. 357–358 wraz z orzecznictwem przywołanym przez autorkę. Zob. Wyrok Sądu Najwyższego (dalej: SN) z 8 III 1972 r., II KR 329/71, Lex nr 21470; Wyrok SN z 25 X 1984 r., V KRN 336/84, OSNPG 1985, nr 5, poz. 66.

[8] A. Grześkowiak, w: *Kodeks karny. Komentarz*, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, s. 868.

[9] M. Iwański, *Odpowiedzialność karna za przestępstwa korupcyjne*, Kraków 2016, s. 645.

z 5 stycznia 2011 r.[10] (wyborów na urząd Prezydenta RP, wyborów do Sejmu i Senatu RP). Należy bowiem zauważyć, że wszystkie wymienione kategorie wyborów nie tylko zostały uregulowane w jednym akcie prawnym, lecz także korzystają z takiej samej ochrony na gruncie kodeksu karnego. Powyższa uwaga w takim samym stopniu będzie odnosić się do wyborów terminowych i do wyborów uzupełniających, ponownych czy przedterminowych, które co do zasady cechują się ograniczonym zasięgiem terytorialnym oraz cieszą się mniejszym zainteresowaniem wyborców. Podobnie ten problem będzie się przedstawiał w przypadku referendów. Ustawodawca, nadając rozdziałowi XXXI kk tytuł *Przestępstwa przeciwko wyborom i referendum* oraz wymieniając określone kategorie głosowań w dyspozycji art. 248 kk, dał wyraz temu, że obu tym instytucjom zamierza udzielać takiej samej ochrony prawnej. Z tego względu poglądy, w świetle których np. głos oddany w referendum lokalnym miałby mieć mniejszą wagę niż głos oddany w referendum ogólnokrajowym czy w wyborach na urząd Prezydenta RP, nie wydają się trafne. Należy bowiem zgodzić się z osądem, że (…) *relatywna siła jednego głosu w wyborach czy referendach lokalnych może okazać się tutaj większa niż w wielu przejawach demokracji o zasięgu ogólnokrajowym*[11].

W kontekście możliwości stosowania art. 250a § 3 kk należy mieć na uwadze również realia towarzyszące referendom ogólnokrajowym i lokalnym. Ich przedmiotem może być zarówno jedno zagadnienie, jak i kilka spraw o różnorodnym charakterze, stopniu skomplikowania czy znaczeniu praktycznym[12]. Nie ulega wątpliwości, że wymienione okoliczności mogą rzutować na możliwość prawnokarnej oceny danego zachowania przez pryzmat art. 250a § 3 kk. Nie można bowiem stawiać znaku równości między udzieleniem i przyjmowaniem korzyści za głosowanie w określony sposób w referendum (zarówno lokalnym, jak i ogólnokrajowym), polegający na zaznaczeniu na karcie do głosowania odpowiedzi na pytania dotyczące kilku istotnych spraw poddawanych pod głosowanie (tj. odpowiedzi na kilka najważniejszych pytań referendalnych),

---

[10] *Ustawa z dnia 5 stycznia 2011 r.* – Kodeks wyborczy (t.j.: DzU z 2020 r. poz. 1319) – przyp. red.

[11] J. Potulski, *Kodeks karny. Komentarz do zmian wprowadzonych ustawą z dnia 13 czerwca 2003 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U.03.111.1061)*, Lex/el 2004, art. 250a kk, teza nr 8.

[12] Zob. *Referendum lokalne. Niedziela 25 maja 2014 r.*, https://www.bip.krakow.pl/?dok_id=60751 [dostęp: 29 VII 2017]. Przykładem ilustrującym istotę tego wywodu mogą być kategorie spraw będących przedmiotem głosowania w referendum lokalnym w Krakowie przeprowadzonym 25 V 2014 r. W ramach referendum zadano następujące pytania: 1. Czy jest Pani/Pan za zorganizowaniem i przeprowadzeniem przez Kraków Zimowych Igrzysk Olimpijskich w 2022 r.? Głosów na „Tak" było 62 453 (30,28%), głosów na „Nie" – 143 796 (69,72%). 2. Czy jest Pani/Pan za budową metra w Krakowie? Głosów na „Tak" było 112 856 (55,11%), głosów na „Nie" – 91 939 (44,89%). 3. Czy jest Pani/Pan za stworzeniem w Krakowie systemu monitoringu wizyjnego, którego celem byłaby poprawa bezpieczeństwa w mieście? Głosów na „Tak" było 142 772 (69,73%), głosów na „Nie" – 61 969 (30,27%). 4. Czy zdaniem Pani/Pana w Krakowie powinno się budować więcej ścieżek rowerowych? Głosów na „Tak" było 175 033 (85,20%), głosów na „Nie" – 30 398 (14,80%). Szerzej na temat tego referendum zob. M. Rulka, *Referendum w sprawie organizacji przez Kraków Zimowych Igrzysk Olimpijskich w 2022 r.*, „Samorząd Terytorialny" 2015, nr 5, s. 56–66.

a głosowaniem wyłącznie w jednej sprawie, która dodatkowo może nie mieć większego znaczenia praktycznego.

Prawnokarna kwalifikacja danego zachowania na podstawie art. 250a § 3 kk będzie uzależniona od skutków wywołanych zachowaniem sprawcy, zwłaszcza ich wpływu na ostateczny rezultat głosowania w wyborach lub referendum. Wspomniana uwaga dotyczy przede wszystkim przekupstwa wyborczego z art. 250a § 2 kk, gdyż w odróżnieniu od sprzedajności wyborczej zachowanie sprawcy co do zasady nie będzie ograniczać się do jednorazowej realizacji znamion tego przestępstwa w trakcie odbywających się wyborów lub referendum. Ocena dokonywana w tym zakresie powinna uwzględniać ostateczny rezultat głosowania, gdyż jak wskazuje się w piśmiennictwie, rozmiar wyrządzonej i grożącej szkody nie może abstrahować od charakteru naruszonego lub zagrożonego dobra[13]. Jeżeli pomimo podejmowania przez sprawcę zachowań wypełniających znamiona sprzedajności lub przekupstwa wyborczego nie dojdzie do osiągnięcia założonego przez niego celu (np. referendum okaże się nieważne z powodu zbyt niskiej frekwencji) bądź sprawca nie uzyska satysfakcjonującego wyniku głosowania (np. otrzyma niewystarczającą liczbę głosów), to nie ulega wątpliwości, że tego rodzaju zachowania będą cechować się mniejszym ładunkiem karygodności niż typowe zamachy korupcyjne związane z wyborami i referendum. Zastosowanie wypadku mniejszej wagi z art. 250a § 3 kk będzie możliwe w sytuacjach, w których pomimo podejmowania przez sprawcę tego rodzaju zamachów korupcyjnych nie wpłynie to negatywnie na ostateczny rezultat głosowania (np. dany kandydat nie miałby problemów z wygraniem wyborów mimo pozyskania określonej liczby głosów w zamian za korzyść majątkową lub osobistą).

Czynnikami, które mogą rzutować na ocenę społecznej szkodliwości, są sposób oraz okoliczności popełnienia danego czynu zabronionego. W piśmiennictwie wskazuje się, że w grę może wchodzić szeroki katalog przesłanek[14], obejmujących zarówno czyn, jak i jego sprawcę[15]. W pierwszej z tych grup czynników należy wyróżnić współdziałanie z nieletnim, premedytację, wykorzystanie nadarzającej się sposobności, z kolei elementem dotyczącym sprawcy będzie np. uleganie wpływom innych osób[16]. Uwzględniając powyższe poglądy, należy wskazać, że przeszkodą w prawnokarnej

[13] O. Górniok, J. Bojarski (aktualizacja), w: *Kodeks karny. Komentarz*, M. Filar (red.), Warszawa 2016, s. 802.

[14] Odmiennie: J. Majewski, w: *Kodeks karny. Część ogólna, tom I. Komentarz do art. 53–116*, W. Wróbel, Z. Zoll (red.), Warszawa 2016, s. 954. Zdaniem autora zakres tego faktora nie jest szeroki i obejmuje czas (np. pora nocna), miejsce (np. miejsce publiczne), a także tzw. kontekst sytuacyjny (działanie publiczne, we współdziałaniu z nieletnim lub w jego obecności, w reakcji na naganne zachowanie się pokrzywdzonego itp.).

[15] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 308.

[16] M. Budyn-Kulik, w: *Kodeks karny. Komentarz*…, s. 358 wraz z przywołaną tam literaturą. Zob. także: Wyrok SN z 15 XI 1984 r., II KR 248/84, OSNKW 1985, nr 7–8, poz. 61. Jak wskazał SN w przywołanym judykacie: „Stopień demoralizacji może przejawiać się nie tylko przez uprzednie popełnianie przestępstw w ogóle czy popadanie w konflikty z prawem, ale może wyrazić się także w sposobie przygotowania i realizacji tego przestępstwa, które jest aktualnie przedmiotem osądu".

kwalifikacji danego czynu na podstawie art. 250a § 3 kk może być publiczny charakter zachowania sprawcy (np. udzielanie i przyjmowanie korzyści majątkowych lub osobistych w okolicach bądź wewnątrz lokalu wyborczego, w miejscach kultu religijnego).

Przedstawiciele doktryny prawa karnego w nielicznych wypowiedziach dotyczących charakterystyki wypadku mniejszej wagi przy korupcji wyborczej co do zasady zgodnie wskazują, że najważniejszą rolę w prawnokarnej kwalifikacji danego zachowania na podstawie art. 250a § 3 kk będą odgrywać wartość korzyści majątkowej i charakter korzyści osobistej[17]. Takie ujęcie tej materii nie powinno dziwić, zwłaszcza że w podobny sposób ten problem jest postrzegany w przypadku innych czynów korupcyjnych wskazanych w Kodeksie karnym z 6 czerwca 1997 r.[18] (art. 228 § 2 kk i art. 229 § 2 kk)[19]. Opisana koncepcja koresponduje z poglądami judykatury, gdyż jak zauważył Sąd Najwyższy w wyroku z 8 marca 1983 r.: *Wielkość udzielonej korzyści majątkowej jest elementem rzutującym na społeczne niebezpieczeństwo przestępstw przekupstwa, a więc elementem wyłączającym możliwość uznania danego czynu jako wypadku mniejszej wagi*[20]. Jak zaznacza Jacek Potulski, w obrębie wypadku mniejszej wagi przy korupcji wyborczej mogą mieścić się przypadki pozyskiwania głosów w zamian za drobne podarunki (w tym za przysłowiową kiełbasę wyborczą)[21]. Należy w pełni zgodzić się z przedstawionym poglądem, gdyż znajduje on oparcie w art. 115 § 2 Kodeksu karnego z 6 czerwca 1997 r., zgodnie z którym tego typu elementy wpływają na ocenę stopnia społecznej szkodliwości czynu. Powyższa uwaga będzie dotyczyć sytuacji, w których korzyścią majątkową będą drobne artykuły spożywcze (takie, jak np.: chleb, mleko, masło, słodycze itp.), napoje alkoholowe o niewielkiej wartości lub ilości (piwo, wino), papierosy bądź niewielkie kwoty pieniężne. Realizacja znamion typu uprzywilejowanego korupcji wyborczej może przybrać postać udzielania tego rodzaju korzyści, częstowania nimi (np. wysokoprocentowymi trunkami) bądź ich sprzedaży po niższej cenie. Należy jednak zachować dużą ostrożność przy dokonywaniu prawnokarnej oceny tego rodzaju zachowań, gdyż nierzadko ich stopień społecznej szkodliwości może oscylować na granicy znikomości i przemawiać za umorzeniem postępowania karnego (art. 17 § 1 pkt 3 kpk). Z tego typu sytuacją możemy mieć do czynienia w przypadku bardzo niskiej wartości korzyści (np. poczęstunku papierosem czy kostką czekolady).

---

[17] M. Iwański, *Odpowiedzialność karna*…, s. 645; J. Jurewicz, *Przestępstwa przeciwko wyborom i referendum z rozdziału XXXI*, „Studia Wyborcze" 2006, t. 2, s. 35–36; J. Potulski, *Kodeks karny. Komentarz do zmian*…, Lex/el. 2004, komentarz do art. 250a kk, teza nr 8; J. Skorupka, *Przestępstwo korupcji wyborczej z art. 250a kk*, „Palestra" 2006, nr 11–12, s. 49–50; R.A. Stefański, *Przestępstwo korupcji wyborczej (art. 250a kk)*, „Prokuratura i Prawo" 2004, nr 4, s. 78; M. Surkont, *Łapownictwo*, Sopot 1999, s. 65.

[18] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (DzU z 1997 r. nr 88 poz. 553, ze zm.) – przyp. red.

[19] J. Lachowski, w: *Kodeks karny. Część szczególna, tom II. Komentarz. Art. 222–316*, M. Królikowski, R. Zawłocki (red.), Warszawa 2017, s. 119.

[20] Wyrok SN z 8 III 1983 r., I KR 387/82, Lex nr 21972.

[21] J. Postulski, *Kodeks karny. Komentarz do zmian*…, Lex/el. 2004, komentarz do art. 250a kk, teza nr 8.

W kontekście korzyści majątkowej najważniejszą sprawą będzie ustalenie kwoty uzasadniającej dokonanie prawnokarnej kwalifikacji danego czynu na podstawie art. 250a § 3 kk. Zasadniczy problem dotyczy trudności w wycenie pojedynczego głosu, gdyż tego rodzaju dobra na co dzień nie występują w obrocie prawnym. Dotychczasowa praktyka stosowania art. 250a kk pokazuje, że kwoty pieniężne, z którymi w takiej sytuacji mamy do czynienia, nie są zbyt wysokie (5 zł, 20 zł, 50 zł)[22], a ich wartość jest wyrazem subiektywnej wyceny głosu przez osoby uprawnione do głosowania. Kwoty te mają wartość zbliżoną do tzw. zwyczajowych dowodów wdzięczności, których udzielanie i przyjmowanie na gruncie art. 228 § 2 kk i 229 § 2 kk nie skutkuje odpowiedzialnością karną. Biorąc to pod uwagę oraz dostrzegając skutki związane z oceną stopnia społecznej szkodliwości, należy stanąć na stanowisku, że za stosowaniem art. 250a § 3 kk będą mogły przemawiać okoliczności, w których korzyść majątkowa nie przekroczy kwoty 20 zł.

Prawnokarna ocena konkretnego zachowania na podstawie art. 250a § 3 kk będzie możliwa w odniesieniu do zachowań korupcyjnych, których treść nie wiąże się z wypełnieniem karty do głosowania, lecz z zastosowaniem określonej techniki (metody) głosowania. Czynnikiem przesądzającym o możliwości przyjęcia w tej sytuacji kwalifikacji czynu jako wypadku mniejszej wagi z art. 250 § 3 kk będzie treść „korupcyjnej umowy", która nie obejmuje tutaj merytorycznego sposobu zdeponowania głosu. W świetle przedstawionego stanowiska jako wypadek mniejszej wagi będzie mogło zostać zakwalifikowane zachowanie, które wiąże się z przyjęciem korzyści majątkowej lub osobistej za głosowanie przy udziale pełnomocnika lub też oddanie głosu w lokalu wyborczym wskazanym przez podmiot udzielający korzyści. Przedstawiony pogląd koresponduje z uwagami przedstawicieli doktryny prawa karnego dotyczącymi czynów korupcyjnych z art. 228 § 2 kk i art. 229 § 2 kk. Wskazuje się, że wśród okoliczności uzasadniających zakwalifikowanie czynu jako wypadku mniejszej wagi jest przyjęcie korzyści majątkowej za wykonanie czynności natury technicznej (np. za pomoc w przygotowaniu dokumentów czy w wypełnianiu wniosku)[23]. Jeżeli tego rodzaju czynności będą pozostawać w ścisłym związku ze sposobem głosowania (tzw. głosowaniem merytorycznym), to ich zwiększony ładunek karygodności będzie – co oczywiste – przemawiać przeciwko prawnokarnej kwalifikacji tych zachowań na podstawie art. 250a § 3 kk.

Równie ważną rolę w tego rodzaju ocenie będzie odgrywać specyfika sytuacji, w których stopień społecznej szkodliwości nie pozwoli na zastosowanie art. 250a § 3 kk, co tym samym będzie skutkować prawnokarną kwalifikacją danego czynu na podstawie art. 250a § 1 albo art. 250 § 2 kk. Wydaje się, że z tego typu sytuacją będziemy

[22] Zob. D. Wąsik, *Przestępstwa przeciwko wyborom i referendum – aspekty karnomaterialne, procesowe i kryminologiczne*, Olsztyn 2012, s. 216–223; tenże, *Sprawca korupcji wyborczej – studium kryminologiczne*, „Radca Prawny" 2011, nr 3, s. 73–80.

[23] J. Lachowski, w: *Kodeks karny. Część szczególna*…, s. 119–120. Zob. również: M. Surkont, *Łapownictwo*…, s. 65.

mieć do czynienia w przypadku zamachów korupcyjnych wymierzonych w głosowanie przez pełnomocnika. Należy bowiem zauważyć, że wskazana alternatywna metoda wyborcza opiera się na szczególnej więzi pełnomocnika z mocodawcą, a jej adresatem jest określona kategoria osób uprawnionych do głosowania (wyborcy niepełnosprawni oraz osoby w podeszłym wieku, tj. mające ukończone co najmniej 75 lat). Przeszkodą w prawnokarnej kwalifikacji tego typu zachowań na podstawie art. 250a § 3 kk będzie ich karygodność. Poza zamachami na dobro prawne podlegające ochronie na gruncie art. 250a kk godzą one również w szczególnego rodzaju instytucję prawną, jaką jest alternatywna procedura wyborcza. W tej sytuacji głosowanie w określony sposób będzie dotyczyć głosu osoby trzeciej – głosującej przez pełnomocnika. Przedstawione stanowisko znajduje oparcie w poglądach judykatury. Wskazuje się, że w przypadku, gdy (…) *czyn zabroniony stanowi zamach na dwa lub większą liczbę dóbr chronionych prawem, to zwiększa się jego stopień społecznej szkodliwości*[24].

Co do zasady przyjęcie wypadku mniejszej wagi nie powinno być możliwe w odniesieniu do „umów korupcyjnych" obejmujących kilka sposobów głosowania w ramach danych wyborów (np. głosowania na radnego gminy oraz wójta) bądź kilka rodzajów głosowań odbywających się w tym samym czasie (np. głosowania w ramach wyborów i referendum odbywających się w tym samym dniu). W tej sytuacji argumentem przeciwko prawnokarnej kwalifikacji danego zachowania na podstawie art. 250a § 3 kk również będzie karygodność tego typu zachowań, których skutki mogą obejmować kilka (niezależnych od siebie) rozstrzygnięć procedowanych w różnych głosowaniach.

Kontrowersje może wywoływać problem prawnokarnej oceny w kategoriach wypadku mniejszej wagi zachowań polegających na przyjęciu korzyści za głosowanie w sposób, który w rzeczywistości pozostaje w zgodzie z preferencjami danego wyborcy (tj. z wcześniej podjętą przez niego suwerenną decyzją wyborczą). W piśmiennictwie zwraca się uwagę, że niezwykle trudno jest wyobrazić sobie w pełni suwerenne głosowanie po otrzymaniu korzyści, ale jej przyjęcie po oddaniu głosu nie wydaje się już zachowaniem społecznie nagannym (np. wówczas, gdy sprawca oddaje głos na określoną osobę i kieruje się przy tym wyłącznie przekonaniem, że jest to właściwy kandydat, a później za taki sposób głosowania przyjmuje korzyść majątkową lub osobistą)[25]. Nie ulega wątpliwości, że w praktyce dowiedzenie tego, że głosowanie było wynikiem suwerennej decyzji osoby uprawnionej, a nie przyjętej przez niego korzyści, może być bardzo trudne, co wynika z obowiązywania zasady tajności głosowania. Przy dokonywaniu weryfikacji tych okoliczności organy ścigania nie powinny poprzestawać wyłącznie na wyjaśnieniach sprawcy, gdyż te mogą wynikać z przyjętej przez niego linii obrony. Nie ulega wątpliwości, że zarówno udzielanie, jak i przyjmowanie korzyści majątkowej lub osobistej za głosowanie w określony sposób, ale będący przejawem suwerennej decyzji wyborcy, cechuje się mniejszym ładunkiem społecznej szkodliwości

[24] Wyrok SN z 11 IV 2011 r., IV KK 382/10, „Prokuratura i Prawo" 2011, nr 10 – dodatek, poz. 5.

[25] J. Potulski, *Kodeks karny. Komentarz do zmian*…, Lex/el. 2004, komentarz do art. 250a kk, teza nr 5.

w porównaniu z sytuacją, w której wpływ na decyzję podjętą przez wyborcę miała przyjęta przez niego wcześniej korzyść.

W podobny sposób należy oceniać sytuacje, w których sprawca sprzedajności wyborczej przyjmie korzyść majątkową lub osobistą za głosowanie w określony sposób, ale ostatecznie decyduje się oddać głos w sposób odmienny od deklarowanego bądź też rezygnuje z udziału w głosowaniu. O ile w pierwszym przypadku obowiązywanie zasady tajności głosowania będzie poważnie utrudniać ustalenie sposobu głosowania, o tyle okoliczność wzięcia przez osobę uprawnioną czynnego udziału w wyborach lub referendum będzie możliwa do zweryfikowania, ze względu na to, że osoba uprawniona potwierdza własnoręcznym podpisem odbiór karty do głosowania.

Przeszkodą w przyjęciu kwalifikacji czynu jako wypadku mniejszej wagi może być dopuszczenie się przestępstwa sprzedajności bądź przekupstwa wyborczego przez osobę pełniącą funkcję związaną z zapewnieniem prawidłowego przebiegu procesu wyborczego lub referendalnego (np. męża zaufania, członka komisji wyborczej (referendalnej), komisarza wyborczego, międzynarodowego obserwatora wyborów). Wskazane okoliczności nie należą bowiem do faktorów stopnia społecznej szkodliwości (art. 115 § 2 kk). Jak zauważa Jacek Giezek, na ocenę stopnia społecznej szkodliwości nie mogą wpływać okoliczności, które mimo że dotyczą sprawcy, to jednak nie pozostają w związku z popełnionym przez niego czynem (np. wiek, stan zdrowia, sytuacja rodzinna i majątkowa, wykształcenie, zawód)[26]. Powyższy pogląd koresponduje ze stanowiskiem Sądu Najwyższego, który w postanowieniu z 4 marca 2009 r. wskazał, że: *Takie okoliczności jak warunki i właściwości osobiste sprawcy, właściwości osobiste pokrzywdzonego i procesowa postawa oskarżonego wobec postawionych mu w procesie zarzutów z pewnością nie mieszczą się w zamkniętym katalogu wymienionych w art. 115 §2 kk elementów wpływających na ocenę stopnia społecznej szkodliwości czynu*[27]. Nie ulega jednak wątpliwości, że wymienione czynniki mogą rzutować na wymiar kary (art. 53 kk).

Wydaje się, że przyjęcie kwalifikacji czynu jako wypadku mniejszej wagi przy przestępstwie przekupstwa wyborczego (art. 250a § 2 kk w związku z art. 250a § 3 kk) nie będzie możliwe w sytuacji, w której sprawca tego przestępstwa udziela korzyści majątkowej lub osobistej na żądanie osoby uprawnionej do głosownia. Warto zwrócić uwagę,

---

[26] J. Giezek, w: *Kodeks karny. Część ogólna. Komentarz*, J. Giezek (red.), Warszawa 2021, s. 876. Odmiennie: Wyrok SN z 21 I 1998 r., V KKN 39/97, „Prokuratura i Prawo" 1998, nr 6 – dodatek, poz. 1. Autor słusznie zauważa, że przywołany judykat został wydany jeszcze podczas obowiązywania Kodeksu karnego z 1969 r., w czasie *vacatio legis* Kodeksu karnego z 6 czerwca 1997 r.

[27] Uchwała SN z 16 IX 2008 r., SNO 68/08, Lex nr 491427. Zgodnie z poglądem SN wyrażonym w tej uchwale: „Niedopuszczalne jest uzależnianie oceny stopnia społecznej szkodliwości danego czynu od czynników bezpośrednio z nim niezwiązanych, które wystąpiły przed jego popełnieniem albo po jego popełnieniu (np. przyznanie się sprawcy do winy, dobrowolne naprawienie przez sprawcę szkody wyrządzonej przestępstwem, wyrażona przezeń skrucha, pogodzenie się z pokrzywdzonym), jak też od okoliczności charakteryzujących wyłącznie szeroko pojmowaną osobowość sprawcy, w szczególności tego, co w przepisach kodeksu określa się mianem „warunków i właściwości osobistych sprawcy" takich, jak np. wiek, stan zdrowia, sytuacja rodzinna i majątkowa, wykształcenie, zawód".

że na gruncie przestępstwa korupcji w sektorze publicznym (art. 228 § 2 kk) tego rodzaju okoliczności przemawiają za prawnokarną kwalifikacją danego zachowania w kategoriach wypadku mniejszej wagi. Jak wskazuje się w piśmiennictwie, w opisanej sytuacji udzielający korzyści znajduje się pod presją, co skutkuje tym, że jego czyn odznacza się niższym ładunkiem społecznej szkodliwości[28]. Nie odmawiając słuszności przedstawionemu poglądowi, należy zwrócić uwagę, że na gruncie korupcji wyborczej istnieje specyficzny układ penalny, który różni się od relacji zachodzących na tle innych czynów korupcyjnych i nie pozwala na zastosowanie art. 250a § 3 kk. Dochodzi tutaj bowiem do odwrócenia ról – podmiotem żądającym korzyści jest osoba uprawniona do głosowania (na gruncie art. 228 § 4 kk jest nim osoba pełniąca funkcję publiczną), która formułując żądanie, artykułuje tym samym propozycję sprzedaży swojego głosu. Nie sposób jednak przyjąć, że w obliczu tak przedstawianego żądania sprawca przekupstwa wyborczego znajduje się w sytuacji przymusowej, gdyż w praktyce wskazaną korzyść może z powodzeniem udzielić innej osobie mającej uprawnienia do głosowania. W przypadku wyborów powszechnych przeprowadzanych na podstawie Kodeksu wyborczego z 5 stycznia 2011 r. liczba osób uprawnionych do głosowania w zależności od rodzaju wyborów oscyluje w Rzeczpospolitej Polskiej wokół 30 mln[29]. Na tym tle odmiennie przedstawia się sytuacja sprawcy przestępstwa z art. 228 § 4 kk, który ze względu na pełnienie funkcji publicznej najczęściej będzie jedynym podmiotem właściwym i kompetentnym do załatwienia określonej sprawy.

Na uwagę zasługuje to, że głównym motywem wyodrębnienia wypadku mniejszej wagi przy przestępstwie korupcji wyborczej, podobnie jak w przypadku innych czynów korupcyjnych wprowadzonych do Kodeksu karnego z 1997 r. przez nowelę antykorupcyjną z 13 czerwca 2003 r., w opinii osób uczestniczących w pracach legislacyjnych, była potrzeba dostosowania ustawowego zagrożenia karą do wszystkich zachowań podlegających kryminalizacji, tj. tych o największym ciężarze gatunkowym, tych „standardowych" i tych najdrobniejszych, których prawnokarna ocena powoduje najwięcej problemów praktycznych. W obrębie tej trzeciej grupy znajdują się bowiem takie zachowania, których ciężar gatunkowy nie koresponduje z dolną granicą sankcji, co prowadzi do nadużywania instytucji nadzwyczajnego złagodzenia kary, a nawet do umarzania postępowania karnego ze względu na znikomy stopień społecznej szkodliwości czynu[30].

---

[28] J. Lachowski, w: *Kodeks karny. Część szczególna*…, s. 137; A. Spotowski, *Przestępstwa służbowe: nadużycie służbowe i łapownictwo w nowym kodeksie karnym*, Warszawa 1972, s. 113; M. Surkont, *Łapownictwo*…, s. 89.

[29] W przypadku wyborów na urząd Prezydenta RP, które odbyły się 12 VII 2020 r., liczba osób uprawnionych do głosowania wynosiła 29 147 064. Zob. *Komunikat Państwowej Komisji Wyborczej z dnia 12 lipca 2020 r. o liczbie osób ujętych w spisach wyborców oraz liczbie wyborców, którym wydano karty do głosowania do godz. 12:00 w ponownym głosowaniu w wyborach Prezydenta Rzeczypospolitej Polskiej w dniu 12 lipca 2020 r.*, https://pkw.gov.pl/uploaded_files/1594594571_komunikat-dot-frekwencji-na-godz-1200-12072020.pdf [dostęp: 12 XII 2020].

[30] B. Mik, *Nowela antykorupcyjna z dnia 13 czerwca 2003 r. Rys historyczny i podstawowe problemy interpretacyjne*, Kraków 2003, s. 150–151.

Jak już wcześniej wskazano, wyodrębnienie typu uprzywilejowanego z art. 250a § 3 kk spotkało się z krytyką przedstawicieli doktryny prawa karnego. Zdaniem Jacka Sobczaka w przypadku przestępstwa korupcji wyborczej sprawca godzi w bardzo istotne dobra chronione prawem, co wydaje się okolicznością podważającą zasadność normatywnego wyodrębnienia wypadku mniejszej wagi[31]. Podjęcie decyzji o rezygnacji z wypadku mniejszej wagi (art. 250a § 3 kk) wydaje się zasadne również z uwagi na ograniczone możliwości stosowania tej regulacji wobec sprawców przestępstwa przekupstwa wyborczego. Istota tej postaci korupcji wyborczej bardzo często zasadza się na wielokrotnej realizacji jego znamion przez jednego sprawcę w trakcie tych samych wyborów i referendum. W tej sytuacji najczęściej znajdzie zastosowanie konstrukcja czynu ciągłego, co też będzie wykluczać możliwość skorzystania z instytucji wypadku mniejszej wagi. Należy w tym miejscu zgodzić się z Mikołajem Iwańskim, który trafnie wskazuje, że popełnienie przestępstwa przekupstwa wyborczego w formie czynu ciągłego, z uwagi na skutki wynikające z tego zachowania (m.in. możliwość wypaczenia rezultatu głosowania w wyborach lub referendum), nie będzie pozwalać na przyjęcie kwalifikacji czynu jako wypadku mniejszej wagi[32].

Trzeba mieć na uwadze, że społeczna szkodliwość czynów spełniających kryteria wypadku mniejszej wagi musi plasować się powyżej minimalnej, ujemnej zawartości, przekraczać swoim zakresem poziom znikomości, ale nie osiągać pułapu właściwego typom podstawowym z art. 250a § 1–2 kk. W praktyce uchwycenie tak wąsko wyznaczonej granicy może okazać się bardzo trudne. Warto zaznaczyć, że na gruncie przestępstwa korupcji wyborczej brak jest typów kwalifikowanych, a różnice w zakresie zagrożenia karnego pomiędzy typami podstawowymi z art. 250a § 1–2 kk (kara od 3 miesięcy do 5 lat pozbawienia wolności) a uprzywilejowanymi z art. 250a § 3 kk (grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat 2) nie są znaczne, jak to jest np. w przypadku przestępstwa korupcji w sektorze publicznym. Na gruncie wskazanego przestępstwa relacje pomiędzy typem podstawowym (kara od 6 miesięcy do 8 lat) a uprzywilejowanym (kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2) oraz kwalifikowanym (kara pozbawienia wolności od roku do lat 10) zostały ukształtowane w sposób zdecydowanie bardziej wyraźny.

Argumentów przemawiających za rezygnacją z utrzymywania instytucji wypadku mniejszej wagi (art. 250a § 3 kk) można również poszukiwać w obowiązujących regulacjach dotyczących wymiaru kary. W przyjętym kształcie nie różnicują one sytuacji sprawców typów podstawowych (art. 250a § 1–2 kk) oraz uprzywilejowanych (art. 250a § 3 kk). O ile bowiem typy przestępstw z art. 250a § 1–2 kk zostały zagrożone karą pozbawienia wolności od 3 miesięcy do lat 5, to przyjęcie wypadku mniejszej wagi implikuje możliwość orzeczenia wobec sprawcy kary grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Występujące na tym tle różnice będę jednak mieć w dużej mierze wymiar teoretyczny, gdyż wymierzenie kary grzywny wobec

[31] J. Sobczak, *Przestępstwo korupcji wyborczej*…, s. 115.

[32] Por. M. Iwański, *Odpowiedzialność karna*…, s. 645–646.

sprawców przestępstw z art. 250a § 1–2 kk nie tylko będzie możliwe, lecz w praktyce może dotyczyć dość częstych sytuacji. Za słusznością powyższego poglądu przemawia treść art. 58 § 1 kk, zgodnie z którym: (…) *jeżeli ustawa przewiduje możliwość wyboru rodzaju kary, a przestępstwo jest zagrożone karą pozbawienia wolności nieprzekraczającą 5 lat, sąd orzeka karę pozbawienia wolności tylko wtedy, gdy inna kara lub środek karny nie może spełnić celów kary*.

Przeprowadzone rozważania wiodą do wniosku, że decyzja legislacyjna polegająca na ustanowieniu wypadku mniejszej wagi w obrębie przestępstwa korupcji wyborczej (art. 250a § 3 kk) nie była trafna i została podjęta zbyt pochopnie. Ustawodawca, ustanawiając art. 250a § 3 kk, całkowicie rozminął się z intencjami, jakimi kierował się podczas tworzenia analizowanej regulacji. Wbrew pozorom praktyka stosowania art. 250a § 3 kk nie dostarcza zbyt wielu argumentów przemawiających za potrzebą utrzymywania tej regulacji w Kodeksie karnym. Wyodrębnienie art. 250a § 3 kk, wbrew intencjom ustawodawcy, nie tylko nie ułatwiło, lecz wręcz przeciwnie – skomplikowało dokonywanie prawnokarnej oceny zachowań korupcyjnych związanych z wyborami i spowodowało wymierne trudności interpretacyjne. Należy zauważyć, że art. 250a § 3 kk nie koresponduje również z charakterem korupcji wyborczej, która w odróżnieniu od innych zachowań korupcyjnych ma w dużej mierze charakter incydentalny, tj. występuje niemal wyłącznie w okresie przeprowadzania wyborów i referendów.

Bibliografia

Iwański M., *Odpowiedzialność karna za przestępstwa korupcyjne*, Kraków 2016, Krakowski Instytut Prawa Karnego Fundacja.

Jurewicz J., *Przestępstwa przeciwko wyborom i referendum z rozdziału XXXI*, „Studia Wyborcze" 2006, t. 2, s. 35–36.

Kodeks karny. Część ogólna. Komentarz, J. Giezek (red.), Warszawa 2021, Wolters Kluwer Polska.

Kodeks karny. Część ogólna, tom I. Komentarz do art. 53–116, W. Wróbel, A. Zoll (red.), Warszawa 2016, Wolters Kluwer Polska.

Kodeks karny. Część szczególna, tom II. Komentarz. Art. 222–316, M. Królikowski, R. Zawłocki (red.), Warszawa 2017, C.H. Beck.

Kodeks karny. Komentarz, A. Grześkowiak, K. Wiak (red.), Warszawa 2021, C.H. Beck.

Kodeks karny. Komentarz, M. Filar (red.), Warszawa 2016, Wolters Kluwer Polska.

Kodeks karny. Komentarz, M. Mozgawa (red.), Warszawa 2017, Wolters Kluwer Polska.

Kodeks karny. Komentarz, R. Stefański (red.), Warszawa 2020, C.H. Beck.

Marek A., *Kodeks karny. Komentarz*, Warszawa 2010, Wolters Kluwer Polska.

Mik B., *Nowela antykorupcyjna z dnia 13 czerwca 2003 r. Rys historyczny i podstawowe problemy interpretacyjne*, Kraków 2003, Kantor Wydawniczy Zakamycze.

Potulski J., *Kodeks karny. Komentarz do zmian wprowadzonych ustawą z dnia 13 czerwca 2003 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U.03.111.1061)*, Lex/el 2004, art. 250a kk, teza nr 8.

Projekt kodeksu karnego oraz przepisów wprowadzających kodeks karny, Warszawa 1968, Wydawnictwo Prawnicze.

Rulka M., *Referendum w sprawie organizacji przez Kraków Zimowych Igrzysk Olimpijskich w 2022 r.*, „Samorząd Terytorialny" 2015, nr 5, s. 56–66.

Skorupka J., *Przestępstwo korupcji wyborczej z art. 250a kk*, „Palestra" 2006, nr 11–12, s. 43–53.

Sobczak J., *Przestępstwo korupcji wyborczej*, w: *Przemiany prawa wyborczego – doświadczenia nowych demokracji*, A. Sokala, Z. Witkowski (red.), Bydgoszcz 2007, Wydawnictwo Kujawsko-Pomorskiej Szkoły Wyższej, s. 106–116.

Spotowski A., *Przestępstwa służbowe: nadużycie służbowe i łapownictwo w nowym kodeksie karnym*, Warszawa 1972, Wydawnictwo Prawnicze.

Stefański R.A., *Przestępstwo korupcji wyborczej (art. 250a kk)*, „Prokuratura i Prawo" 2004, nr 4, s. 68–79.

Surkont M., *Łapownictwo*, Sopot 1999, Wydawnictwo Prawnicze LEX.

Wąsik D., *Przestępstwa przeciwko wyborom i referendum – aspekty karnomaterialne, procesowe i kryminologiczne*, Olsztyn 2012, Wydawnictwo Volumina.pl.

Wąsik D., *Sprawca korupcji wyborczej – studium kryminologiczne*, „Radca Prawny" 2011, nr 3, s. 73–82.

Żurowska R., *Przestępstwo korupcji w sporcie*, Poznań 2010, Wydawnictwo Poznańskie.

Źródła internetowe

Komunikat Państwowej Komisji Wyborczej z dnia 12 lipca 2020 r. o liczbie osób ujętych w spisach wyborców oraz liczbie wyborców, którym wydano karty do głosowania do godz. 12:00 w ponownym głosowaniu w wyborach Prezydenta Rzeczypospolitej Polskiej w dniu 12 lipca 2020 r., https://pkw.gov.pl/uploaded_files/1594594571_komunikat-dot-frekwencji-na-godz-1200-12072020.pdf [dostęp: 12 XII 2020].

Referendum lokalne. Niedziela 25 maja 2014 r., https://www.bip.krakow.pl/?dok_id=60751 [dostęp: 29 VII 2017].

Akty prawne

Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (t.j.: DzU z 2020 r. poz. 1319).

Ustawa z dnia 13 czerwca 2003 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU z 2003 r. nr 111 poz. 1061).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (DzU z 1997 r. nr 88 poz. 553, ze zm.).

Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny (DzU z 1969 r. nr 13 poz. 94).

Rozporządzenie Prezydenta Rzeczypospolitej z 11 lipca 1932 r. – Kodeks karny (DzU z 1932 r. nr 60 poz. 571).

Orzecznictwo

Wyrok Sądu Najwyższego z 11 IV 2011 r., IV KK 382/10, „Prokuratura i Prawo" 2011, nr 10 – dodatek, poz. 5.

Uchwała Sądu Najwyższego z 16 IX 2008 r., SNO 68/08, Lex nr 491427.

Wyrok Sądu Najwyższego z 21 I 1998 r., V KKN 39/97, „Prokuratura i Prawo" 1998, nr 6 – dodatek, poz. 1.

Wyrok Sądu Najwyższego z 15 XI 1984 r., II KR 248/84, OSNKW 1985, nr 7–8, poz. 61.

Wyrok Sądu Najwyższego z 25 X 1984 r., V KRN 336/84, OSNPG 1985, nr 5, poz. 66.

Wyrok Sądu Najwyższego z 8 III 1983 r., I KR 387/82, Lex nr 21972.

Wyrok Sądu Najwyższego z 8 III 1972 r., II KR 329/71, Lex nr 21470.

Abstrakt

Artykuł jest poświęcony problematyce typu uprzywilejowanego przestępstwa korupcji wyborczej. Autor omawia przykłady zachowań umożliwiających prawnokarną kwalifikację na podstawie art. 250a § 3 kk, a także sytuacje niepozwalające na zastosowanie tej regulacji. Przeprowadza również rozważania dotyczące zasadności wyodrębnienia wypadku mniejszej wagi w normatywnej konstrukcji przestępstwa korupcji wyborczej, jak też postulowanych w tym zakresie zmian legislacyjnych.

Słowa kluczowe: wypadek mniejszej wagi, sprzedajność wyborcza, przekupstwo wyborcze, nowela antykorupcyjna, typy korupcji wyborczej.

Mitigated forms of election corruption crimes

Abstract

The article examines the problem of the type of mitigated crime of electoral corruption. The author discusses examples of behaviour enabling criminal qualification under Art. 250a § 3 of the Penal Code, as well as situations that do not allow the application of this regulation. He also considers the legitimacy of isolating a minor accident in the normative structure of the election corruption crime, as well as the proposed legislative changes in this regard.

Keywords: minor accident, electoral venality, electoral bribery, anti-corruption amendment, types of electoral corruption.

IZABELA DĄBROWSKA
ORCID: 0000-0001-7351-7607

DOI: 10.4467/20801335PBW.21.031.14308

Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika[1]

Zapewnienie bezpieczeństwa narodowego oraz skutecznego funkcjonowania systemu obronnego państwa wymaga posiadania wiedzy na temat metod działania potencjalnych przeciwników, w tym sposobów maskowania prowadzonych przez nich działań. Uwarunkowania historyczne oraz położenie geostrategiczne Polski jako państwa będącego wschodnią granicą Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego (NATO) sprawiają, że Siły Zbrojne Rzeczypospolitej Polskiej (SZ RP) oraz wszelkie podmioty zaangażowane w zapewnianie bezpieczeństwa państwa powinny mieć niezbędne informacje o sposobach działania państw graniczących z naszym krajem, zwłaszcza tych leżących po stronie wschodniej. Jednym z nich jest Federacja Rosyjska (FR), której doktryna maskowania działań, zwana maskirowką, ma najdłuższe tradycje oraz jest jedną z najbardziej skutecznych na świecie.

Maskowanie zaistniało niemal równocześnie z pojawieniem się walki zbrojnej. Kamuflaż, mylenie przeciwnika czy pozorowanie to czynniki mające wpływ na osiąganie przewagi na polu walki i w konsekwencji decydujące o zwycięstwie. W *Słowniku języka polskiego* pojęcie „maskowanie" definiuje się jako „uczynienie czegoś lub kogoś niewidocznym", a także jako „ukrycie rzeczywistych zamiarów, uczuć, nastrojów"[2]. W SZ RP maskowanie w kontekście militarnym zostało opisane w doktrynie *Maskowanie operacyjne: DD-3.31(A)* jako zespół przedsięwzięć, których celem jest oddziaływanie na proces decyzyjny przeciwnika, zwłaszcza jego zakłócanie. Do tych przedsięwzięć zaliczamy ukrywanie wojsk oraz infrastruktury obronnej przed rozpoznaniem

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika* (Akademia Sztuki Wojennej, Wydział Wojskowy). Autorka wykorzystała rozdziały: I, II oraz III.

[2] Zob. *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/maskowac;2481616.html [dostęp: 9 X 2019].

strony przeciwnej, a także działalność dezinformacyjną dotyczącą dyslokacji wojsk oraz celów prowadzonych działań. W SZ RP maskowanie jest dzielone w zależności od poziomu dowodzenia na: strategiczne, operacyjne oraz taktyczne (nazywane również maskowaniem bezpośrednim)[3].

Charakterystyka maskowania operacyjnego w Siłach Zbrojnych Federacji Rosyjskiej

W Siłach Zbrojnych Federacji Rosyjskiej (SZ FR) maskowanie operacyjne jest nazywane **maskirowką**[4] (ros. *маскировка*). Zdefiniowano je jako kompleksowe działania mające na celu ukrycie żołnierzy i obiektów przed przeciwnikiem, a także wprowadzanie go w błąd co do obecności, dyslokacji, stanu, składu wojsk, podejmowanych przez nie działań oraz zamiarów żołnierzy. Maskirowkę uznaje się za jeden z głównych rodzajów wsparcia działań militarnych. Obejmuje ona wszelkie sposoby mające na celu zabezpieczenie zarówno operacji wojennych, jak i codziennych aktywności wojska. Dzięki niej jest możliwe uzyskanie efektu zaskoczenia, zachowanie zdolności bojowej wojsk oraz zwiększenie ich żywotności. Maskowanie jest realizowane na wszystkich szczeblach dowodzenia, zarówno podczas przygotowań, jak i prowadzenia działań wojennych oraz ćwiczeń wojskowych, a także w czasie dowodzenia działaniami specjalnymi. Zadaniami z zakresu maskirowki są objęte również oddziały o stałej gotowości bojowej i oddziały pełniące obowiązki bojowe[5]. Maskowanie operacyjne dotyczy: personelu, wyposażenia i uzbrojenia oddziałów, fortyfikacji, pozycji oddziałów, stanowisk dowodzenia, zapór, przepraw, lotnisk, rurociągów, miejsc przechowywania zapasów środków materiałowych oraz innych obiektów, w tym m.in. ważnych zabytków, które znajdują się na maskowanym terenie[6].

Maskirowka opiera się na pięciu głównych zasadach, wskazujących warunki, które powinny być spełnione, aby maskowanie było skuteczne[7]:

1) **aktywność** (ros. *активность*) – polega na stałym narzucaniu przeciwnikowi fałszywych wizji dotyczących zamiarów dowódców, stanu, lokalizacji oraz działalności wojsk oraz obiektów;
2) **realistyczność** (ros. *убедительность*) – podejmowane działania powinny sprawiać wrażenie wiarygodnych, być dopasowane do warunków otoczenia oraz uwzględniać możliwości oddziałów rozpoznawczych przeciwnika;

---

[3] *Maskowanie operacyjne: DD-3.31(A)*, Bydgoszcz 2018, s. 13.

[4] Wszystkie wyróżnienia w tekście pochodzą od autorki (przyp. red.).

[5] Zob. А.Ю. Королёв, А.А. Королёва, А.Д. Яковлев, *Маскировка. Вооружения, техники и объектов*, Санкт-Петербург 2015, s. 6.

[6] Por. *Классификация и способы маскировки*, http://red-tent.ru/mask/maskirovka [dostęp: 31 X 2019].

[7] Zob. А.Ю. Королёв, А.А.Королёва, А.Д. Яковлев, *Маскировка. Вооружения*…, s. 8.

3) **ciągłość** (ros. *непрерывность*) – maskowanie powinno być prowadzone stale, w każdej sytuacji, tj. w czasie ćwiczeń wojskowych, działań bojowych, zmiany dyslokacji wojsk czy obsługi obiektów;
4) **różnorodność** (ros. *разнообразность*) – przy wykonywaniu zadań z zakresu maskowania należy unikać trzymania się wzorców, stosować nowoczesne środki i techniki kamuflażu;
5) **kompleksowość** (ros. *комплексность*) – należy jednocześnie wykorzystywać różnorodne środki maskowania, które będą w stanie zmylić środki rozpoznawcze przeciwnika[8].

Wyróżnia się cztery główne sposoby prowadzenia maskirowki. Są to: ukrycie, imitacja, działania demonstracyjne oraz dezinformacja[9].

1) **ukrycie** (ros. *скрытие*) – polega na upodabnianiu maskowanego obiektu do otaczającego go tła i warunków terenowych zgodnie z zasadami i sztuką maskowania. Skuteczne ukrycie wymaga stałego przestrzegania dyscypliny maskowania przez oddziały i pododdziały, zarówno w czasie prowadzenia działań, jak i odpoczynku w rejonach ześrodkowania. Ma ono zapobiegać wykrywaniu wojsk i obiektów, a także służyć eliminowaniu cech charakterystycznych, które mogą je zdemaskować[10].
2) **imitacja (pozorowanie)** (ros. *имитация*) – polega na tworzeniu fałszywych obszarów dyslokacji i ruchu wojsk oraz makiet uzbrojenia i sprzętu wojskowego w celu zwrócenia uwagi przeciwnika na obiekty pozorne. Warunkiem skuteczności imitacji jest maskowanie ich dokładnie w taki sam sposób jak prawdziwego sprzętu. Zakłada się, że przy maskowaniu obiektów pozornych powinno się celowo popełnić błędy umożliwiające przeciwnikowi rozpoznanie tych obiektów, jednak należy to zrobić w taki sposób, aby nie wzbudzić jego podejrzeń[11].
3) **działania demonstracyjne** (ros. *демонстративные действия*) – polegają na wykonywaniu pozornych ruchów wojsk i realizowaniu innych przedsięwzięć w celu zmylenia przeciwnika co do dyslokacji i rzeczywistych działań wojsk i ich zamiarów.
4) **dezinformacja** (ros. *дезинформация*) – jest to celowe opracowywanie i przekazywanie przeciwnikowi fałszywych lub częściowo fałszywych informacji

[8] Zastosowanie wszystkich wyżej wymienionych zasad jest warunkiem skuteczności maskowania. Aby zwiększyć prawdopodobieństwo uzyskania dobrych wyników, pod uwagę bierze się również ilość sił i środków, które zostają przeznaczone do realizacji zadań z zakresu maskowania, zgodność zastosowanych środków kamuflażu z zadaniami wykonywanymi aktualnie przez żołnierzy oraz ich realistyczność. Ogromne znaczenie mają również stałe monitorowanie jakości wykorzystywanych środków oraz terminowa realizacja zadań.

[9] Por. А.Ю. Королёв, А.А.Королёва, А.Д. Яковлев, *Маскировка. Вооружения*…, s. 7.

[10] Zob. *Маскировка,* https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=13494 [dostęp: 30 X 2019].

[11] *Maskowanie wojsk i wojskowej infrastruktury obronnej – DD-3.20*, Warszawa 2010, s. 10.

dotyczących stanu wojsk i ich zamiarów. Są one rozpowszechniane z wykorzystaniem różnych środków i kanałów, m.in. za pomocą technicznych środków komunikacji i środków masowego przekazu, jak również przekazywane agentom wywiadu lub komórkom rozpoznawczym przeciwnika.

Warto w tym miejscu zaznaczyć, że zadania z zakresu ukrywania są realizowane przez wszystkie pododdziały, oddziały i jednostki wojskowe, bez konieczności wydawania specjalnych rozkazów czy instrukcji. Natomiast zadania z zakresu imitacji, działań demonstracyjnych oraz dezinformacji są przeprowadzane na rozkaz i pod nadzorem dowódcy.

W rosyjskiej armii istnieje również podział na maskowanie naturalne i sztuczne.

Maskowanie naturalne – polega na ukrywaniu przedmiotów i obiektów dzięki dostosowywaniu ich do otaczającego je terenu. Wykorzystuje się właściwości maskujące m.in. lasów, gajów, wąwozów; panujące warunki oświetleniowe, w tym zmrok, cienie rzucane przez lokalne obiekty; warunki atmosferyczne, np. deszcz, mgłę, opady śniegu. Celem jest ograniczenie widoczności przedmiotów, obiektów oraz działań wojskowych i zmniejszenie ryzyka ich zaobserwowania przez przeciwnika.

Maskowanie sztuczne – wykorzystuje środki techniczne i polega na tworzeniu sztucznych obiektów i makiet, malowaniu maskującym, upodobniającym przedmioty i obiekty do otaczającego je tła, ustawianiu zasłon dymnych, tworzeniu systemów maskowania radiolokacyjnego i obrazowego. Do maskowania sztucznego zalicza się także maskowanie radiowe, świetlne i akustyczne[12].

Ponadto istnieje podział maskowania ze względu na rodzaj środków rozpoznawczych stosowanych przez przeciwnika. Wyróżnia się m.in.[13]:

- maskowanie optyczne,
- maskowanie termiczne,
- maskowanie radiolokacyjne,
- maskowanie radiotechniczne,
- maskowanie akustyczne,
- maskowanie hydroakustyczne.

Maskowanie optyczne (ros. *оптическая маскировка*) – ma przeciwdziałać fotografowaniu, nagrywaniu oraz obserwacji wizualnej (również przy użyciu przyrządów elektrooptycznych). Wykorzystuje się w nim maskujące właściwości terenu, warunki ograniczonej widoczności, dostępne materiały i sprzęty do kamuflażu, w tym występujące lokalnie, malowanie maskujące. Stosowane są również makiety sprzętu, fałszywe konstrukcje oraz inne środki imitacji.

Maskowanie termiczne (ros. *тепловая маскировка*) – ma na celu zapobieganie wykrywaniu żołnierzy i sprzętu za pomocą urządzeń termowizyjnych. Wykorzystuje się maskujące właściwości terenu, osłania rozgrzane powierzchnie sprzętu wojskowego

[12] Zob. С. Монетчиков, *Маскировка. Искусство быть невидимым*, 8 VI 2013 r., https://topwar.ru/30425-maskirovka-iskusstvo-byt-nevidimym.html [dostęp: 23 X 2019].

[13] Por. *Классификация и способы маскировки*…

(zwłaszcza pojazdów) specjalnymi pokryciami deformującymi zobrazowanie termalne obiektu i zmniejszającymi różnicę temperatur pomiędzy maskowanym obiektem a otaczającym go tłem. Stosuje się także fałszywe cele termiczne.

Maskowanie radiolokacyjne (ros. *радиолокационная маскировка*) – ma na celu eliminację, zmniejszenie skuteczności lub zniekształcenie rozpoznania radiolokacyjnego przeciwnika. Wykorzystuje się w nim środki odbijające fale radiowe, ekrany chroniące przed falami radiowymi, a także tworzy fałszywe cele dla przeciwnika.

Maskowanie radiotechniczne (ros. *радиотехническая маскировка*) – jest sposobem przeciwdziałania rozpoznaniu radiotechnicznemu przeciwnika. Tego rodzaju maskowanie polega na wprowadzeniu zakazu lub ograniczeń użytkowania sprzętu radiowego i elektronicznego, zmniejszeniu mocy promieniowania stacji radiowych, nadawaniu krótkich lub fałszywych sygnałów.

Maskowanie akustyczne (ros. *бвуковая маскировка*) – ma za zadanie przeciwdziałać podsłuchowi. Aby zmylić przeciwnika, redukuje się hałas generowany przez sprzęt wojskowy, tłumi dźwięki za pomocą kurtyn powietrznych, a także generuje fałszywy hałas wywoływany przez sprzęt wojskowy, strzały, wybuchy.

Maskowanie hydroakustyczne (ros. *гидроакустическая маскировка*) – jest sposobem przeciwdziałania akustycznym środkom rozpoznawczym przeciwnika znajdującym się na okrętach podwodnych. Wykorzystuje się urządzenia dźwiękoszczelne i pochłaniające dźwięki, chroni okręty podwodne pod kanałami dźwiękowymi, wyłącza głośne mechanizmy pomocnicze. W celu rozproszenia uwagi przeciwnika oraz skierowania go w fałszywym kierunku stosuje się również urządzenia samobieżne i zużyte sprzęty, które mają akustycznie imitować okręty podwodne.

Formy i metody maskirowki są dobierane adekwatnie do wymogów aktualnej sytuacji, charakteru planowanych i realizowanych działań oraz zależą od poziomu prowadzenia maskowania. Inne formy i metody będą wykorzystywane na poziomie taktycznym, na którym głównym celem będzie ukrycie pojedynczych żołnierzy i sprzętu wojskowego, a inne na poziomie operacyjnym, na którym celem będzie zachowanie tajności planowanej operacji. Istotnymi czynnikami branymi pod uwagę są również specyfika działań oraz rodzaj użytych sił i środków. Dzięki właściwemu zaplanowaniu i zorganizowaniu, a także konsekwentnej realizacji przedsięwzięć z zakresu maskowania osiąga się pożądany poziom ochrony wojsk oraz redukuje zagrożenia wywołane oddziaływaniami przeciwnika. Stosując maskirowkę, dąży się do stworzenia fałszywego obrazu rzeczywistości w celu ukrycia prawdy przed docelowymi odbiorcami. Ten obraz, niezależnie od tego, czy pozorny, czy mający mało istotne znaczenie, ma za zadanie odwrócić uwagę przeciwnika od ważnych informacji. Maskowanie ma także na celu zmuszenie przeciwnika do popełnienia błędów, których w innych warunkach by nie popełnił, oraz sprowokowanie go do podjęcia niekorzystnych dla niego działań. Szczegółowe cele maskowania są dostosowywane do charakteru i specyfiki konkretnej sytuacji taktycznej, planowanej operacji oraz zamiarów dowódców.

Zadania maskowania określają sposób, w jaki będą realizowane zaplanowane przedsięwzięcia. Rodzaj oraz zakres tych zadań zależą od wielu czynników. Są to m.in.: aktualna sytuacja operacyjna, czas przeznaczony na realizację działań z zakresu maskowania, ich charakter, szczebel realizacji przedsięwzięć, a także cechy demaskujące wojska, ukształtowanie terenu, warunki atmosferyczne, sposoby oraz intensywność działalności rozpoznawczej przeciwnika, ilość sił i środków, które mogą zostać wykorzystane do realizacji tych zadań[14].

Do głównych zadań maskirowki na poziomie operacyjnym zalicza się[15]:

- ochronę informacji stanowiących tajemnicę państwową;
- rozmieszczanie i przemieszczanie wojsk i obiektów w sposób tajny, z wykorzystaniem maskujących właściwości terenu i warunków ograniczonej widoczności;
- wykorzystanie przez wojska środków maskujących – tj. materiałów występujących w danym środowisku oraz zasłon dymnych;
- malowanie maskujące uzbrojenia, sprzętu wojskowego i obiektów;
- wykonywanie działań demonstracyjnych;
- tworzenie pozornych obszarów lokalizacji wojsk, pozycji i obiektów;
- stosowanie innych środków i metod kamuflażu przeciwdziałających wszelkim rodzajom rozpoznania przeciwnika;
- ścisłe przestrzeganie zasad i sztuki maskowania[16].

Szczegółowe zadania z zakresu maskowania operacyjnego zostały podzielone na trzy grupy (zob. tabela). Obejmują one działania:

1) organizacyjne,
2) inżynieryjne,
3) techniczne.

[14] *Maskowanie operacyjne: DD-3.31(A)…*, s. 19.

[15] А.Ю. Королёв, А.А. Королёва, А.Д. Яковлев, *Маскировка. Вооружения…*, s. 6.

[16] Zadania będą podlegać ciągłym modyfikacjom ze względu na zmiany zachodzce w środowisku walki zbrojnej oraz zmianę charakteru przyszłych wojen. Wprowadzanie nowych środków walki, organizacji i struktur wojsk, nowoczesnych wielozakresowych systemów maskujących, nowych pokryć maskujących i technik kamuflażu będzie miało duży wpływ na dobór zadań maskowania, a także przyczyni się do powstania nowych środków maskujących.

Tabela. Szczegółowe zadania z zakresu maskowania operacyjnego.

Działania organizacyjne	Działania inżynieryjne	Działania techniczne
– stałe zarządzanie maskowaniem oraz systematyczna kontrola jego aktualności i jakości; – wykorzystywanie maskujących właściwości terenu, dzięki którym można ukryć lub zmniejszyć widoczność sprzętu wojskowego i żołnierzy; – wykorzystywanie warunków ograniczonej widoczności (np. mgły, opadów, zachmurzenia, nocy) w celu przemieszczenia wojsk; – rozśrodkowanie wojsk oraz czasowe zmiany ich dyslokacji; – działania demonstracyjne; – ochrona informacji stanowiących tajemnicę państwową; – ścisłe przestrzeganie zasad i sztuki maskowania	– malowanie maskujące; – stosowanie systemów maskowania optycznego, termicznego i radiolokacyjnego; – stosowanie metod ukrywania i imitacji znaków demaskujących; – maskowanie dźwiękowe; – wykorzystywanie makiet i konstruowanie obiektów pozonych; – wykorzystywanie występującej roślinności i właściwości terenu; – nadawanie przedmiotom i obiektom maskujących form, dzięki którym zostaną upodobnione do lokalnych przedmiotów i obiektów	– stosowanie zasłon dymnych, materiałów pirotechnicznych i innych środków

Źródło: Opracowanie własne na podstawie: А.Ю. Королёв, А.А. Королёва, А.Д. Яковлев, *Маскировка. Вооружения, техники и объектов*, Санкт-Петербург 2015, s. 8–9.

Maskirowka jest realizowana na wszystkich poziomach działań zbrojnych[17]:

- strategicznym,
- operacyjnym,
- taktycznym.

Maskowanie na poziomie strategicznym służy ukryciu przygotowań do operacji strategicznej, kampanii i obejmuje działania dezinformacyjne dotyczące przegrupowywania sił zbrojnych, ich stanu i zamiarów oraz stanu obiektów o znaczeniu strategicznym (w tym ich zabezpieczenia). Zadaniem maskirowki strategicznej jest także wprowadzenie przeciwnika w błąd co do intencji i decyzji przywódców polityczno-wojskowych oraz ich planów strategicznych. Maskowanie na tym poziomie obejmuje posługiwanie się strategicznymi środkami kamuflażu i dezinformacji w celu zachowania tajemnic państwowych i wojskowych, zneutralizowania działań wywiadu wojskowego przeciwnika, w tym stosowanych przez niego technicznych środków rozpoznania. Wykorzystuje się do tego m.in. państwowy system informacyjny (np. prasę, radio, telewizję) oraz kanały dyplomatyczne. W celu zwiększenia skuteczności działań stosuje się fałszywe „wycieki" informacji oraz działania demonstracyjne. Maskirowka na poziomie strategicznym jest

[17] Por. А.Ю. Королёв, А.А. Королёва, А.Д. Яковлев, *Маскировка. Вооружения*…, s. 8.

przeprowadzana na podstawie decyzji Naczelnego Dowódcy SZ FR. Jej planowaniem i organizacją zajmuje się Sztab Generalny SZ FR[18].

Współcześnie maskirowka na poziomie strategicznym jest widoczna także w działaniach państwa w czasach pokoju. Jej przejawami są m.in.: zatajanie podejmowanych decyzji politycznych, unikanie mówienia o kwestiach istotnych dla społeczeństwa, realizowanie działań dezinformacyjnych i propagandowych – zarówno na arenie międzynarodowej, jak i wewnątrz kraju. Maskowanie nie jest więc ukierunkowane jedynie na przeciwnika zewnętrznego. Coraz częściej wykorzystuje się je przeciwko własnemu społeczeństwu w celu ukształtowania takiej opinii publicznej, która stanie się jednym z filarów polityki państwa[19]. W ostatnich latach maskirowkę strategiczną uznaje się za integralną część koncepcji wojny informacyjnej[20].

Maskowanie na poziomie operacyjnym ma zapewniać tajność przygotowywanym operacjom, aby uzyskać efekt zaskoczenia oraz zapewnić odpowiednią żywotność wojsk. Ten rodzaj maskowania obejmuje działania demonstracyjne, pozorowane skoncentrowanie lub rozśrodkowanie wojsk i obiektów wojskowych, prowadzenie dezinformacji dotyczącej stanu wojsk, charakteru planowanych działań w zakresie przygotowania i realizowania operacji. Wymienione działania służą wywieraniu wpływu na organy decyzyjne przeciwnika przez dostarczanie im fałszywych informacji i ukrywanie rzeczywistej aktywności wojsk. Wykorzystuje sie w tym celu jego system gromadzenia, przetwarzania i analizowania informacji. Dzięki dezorientowaniu i dezinformowaniu przeciwnika zmusza się go do wyciągania błędnych wniosków, a w rezultacie – do podejmowania niewłaściwych decyzji[21]. W FR maskirowka na poziomie operacyjnym jest planowana i organizowana przez Połączone Dowództwa Operacyjno-Strategiczne (PDO-S) oraz dowództwa ich armii w Marynarce Wojennej przez dowództwa flot, a w Siłach Powietrznych przez dowództwa armii lotniczych i obrony powietrznej.

Czynnikiem wpływającym na skuteczność maskowania operacyjnego jest tajność działalności organów, które nim dowodzą[22]. Ponieważ jest ono realizowane jednocześnie przez wiele jednostek wyższego i niższego szczebla, konieczne jest skoordynowanie planów działania dowódców oddziałów i pododdziałów z planami dowódców wyższego szczebla. Równie istotne jest wsparcie ze strony wywiadu

---

[18] Zob. В.А. Мацуленко, *Оперативная маскировка войск*, Москва 1975, s. 4–5.

[19] Por. В. Денисенко, *Стратегическая маскировка как образ российской политической жизни*, ИноСМИ.RU, 26 VI 2015 r., https://inosmi.ru/russia/20150626/228788387.html [dostęp: 30 X 2019].

[20] Zob. *Стратегическая маскировка и дезинформация*, http://politike.ru/termin/strategicheskaja-maskirovka-i-dezinformacija.html [dostęp: 30 X 2019].

[21] Por. *Оперативная маскировка*, Студопедия, 11 III 2015 r., https://studopedia.info/2-14013.html [dostęp: 30 X 2019].

[22] Por. П. Марущенко, *Идею введения противника в заблуждение необходимо формировать путем группирования отдельных мер обмана противника по выбранным признакам*, Бюро военно-политического анализа, 23 III 2018 r., http://bvpa.ru/обман-противника-процесс-творчески/ [dostęp: 20 XI 2019].

wojskowego. Pomaga on wskazać obiekty przeciwnika, wobec których będą stosowane działania z zakresu maskowania, opracować wiarygodną wersję fałszywych informacji używanych podczas realizowania działań dezinformacyjnych, wybrać najbardziej podatne cele tych działań, a także ocenić ich skuteczność.

Maskowanie na poziomie taktycznym ma na celu bezpośrednie ukrycie pozycji pododdziałów, stanowisk dowodzenia, uzbrojenia i sprzętu wojskowego, urządzeń logistycznych, rejonów koncentracji wojsk i sprzętu, punktów obserwacyjnych, manewrów formacji bojowych i marszowych oraz innych obiektów istotnych dla stron w celu ich ochrony przed rozpoznaniem i oddziaływaniem przeciwnika. Polega na dostosowywaniu się do otaczającego tła, np. za pomocą malowania maskującego, wykorzystania roślinności i ukształtowania terenu, a także stawiania zasłon dymnych. Jest realizowane przez wszystkie rodzaje wojsk oraz służb, na podstawie decyzji dowódców oddziałów lub pododdziałów. Za realizację odpowiada cały personel SZ FR, bez bezpośrednich instrukcji[23].

Maskowanie taktyczne musi być zgodne z wykonywanym zadaniem, zasadami maskowania oraz aktualną sytuacją bojową. Przygotowując je, dowódca wyznacza siły i organizuje środki (w tym materiały występujące w danym terenie czy też środowisku działań) przeznaczone do wykonania maskowania, określa czas i warunki jego realizacji, zgodność z zasadami maskowania i kamuflażu, etapy realizacji działań z zakresu kamuflażu oraz zasady jego monitorowania i aktualizowania w czasie wykonywania działań[24].

Współcześnie bardzo ważnym narzędziem maskirowki jest **zarządzanie refleksyjne** (ros. *рефлексивное управление*), znane również jako sterowanie refleksyjne (ros. *рефлексивный контроль*). Jego koncepcję opracował w latach 60. XX w. rosyjski psycholog i matematyk Władimir Lefewr. Uważał on, że wykorzystanie teorii gier jako paradygmatu bezpieczeństwa będzie podstawą podejmowania działań w sytuacji konfliktu. „Zarządzanie refleksyjne" jest definiowane jako wpływ informacyjny na obiekty, które mają świadomość oraz wolę. Tymi obiektami mogą być zarówno pojedyncze jednostki ludzkie, jak i całe wspólnoty, takie jak rodziny, grupy, narody, społeczeństwa, a nawet całe cywilizacje[25]. Zarządzanie refleksyjne polega na zdobyciu umiejętności postrzegania sytuacji w taki sposób jak strona przeciwna. Każda ze stron konfliktu dąży do przeniknięcia do umysłu przeciwnika oraz zniekształcenia jego wyobrażeń na temat danej sytuacji w sposób korzystny dla siebie, co przełoży się na decyzje i działania podejmowane przez stronę przeciwną. Sterowanie przeciwnikiem odbywa się głównie za pomocą podsuwania mu pewnych przesłanek, które mają mu pomóc podjąć w logiczny sposób decyzje korzystne dla drugiej strony. Te przesłanki muszą być przekazywane

[23] Zob. https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=13494@morfDictionary [dostęp: 30 X 2019].

[24] Maskowanie na poziomie taktycznym organizuje się według znanych zasad maskowania, bez oczekiwania na wydanie dodatkowych rozkazów w tym zakresie. Zob. https://red-tent.ru/mask/maskirovka [dostęp: 20 XI 2019].

[25] K. Giles, J. Sherr, C. House, *Russian Reflexive Control*, Kingston 2008, s. 5.

w sposób niedostrzegalny dla przeciwnika, oparty na wiedzy dotyczącej jego sposobu działania, myślenia i procesu decyzyjnego. Zarządzanie refleksyjne opiera się na czterech głównych zasadach[26]:

1) przekazywanie fałszywych informacji o sytuacji lub nieprawdziwego obrazu pewnego obiektu;
2) wykreowanie celu dla przeciwnika, np. za pomocą aktów terrorystycznych czy dywersji ideologicznej;
3) sformułowanie doktryny (systemu działania)[27] korzystnej dla strony, która stosuje zarządzanie refleksyjne, i przekazanie jej stronie przeciwnej;
4) zdezorientowanie przeciwnika przez wykreowanie wielu fikcyjnych celów, co uniemożliwi mu odkrycie rzeczywistego celu strony, która stosuje zarządzanie refleksyjne.

Tego rodzaju strategie są wykorzystywane nie tylko w wojskowości, lecz także w polityce wewnętrznej, zagranicznej oraz w reklamie i marketingu.

Ewolucja sztuki maskowania operacyjnego Federacji Rosyjskiej

Maskowanie działań ma w rosyjskim wojsku wielowiekową tradycję. Zastosowano je już w XIV w., w czasie bitew Księstwa Moskiewskiego ze Złotą Ordą. Najbardziej znanym przykładem z tego okresu jest bitwa na Kulikowym Polu, podczas której Dymitr Doński pokonał wojska Złotej Ordy dzięki podstępowi oraz wykorzystaniu warunków atmosferycznych i terenowych. Cztery wieki później skuteczne maskowanie przeprowadził Aleksandr Suworow w bitwie pod Fokszanami w 1789 r. Działania demonstracyjne w rejonie twierdzy Izmił pozwoliły mu skupić uwagę przeciwnika na obiekcie pozornym. Suworow wykorzystał maskirowkę również w czasie kampanii włoskiej, podczas której upozorował kierunek głównego działania oraz skutecznie zamaskował swoje zamiary i sposób działania. W czasach carskich, a następnie w bolszewickiej Rosji podstęp i zaskoczenie wykorzystywano głównie w polityce.

W rosyjskim wojsku do maskowania operacyjnego zaczęto przykładać szczególną wagę podczas I wojny światowej. Zapoczątkowano wtedy stosowanie technicznych środków maskujących, takich jak farby do kamuflażu, siatki maskujące czy zasłony dymne. Z maskowania korzystały zarówno oddziały walczące na froncie, jak i jednostki tyłowe. Rozpoczęto także publikację podręczników i instrukcji dotyczących maskowania. Jego pierwsze zasady zostały określone w sowieckiej doktrynie wojskowej wydanej w 1924 r. Miało być ono naturalne, oparte na metodach działania wojsk, różnorodne i ciągłe, wykorzystywać sposoby zatajania informacji o planach i działaniach

[26] M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 20.

[27] Powinien to być skończony ciąg czynności, które są konieczne do wykonania określonego zadania lub prowadzą do ułatwienia podjęcia decyzji czy czynności.

wojsk, imitację, działania demonstracyjne oraz dezinformację. W latach 1936–1939 w przepisach polowych Armii Czerwonej zawarto informacje o konieczności stosowania wszelkiego rodzaju podstępów, gdyż tylko dzięki nim jest możliwe osiągnięcie efektu zaskoczenia[28].

Największym zainteresowaniem maskirowka cieszyła się w czasie II wojny światowej. Efekt zaskoczenia oraz możliwości, jakie daje sztuka podstępu wojennego, zostały docenione po niemieckim ataku na ZSRR w 1941 r. Już 26 czerwca 1941 r. wydano pierwszą instrukcję operacyjną na temat ukrycia obiektów wojskowych przed atakami sił powietrznych przeciwnika. Za pierwszą próbę wykorzystania maskirowki na szeroką skalę uznaje się radziecką kontrofensywę pod Moskwą w 1941 r., w czasie wielkiej wojny ojczyźnianej. Zastosowano w niej dyscyplinę w zakresie używania dźwięku i światła, ograniczono do minimum korzystanie z komunikacji radiowej, a przegrupowania wojsk ukrywano dzięki przemieszczaniu się w nocy. Od tej pory maskirowka w różnych formach i zakresach była stosowana w niemal wszystkich operacjach przeprowadzonych przez sowieckie wojska podczas II wojny światowej. Do najsłynniejszych jej przykładów możemy zaliczyć: bitwę z japońskimi wojskami nad Chałchin-Goł, operację rżewsko-wiaziemską, operację Uran, bitwę pod Kurskiem oraz operację Bagration. Wojna ojczyźniana nauczyła Sowietów, jak ogromne znaczenie ma maskowanie rozmiarów, dokładnego czasu oraz kierunków działania. Za środki, dzięki którym można osiągnąć skuteczny efekt zaskoczenia, uznano: utrzymywanie w tajemnicy przegrupowywania wojsk, działania demonstracyjne, działania symulacyjne, mające doprowadzić do zmian w szykach przeciwnika, maskowanie prawdziwych zamiarów i miejsc dyslokacji wojsk oraz dezinformację szerzoną za pomocą środków technicznych, wydawania fałszywych rozkazów oraz rozgłaszania pogłosek. Doświadczenia wojenne potwierdziły również konieczność ścisłego powiązania maskirowki taktycznej, operacyjnej i strategicznej, ponieważ skuteczność ich działania jest od siebie uzależniona[29].

Po zakończeniu II wojny światowej zainteresowanie maskirowką w Rosji w dalszym ciągu rosło w związku z gwałtownym rozwojem uzbrojenia oraz środków rozpoznania. W latach 50. oraz 60. XX w. maskowanie strategiczne i maskowanie operacyjne były ściśle powiązane z bronią nuklearną. Przykładem może być operacja Anadyr, która doprowadziła do wybuchu kubańskiego kryzysu rakietowego w 1963 r. Jej celem było skryte rozmieszczenie na Kubie sowieckich wyrzutni rakiet balistycznych średniego i dalekiego zasięgu. Do działań z zakresu maskirowki zaliczono nowe metody osiągania efektu zaskoczenia, m.in. wykorzystanie ćwiczeń lub manewrów wojskowych do przemieszczenia wojsk. Taką formą maskowania przerzutu sił zastosowano zarówno podczas inwazji wojsk sowieckich na Czechosłowację w 1968 r., jak i w czasie inwazji na Afganistan w 1979 r. Maskowanie w okresie powojennym było ściśle wspierane i koordynowane przez KGB. Od lat 70. XX w. maskirowkę zaczęto coraz wyraźniej łączyć

[28] D. Glantz, *Soviet Military Deception in the Second World War*, New York 2005, s. 5–20.

[29] J. Latimer, *Podstęp na wojnie*, Warszawa 2017, s. 244–262.

ze sferą polityczną, gospodarczą i dyplomatyczną, a nie, jak wcześniej, wyłącznie z militarną. Wraz z zakończeniem zimnej wojny nie zaprzestano korzystania z maskirowki. Obecnie również można znaleźć wiele przykładów jej stosowania na poziomie strategicznym, nie tylko w sferze militarnej, lecz także politycznej, gospodarczej czy społecznej. Jest ona jednym z coraz skuteczniejszych i coraz częściej wykorzystywanych narzędzi w polityce zagranicznej oraz w celu kształtowania opinii międzynarodowej. Współczesna maskirowka przekształca się ze strategii działania stricte wojskowego w strategię geopolityczną, ale jej główne cele, tj. ukrycie swoich zamiarów, odwrócenie uwagi przeciwnika i dezinformacja, aby opóźnić jego reakcję, pozostają niezmienne.

Współczesne przykłady stosowania maskirowki

Federacja Rosyjska korzystała z maskirowki podczas wojny w Gruzji. Konflikt rozpoczął się w nocy z 7 na 8 sierpnia 2008 r. pomiędzy Gruzją a Osetią Południową wspieraną przez FR. Do działań zbrojnych 10 sierpnia 2008 r. dołączyła Abchazja. Główne przyczyny tej wojny to trwające od wielu lat konflikty etniczne pomiędzy Gruzinami a Osetyjczykami oraz dążenia Osetii Południowej i Abchazji do oderwania się od terytorium Gruzji i uzyskania pełnej niepodległości. Wzrost napięć pomiędzy Gruzją a Rosją nastąpił po ogłoszeniu przez rząd FR 6 marca 2008 r. informacji o zakończeniu uczestnictwa w sankcjach gospodarczych nałożonych w 1996 r. na Abchazję przez Wspólnotę Niepodległych Państw. W tym czasie nawiązała ona bezpośrednie stosunki z separatystycznymi władzami Osetii Południowej i Abchazji. W dniu 1 marca 2008 r. Wasilij Lunev, jeden z rosyjskich ministrów, były zastępca dowódcy Syberyjskiego Okręgu Wojskowego, został ministrem obrony Osetii Południowej. Kilka dni później parlamenty Abchazji oraz Osetii Południowej wezwały Rosję oraz pozostałych członków Wspólnoty Niepodległych Państw oraz ONZ do uznania ich niepodległości[30].

Działania FR były bezpośrednio związane z dążeniem Gruzji do wstąpienia do NATO oraz z deklaracją niepodległości złożoną przez Kosowo. Rosja postanowiła wykorzystać precedens proklamowania niepodległości przez Kosowo i uznania tego kraju przez kilkadziesiąt państw. Ta sytuacja pokazała bowiem, że jedna z głównych zasad powojennego ładu europejskiego dotycząca niezmienności granic nie jest już powszechnie obowiązująca. Dzięki temu Rosja miała mocny argument przemawiający za wsparciem przez nią dążeń niepodległościowych ludności osetyjskiej i abchaskiej. Należy również zauważyć, że poparcie autonomicznych planów Kosowa przez państwa europejskie, nieuwzględnienie stanowiska FR w tej sprawie, a także bezpośrednie uderzenie w interesy Serbii, która jest bliskim sojusznikiem Rosji w regionie bałkańskim,

[30] *Как готовилась война*, „Новая газета", 27 VI 2009 r., https://novayagazeta.ru/articles/2009/06/28/42316-kak-gotovilas-voyna [dostęp: 10 II 2020].

pokazały osłabienie pozycji Rosji na arenie międzynarodowej oraz w regionie byłej Jugosławii[31].

Bardzo ważnym elementem maskowania działań FR poprzedzającym rozpoczęcie konfliktu gruzińskiego było zastosowanie zarządzania refleksyjnego. Obiektami operacji informacyjno-psychologicznej była strona gruzińska, na czele z prezydentem Micheilem Saakaszwilim, a także światowa opinia publiczna. Jednym z dowodów, który to potwierdza, jest sporządzenie przez Wiktora Ruczkina profilu psychologicznego ówczesnego prezydenta Gruzji. Zostały w nim opisane dzieciństwo i młodość Saakaszwilego, przeanalizowano jego modele zachowania, wewnętrzne komponenty emocjonalne, sposób wyrażania emocji, czynniki motywacyjne oraz intelekt. Na tej podstawie wydano zalecenia dotyczące działań związanych z osobą Saakaszwilego. Można więc uznać, że operacja wymierzona w prezydenta Gruzji przybierała formy nacisku siłowego, wywierania wpływu na algorytm podejmowania decyzji, a także kreowania i przekazywania fałszywych informacji o sytuacji[32].

Przed rozpoczęciem działań wojennych batalion żołnierzy wojsk inżynieryjnych, w skład którego wchodziło 400 żołnierzy, wkroczył do Abchazji bez pozwolenia gruzińskiego rządu w celu naprawy nieczynnej linii kolejowej między stolicą Abchazji Suchumi a miastem Ochamchire, leżącym w bezpośrednim sąsiedztwie abchasko-gruzińskiej linii rozgraniczającej. Do wiadomości publicznej podano informację, że chodzi o poprawienie infrastruktury kolejowej przed zimowymi igrzyskami w Soczi. Jednak prawdziwym celem naprawy połączeń kolejowych było ułatwienie przerzutu sił i środków rosyjskich wojsk przeznaczonych do wzięcia udziału w wojnie w Gruzji[33]. W tym czasie (od 30 maja do 30 czerwca 2008 r.) zbudowano także trzy nowe hangary dla samolotów i amunicji w bazie lotniczej Bombora w pobliżu Suchumi. Obawy rządu w Tbilisi wzbudzały także nieautoryzowane transporty broni i materiałów wybuchowych, organizowane przez wojska rosyjskie w rejonie miasta Zugdidi położonego w zachodniej Gruzji oraz zwiększenie do 3 tys. liczby rosyjskich żołnierzy przebywających na terytorium Abchazji[34].

Kolejnym przejawem stosowania działań dezinformacyjnych były ćwiczenia „Kaukaz 2008", odbywające się na Kaukazie Północnym, tuż przy granicy z Gruzją. Określono je jako ćwiczenia poświęcone wspólnej odpowiedzi sił wojskowych na zagrożenie z południa. W ramach manewrów do Osetii Północnej przerzucono ok. 8 tys. żołnierzy

---

[31] K. Kubiak, *Wojna w Gruzji w 2008 roku. Geneza i przebieg działań zbrojnych*, „Międzynarodowe Prawo Humanitarne" 2011, t. 2: *Konflikt rosyjsko-gruziński w 2008 r.*, s. 16.

[32] Zob. В. Ручкин, *Вирус вождизма*, „Красная звезда", 13 VIII 2008 r., http://old.redstar.ru/2008/08/13_08/4_06.html [dostęp: 10 II 2020].

[33] Zob. *Медведев разъяснил Саакашвили задачи железнодорожных войск России в Абхазии*, NEWSru.com, 3 VI 2008 r., http://palm.newsru.com/russia/03jun2008/medsaak.html [dostęp: 10 II 2020].

[34] C.W. Blandy, *Provocation, Deception, Entrapment: The Russo-Georgian Five Day War*, Swindon 2009, s. 4.

i 700 pojazdów[35]. Podana liczba żołnierzy została najprawdopodobniej zaniżona, zważywszy na to, że w ćwiczeniach nie brali udziału międzynarodowi obserwatorzy. Ich uczestnicy otrzymali ulotki zatytułowane *Żołnierzu! Znaj swojego wroga!*, które zawierały opis cech charakterystycznych gruzińskich sił zbrojnych. W czasie ćwiczeń specjalny oddział medyczny ustawił szpital polowy w mieście Tarskoje, który mógł przyjąć dziennie do 300 rannych. Po ich zakończeniu szpital nie został zlikwidowany. Pretekstem do jego utrzymania miał być wniosek otrzymany od lokalnych władz, które zwróciły się z prośbą o pozostawienie szpitala w celu zapewniania lokalnym mieszkańcom pomocy konsultacyjnej i diagnostycznej. Prawdziwym celem ćwiczeń „Kaukaz 2008" było pokazanie, że po zmianach na stanowiskach dowodzenia wojska FR nie są w pełni zgrane, a sam system dowodzenia nie jest całkowicie sprawny. Oznaczało to nieprzygotowanie wojsk rosyjskich do prowadzenia działań zbrojnych i konieczność odtworzenia ich zdolności bojowych. Manewry „Kaukaz 2008" umożliwiły również ukrycie części sił w rejonie Abchazji oraz pozostawienie zamaskowanego sprzętu w okolicach tunelu Roki.

Posunięciami, które również miały odwrócić uwagę od rosyjskich działań w Gruzji, były wyjazd premiera FR na otwarcie XXIX Letnich Igrzysk Olimpijskich w Pekinie oraz urlop prezydenta. Urlop miał sugerować, że w tym czasie prezydent nie wyda decyzji o przeprowadzeniu operacji angażującej SZ FR.

Pierwsze informacje o wybuchu konfliktu pojawiły się w serwisach informacyjnych niemal od razu, a zamieszczone w nich zdjęcia ukazywały gruziński nocny ostrzał artyleryjski Cchinwali. Miało to ułatwić osetyjskim separatystom i rosyjskiej propagandzie wykreowanie wizerunku Gruzji jako agresora ostrzeliwującego uśpione miasto, a także pokazać, że przeprowadza ona operacje ludobójcze. Działania wojsk gruzińskich wywołały szybką i zdecydowaną reakcję strony rosyjskiej. Przed świtem 8 sierpnia 2008 r. wydano decyzję o użyciu sił zbrojnych w celu rozwiązania konfliktu, pomimo trwania wakacji parlamentarnych i braku możliwości szybkiego zwołania Dumy Państwowej, która musi wyrazić zgodę na wykorzystanie SZ FR. Aby rozwiązać ten formalno-prawny problem, wykorzystano to, że siły Federacji Rosyjskiej miały mandat do przebywania na terytorium Osetii w ramach sił pokojowych. Akcje zbrojne uznano za przedłużenie tego mandatu.

Federacja Rosyjska próbowała usprawiedliwić swoje działania i przekonać opinię międzynarodową, że wszystkie podejmowane przez nią decyzje były odpowiedzą na gruzińską agresję. Dużą wagę przykładano do pokazywania, że są one uchwalane ad hoc, aby uwiarygodnić brak istnienia wcześniejszych planów wojny z Gruzją. Chodziło o wykreowanie przeświadczenia, że FR była zaskoczona zaistniałą sytuacją, co miało zdjąć z niej odpowiedzialność za rozpoczęcie konfliktu[36]. Na terytorium działań wojennych zabrano dziennikarzy, którzy mieli relacjonować gruzińskie okrucieństwa

[35] Zob. J. Zawadzki, *Współczesny rozbiór państwa. Casus Gruzji*, „Nowa Polityka Wschodnia" 2011, nr 1, s. 164.

[36] B. Ellison, *Russian Grand Strategy in the South Ossetia War*, „Demokratizatsiya: The Journal of Post-Soviet Democratization" 2011, nr 19, s. 348.

oraz działania Rosji podejmowane w celu ochrony jej obywateli. Wojska rosyjskie ukazywano jako wyzwolicieli miejscowej ludności[37]. Dmitrij Miedwiediew oskarżył Gruzję o ludobójstwo mieszkańców Osetii Południowej. Zbrodnie, których mieli dopuścić się Gruzini, miały polegać na podpalaniu ludzi, cięciu ich na kawałki, najeżdżaniu na nich gąsienicami czołgów[38]. Strona rosyjska celowo zawyżała liczbę cywilów, którzy zginęli 8 sierpnia 2008 r. w czasie ostrzału Osetii Południowej przez wojska gruzińskie. Organizacja Humans Rights Watch, badająca sprawę śmierci cywilów, podała, że informacje o 1400 ofiarach pierwszego dnia walk w Cchinwali są mocno przesadzone, gdyż według danych przedstawionych przez miejscowy szpital w tym dniu trafiło do niego 273 rannych, a do kostnicy przywieziono 44 ciała. Doniesienia o grzebaniu ofiar w przydomowych ogródkach nie zostały przyjęte przez społeczność międzynarodową, ponieważ nie uzyskano żadnych danych personalnych tych zmarłych[39].

Opisane działania miały wywrzeć silny wpływ psychologiczny na społeczność międzynarodową i usprawiedliwić kontynuację operacji, określanej przez stronę rosyjską jako pokojowa. Dezinformacja miała wpłynąć również na społeczność osetyńską i wzmocnić ruchy separatystyczne oraz rozpalić nienawiść do ludności gruzińskiej. Próba zamaskowania działań FR w Gruzji stanowiła pewną analogię do działań NATO w Kosowie – nagminne łamanie praw człowieka przez państwo miało doprowadzić do interwencji innego państwa czy sojuszu międzynarodowego w celu ochrony ludności przed represjami. Skutkiem takiej interwencji miało być uznanie prawa mniejszości narodowej do własnej państwowości[40].

Działania dezinformacyjne nie zakończyły się wraz z wojną. Krótko po jej ustaniu strona rosyjska zaczęła rozpowszechniać materiały publicystyczne oraz filmowe, które miały dowodzić, że gruzińska agresja była wspierana przez Stany Zjednoczone oraz Ukrainę. W ten sposób chciano zdyskredytować ukraińskiego prezydenta przed zbliżającymi się wyborami prezydenckimi na Ukrainie, przedstawić go jako wroga i zdrajcę rosyjskiego narodu[41].

Maskirowka została wykorzystana również podczas aneksji Krymu (od 20 lutego do 26 marca 2014 r.), do której doszło po tragicznych wydarzeniach na ukraińskim Majdanie Niepodległości i po ucieczce Wiktora Janukowycza do Rosji. Początkiem działań autonomicznych na Krymie było przemówienie Władimira Konstantinowa, przewodniczącego Rady Najwyższej Autonomicznej Republiki Krymu, wygłoszone 20 lutego 2014 r.

---

[37] C. Donovan, *Russian Operational Art…*, s. 21.

[38] Zob. V. Radyuhin, *Medvedev, Putin accuse Georgia of genocide*, 11 VIII 2018 r., https://www.thehindu.com/todays-paper/tp-international/Medvedev-Putin-accuse-Georgia-of-genocide/article15279050.ece [dostęp: 25 I 2020].

[39] Por. T. Parfitt, *Russia exaggerating South Ossetian death toll, says human rights group*, „The Guardian", 13 VIII 2008 r., https://www.theguardian.com/world/2008/aug/13/georgia [dostęp: 25 I 2020].

[40] V. Cheterian, *The August 2008 war in Georgia: from ethnic conflict to border wars*, „Central Asian Survey" 2019, nr 2, s. 160–161.

[41] Zob. P. Andrusieczko, *Ukraiński konflikt gruzińsko-rosyjski*, 11 VIII 2010 r., http://www.new.org.pl/228-ukrainski-konflikt-gruzinsko-rosyjski [dostęp: 25 I 2020].

Stwierdził on, że w przypadku zwycięstwa Majdanu i odsunięcia Janukowycza od władzy Krym może oddzielić się od Ukrainy i przyłączyć do Rosji. Do pierwszych demonstracji doszło 23 lutego 2014 r. w Kerczu i Sewastopolu, podczas powitania żołnierzy Berkutu powracających na Półwysep Krymski. W miastach ściągnięto ukraińskie flagi, a w ich miejsce wywieszono rosyjskie. Na prorosyjskim spotkaniu, które odbyło się w Sewastopolu, ustalono, że miasto nie będzie już przekazywało podatków do Kijowa. Na mera Sewastopola wybrano prorosyjskiego działacza Aleksieja Czałego. Przedstawiciele partii politycznej Rosyjski Blok ogłosili z kolei, że rozpoczynają formowanie oddziałów samoobrony[42]. Do kolejnej demonstracji doszło dwa dni później. Jej uczestnicy domagali się zwołania w trybie nadzwyczajnym sesji Rady Republiki Autonomicznej Krymu, na której miałoby zostać rozpisane referendum w sprawie niepodległości Krymu i Sewastopola. W tym dniu Konstantinow wydał oświadczenie, w którym poinformował o nieuznawaniu regulacji prawnych stanowionych przez Radę Najwyższą Ukrainy. Rosyjskie władze postawiły w stan podwyższonej gotowości Flotę Czarnomorską stacjonującą w Sewastopolu[43].

Po powołaniu nowego rządu Ukrainy 27 lutego 2014 r. ok. godziny 4:20 siły opozycyjne zajęły budynki rządu oraz parlamentu Autonomicznej Republiki Krymu położone w Symferopolu. W tym samym czasie na ulicach Krymu zaczęły się pojawiać tzw. zielone ludziki, tj. zamaskowani bojownicy nieposiadający oznaczeń identyfikacyjnych, w rosyjskich mundurach i z rosyjskim wyposażeniem i uzbrojeniem[44]. Prezydent Rosji zaprzeczył, że są to rosyjscy żołnierze. Stwierdził, że takie mundury można kupić w dowolnym sklepie z militariami, a ci mężczyźni są przedstawicielami lokalnych jednostek samoobrony[45]. W krótkim czasie zostały opanowane wszystkie strategiczne budynki, a bazy ukraińskich sił zbrojnych zablokowane. Umożliwiła to bierna reakcja sił ukraińskich oraz przejście części oddziałów na stronę rosyjską[46]. Tego samego dnia jednostki Berkutu opanowały Przesmyk Perekopski, co pozwoliło na przejęcie całkowitej kontroli nad ruchem pomiędzy Krymem a terytorium Ukrainy. Deputowani parlamentu Krymu zadecydowali o zorganizowaniu referendum 25 maja 2014 r. Za jego przeprowadzeniem opowiedziało się 61 z 64 deputowanych. W tym dniu parlament podjął również decyzję (przyczyniło się do tego głosowanie o wotum nieufności), że ówczesnego premiera Republiki Krymskiej Anatolija Mohylewa zastąpi

[42] Zob. H. Amos, *Ukraine crisis fuels secession calls in pro-Russian south*, „The Guardian", 23 II 2014 r., https://www.theguardian.com/world/2014/feb/23/ukraine-crisis-secession-russian-crimea [dostęp: 12 III 2020].

[43] M. Gołda-Sobczak, *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016, s. 198.

[44] Zob. J. Sabak, *Pół dekady okupacji Krymu i wojny w Donbasie*, Defence 24, 11 III 2019 r., https://www.defence24.pl/pol-dekady-okupacji-krymu-i-wojny-w-donbasie-opinia [dostęp: 14 III 2020].

[45] Zob. L. Ash, *How Russia outfoxes its enemies*, BBC, 29 I 2015 r., https://www.bbc.com/news/magazine-31020283 [dostęp: 14 III 2020].

[46] M. Lakomy, *Przebieg i uwarunkowania konfliktu na wschodzie Ukrainy*, w: M. Stolarczyk, M. Lakomy, K. Czornik, *Implikacje konfliktu ukraińskiego dla bezpieczeństwa Polski. Aspekty polityczne, wojskowe, gospodarcze i społeczne*, Katowice 2015, s. 18.

Siergiej Aksionow, lider partii Rosyjska Jedność. Wyniki zarówno jednego, jak i drugiego głosowania są kwestionowane, ponieważ w dniu głosowania gmach parlamentu został przejęty przez nieoznakowane oddziały. Uniemożliwiły one dziennikarzom wejście do budynku, a parlamentarzystom odebrano telefony. Pojawiły się również informacje o sfałszowaniu głosowania, polegającym na oddawaniu głosów za nieobecnych deputowanych[47]. Siły opozycyjne zaczęły zajmować wojskowe lotniska sił zbrojnych Ukrainy zlokalizowane na Krymie[48]. Dzień później szef Głównej Dyrekcji Policji Krymu Walerij Radczenko złożył rezygnację, a na jego miejsce nowe władze Krymu wyznaczyły burmistrza Teodozji. Było to działanie niezgodne z konstytucją Republiki Krymu, w której określono, że mianowanie szefów sił bezpieczeństwa musi odbyć się we współpracy z Radą Najwyższą Ukrainy[49].

Dnia 1 marca 2014 r. Aksionow zaapelował do prezydenta FR Władimira Putina o pomoc w rozwiązaniu konfliktu na Półwyspie Krymskim. Siły bezpieczeństwa nie były bowiem w stanie skutecznie kontrolować sytuacji oraz uspokoić zamieszek, podczas których dochodziło do użycia broni, co miało stwarzać realne niebezpieczeństwo dla zdrowia i życia obywateli. Administracja FR oświadczyła, że apel premiera Krymu nie zostanie zlekceważony. Putin niezwłocznie zwrócił się do Rady Federacji o zgodę na interwencję wojskową na Ukrainie w związku z zagrożeniem życia obywateli FR – mieszkańców Krymu i personelu sił zbrojnych FR, które zostały rozmieszczone na terytorium Autonomicznej Republiki Krymu. Jej celem miało być unormowanie sytuacji społeczno-politycznej w kraju. Pomimo protestów rosyjskich obywateli Rada Federacji wydała zgodę na tę operację[50].

Nowo wybrane władze ukraińskie zareagowały na rosyjskie działania dopiero na początku marca. Dnia 2 marca 2014 r. została ogłoszona mobilizacja, ale dziesięć dni później Oleg Turczynow, pełniący obowiązki prezydenta Ukrainy, ogłosił, że armia ukraińska nie weźmie udziału w akcji na Krymie, ponieważ musi się skoncentrować na obronie wschodniej granicy państwa. Tę decyzję można tłumaczyć słabością państwa po zmianie władzy, obawą o eskalację konfliktu, brakiem zaufania do armii oraz niepewnością co do reakcji społeczeństwa ukraińskiego. Strona ukraińska chciała również zademonstrować swoje pokojowe zamiary, dzięki czemu mogłaby uzyskać poparcie Unii Europejskiej i Stanów Zjednoczonych.

Dnia 4 marca 2014 r. Sztab Generalny Sił Zbrojnych Ukrainy oświadczył, że na Krymie przebywają żołnierze FR nienależący do Floty Czarnomorskiej. Stwierdzono, że znajdują się tam żołnierze 1 Batalionu Zmotoryzowanego „Wostok" (wchodzącego

---

[47] Por. *RPT-INSIGHT-How the separatists delivered Crimea to Moscow*, Reuters, 13 III 2014 r., https://www.reuters.com/article/ukraine-crisis-russia-aksyonov-idINL6N0M93AH20140313?-edition-redirect=in [dostęp: 12 III 2020].

[48] M. Gołda-Sobczak, *Krym jako przedmiot sporu*…, s. 198.

[49] Zob. *Премьер-министр Крыма попросил Путина о помощи*, Tacc, 1 III 2014 r., https://tass.ru/mezhdunarodnaya-panorama/1013127 [dostęp: 12 III 2020].

[50] Zob. *Владимир Путин внёс обращение в Совет Федерации*, 1 III 2014 r., http://www.kremlin.ru/events/president/news/20353#sel=2:17:t6V,2:25:991 [dostęp: 12 III 2020].

w skład 18 Samodzielnej Zmotoryzowanej Brygady Strzeleckiej SZ FR), który stacjonuje w Kalinówce w Czeczenii, żołnierze 31 Samodzielnej Gwardyjskiej Brygady Powietrzno-desantowej dyslokowanej w Uljanowsku oraz żołnierze 22 Brygady Sił Specjalnego Przeznaczenia[51]. Minister obrony narodowej Ukrainy oświadczył, że na terytorium Krymu przebywa do 16 tys. rosyjskich żołnierzy, w tym ok. 5,5 tys. to żołnierze wojsk specjalnych[52]. Putin zaprzeczał jakoby nieoznakowani, uzbrojeni, rosyjskojęzyczni żołnierze, którzy zajęli najważniejsze miejsca na Krymie, należeli do rosyjskich sił specjalnych. Stwierdził, że są to prorosyjskie, lokalne siły samoobrony. Tę samą narrację podtrzymywał minister spraw zagranicznych Siergiej Ławrow. Podczas konferencji prasowej w Madrycie z udziałem hiszpańskiego ministra spraw zagranicznych powiedział on, że nieoznakowani żołnierze należą do jednostek samoobrony tworzonych przez mieszkańców Półwyspu Krymskiego, którym rząd rosyjski nie wydaje żadnych rozkazów[53].

Data referendum została dwukrotnie przełożona, początkowo na 30 marca 2014 r., a ostatecznie na 16 marca. Mieszkańcy mieli odpowiedzieć na dwa pytania[54]:

1. Czy jesteś za zjednoczeniem Krymu z Rosją jako członkiem FR?
2. Czy jesteś za przywróceniem Konstytucji Republiki Krymu z 1992 r. i za statusem Krymu jako części Ukrainy[55]?

Referendum odbyło się mimo sprzeciwu rządu ukraińskiego, który uznał je za niezgodne z konstytucją i unieważnił. Podano, że frekwencja wyniosła 83 proc. Według oficjalnych wyników 96,7 proc. głosujących opowiedziało się za zjednoczeniem Półwyspu Krymskiego z FR. Wyniki tego referendum zostały zakwestionowane, pojawiły się głosy, że prawdziwa frekwencja wyniosła zaledwie 30–40 proc., a jedynie połowa uczestników opowiedziała się za przyłączeniem Krymu do Rosji. Do monitorowania sposobu przeprowadzenia referendum nie dopuszczono żadnych obiektywnych obserwatorów ze społeczności międzynarodowej. Rosja zaprosiła jedynie grupę obserwatorów z europejskich

---

[51] Zob. *В Крыму находятся российские военнослужащие не только из частей ЧФ РФ, утверждают в Генштабе ВСУ*, Интерфакс, 4 III 2014 r., https://interfax.com.ua/news/general/194412.html [dostęp: 12 III 2020].

[52] Por. *Росія збільшила свій контингент в Криму до 16 тисяч військовослужбовців – Тенюх*, УНІАН, 4 III 2014 r., https://www.unian.ua/politics/892512-rosiya-zbilshila-sviy-kontingent-v-krimu-do-16-tisyach-viyskovoslujbovtsiv-tenyuh.html [dostęp: 12 III 2020].

[53] Zob. *Russia says cannot order Crimean 'self-defense' units back to base*, Reuters, 5 III 2014 r., https://www.reuters.com/article/us-ukraine-crisis-lavrov-spain-idUSBREA240NF20140305 [dostęp: 12 III 2020].

[54] Por. В. Шляхов, *Референдум в Крыму: ответ «нет» не предусмотрен*, „Голос Америки", 12 III 2014 r., https://www.golosameriki.com/a/world-ukraine-crisis-referendum/1869197.html [dostęp: 12 III 2020].

[55] Drugie pytanie, mimo że na pierwszy rzut oka wskazuje na możliwość wyrażenia woli pozostawienia Półwyspu Krymskiego jako części Ukrainy, oznaczało tak naprawdę opowiedzenie się za uzyskaniem przez Krym wszystkich administracyjno-terytorialnych praw niezależnego podmiotu. Byłby on co prawda częścią Ukrainy, ale miałby prawo do stanowienia o swoim losie i nawiązywania stosunków z dowolnymi państwami, co według analityków oznaczało jedynie wydłużenie procesu przejścia Półwyspu pod kontrolę rosyjską.

skrajnie prawicowych partii politycznych[56]. Dzień po przeprowadzeniu referendum Rada Najwyższa Krymu ogłosiła formalne uniezależnienie się Autonomicznej Republiki Krymu wraz z miastem Sewastopol od Ukrainy. Zwrócono się także do FR z prośbą o przyłączenie do niej Krymu. Dnia 18 marca 2014 r. pomiędzy Autonomiczną Republiką Krymu a Federacją Rosyjską został podpisany traktat o jej przystąpieniu wraz z Sewastopolem (jako podmioty federalne) do Rosji. Został on ratyfikowany przez Zgromadzenie Federalne 21 marca 2014 r.[57]

Putin na spotkaniu z Frontem Ludowym 10 kwietnia 2014 r. zaprzeczył jakoby Rosja przygotowywała się do przyłączenia Krymu do FR. Oświadczył, że wszelkie decyzje zostały podjęte dopiero po zbadaniu nastrojów społecznych i przeanalizowaniu wyników sondaży, z których wynikało, że 80 proc. mieszkańców Półwyspu Krymskiego chciałoby jego przyłączenia do Rosji[58]. Inną wersję wydarzeń prezydent FR przedstawił niemal rok później, 9 marca 2015 r. Po raz pierwszy przyznał wtedy, że plan aneksji Krymu został sporządzony 22 lutego 2014 r., na całonocnym spotkaniu zwołanym po usunięciu Janukowycza z urzędu prezydenta Ukrainy[59]. Władze rosyjskie przyznały się również do zaangażowania swoich wojsk w działania na Półwyspie Krymskim. Opowiedział o tym 17 kwietnia 2014 r. prezydent FR, który wziął udział w programie telewizyjnym *Linia bezpośrednia z Władimirem Putinem*. Przyznał on wtedy, że interwencja nie miała być operacją stricte wojskową, lecz sposobem na zapewnienie bezpieczeństwa ludności rosyjskojęzycznej oraz komfortowego środowiska dla wyrażania dążeń separatystycznych przez mieszkańców Półwyspu[60].

Maskirowkę wykorzystano także podczas konwoju przygotowanego przez FR, mającego dostarczyć pomoc humanitarną na Ukrainę, dla ludności cywilnej zamieszkującej obwody, w których toczyły się regularne walki pomiędzy separatystami a siłami rządowymi. Prezydent Putin w czasie rozmowy telefonicznej przeprowadzonej 11 sierpnia 2014 r. z przewodniczącym Komisji Europejskiej José Manuelem Barrosem poinformował go o przygotowywaniu przez Rosję takiego konwoju. W nocy 12 sierpnia ciężarówki wyruszyły z Podmoskowia i mimo protestów władz ukraińskich 22 sierpnia przekroczyły granicę. Przejazd odbył się na odcinku, który był kontrolowany przez rebeliantów. Uniemożliwiło to dokonanie inspekcji przez ukraińską straż graniczną oraz Międzynarodowy

---

[56] Zob. P.R. Gregory, *Putin's 'Human Rights Council' Accidentally Posts Real Crimean Election Results*, „Forbes", 5 V 2014 r., https://www.forbes.com/sites/paulroderickgregory/2014/05/05/putins-human-rights-council-accidentally-posts-real-crimean-election-results-only-15-voted-for-annexation/ [dostęp: 12 III 2020].

[57] Por. *Crimea, Sevastopol officially join Russia as Putin signs final decree*, RT, 21 III 2014 r., https://www.rt.com/news/russia-parliament-crimea-ratification-293/ [dostęp: 12 III 2020].

[58] Zob. *Путин: Россия не планировала присоединять Крым*, Tacc, 10 IV 2014 r., https://tass.ru/politika/1111359 [dostęp: 14 III 2020].

[59] Por. *Putin reveals secrets of Russia's Crimea takeover plot*, BBC, 9 III 2015 r., https://www.bbc.com/news/world-europe-31796226 [dostęp: 14 III 2020].

[60] Zob. *Direct Line with Vladimir Putin*, 17 IV 2014 r., http://en.kremlin.ru/events/president/news/20796 [dostęp: 12 III 2020].

Komitet Czerwonego Krzyża (MKCK). Przejazd konwoju bez zgody rządu w Kijowie czy kontroli MKCK był wyrazem lekceważącego stosunku Rosji do Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych. Pojawiły się wątpliwości co do prawdziwego celu przejazdu ciężarówek. Zamiast wsparcia ludności bardziej prawdopodobna stała się wersja o uzupełnianiu zapasów uzbrojenia i amunicji separatystów lub o zaplanowaniu przejazdu konwoju w taki sposób, aby dać FR pretekst do jawnej inwazji na terytorium Ukrainy. Jasne było bowiem, że w pobliżu granicy rosyjsko-ukraińskiej znajdują się siły wojskowe w liczbie ok. 20 tys. żołnierzy, zdolne do wejścia na terytorium tego państwa w krótkim czasie[61]. Do spekulacji społeczności międzynarodowej odniosło się Ministerstwo Spraw Zagranicznych FR, które oświadczyło, że ze względu na opóźnienia i wymówki ze strony rządu ukraińskiego Rosji po dziesięciu dniach „zabrakło cierpliwości". Oskarżono rząd ukraiński o celowe spowalnianie tempa dostarczania pomocy do obwodu ługańskiego[62]. Można przyjąć, że przejazd białego konwoju mógł być sposobem zamaskowania wprowadzenia żołnierzy FR na terytorium Ukrainy oraz przygotowań do działań militarnych. Według premiera Ukrainy nielegalny wjazd ciężarówek mógł być również próbą odwrócenia uwagi społeczności międzynarodowej od katastrofy lotu MH17 linii lotniczych Malaysia Airlines, do której doszło miesiąc wcześniej na terytorium Ukrainy[63].

W tym samym czasie na Ukrainie coraz bardziej widoczna stała się działalność wojsk rosyjskich, zwłaszcza grup dywersyjnych. Pojawiły się także cztery taktyczne grupy batalionowe, których aktywność zaobserwowano na południowy wschód od Ługańska, w kierunku południowym od Iłowajska, w rejonie Doniecka oraz pod Nowoazowskiem[64]. W pobliżu miejscowości Dzerkalne znajdującej się w obwodzie donieckim 25 lipca 2014 r. wojska ukraińskie schwytały dziesięciu rosyjskich spadochroniarzy. Strona rosyjska tłumaczyła to zdarzenie przypadkowym przekroczeniem granicy podczas patrolu rozpoznawczego odbywającego się wzdłuż linii granicznej na nieoznaczonym odcinku[65]. Późnym wieczorem 14 sierpnia 2014 r. przejście graniczne w miejscowości Izwaryne przekroczyły 23 transportery wojskowe, tworzące zgrupowanie wojsk rosyjskich[66]. Separatyści w czasie walk coraz częściej używali

[61] Zob. K. Demirjian, M. Birnbaum, *Russia escalates tensions with aid convoy, reported firing of artillery inside Ukraine*, „The Washington Post", 22 VIII 2014 r., https://www.washingtonpost.com/world/russian-humanitarian-convoy-enters-ukraine-despite-warnings/2014/8/22/7b14fa8e-29e1-11e4-8593-da634b334390_story.html [dostęp: 8 III 2020].

[62] http://www.kremlin.ru/events/president/news/page/307 [dostęp: 8 III 2020].

[63] *Ukraine crisis: Russia aid convoy 'invades Ukraine'*, BBC, 22 VIII 2014 r., https://www.bbc.com/news/world-europe-28892525 [dostęp: 8 III 2020].

[64] I. Hurak, *Rosyjska obecność militarna oraz dyplomacja rosyjska w kontekście konfliktu na wschodzie Ukrainy*, „Wschód Europy" 2015, nr 2, s. 174.

[65] Por. *Captured Russian troops 'in Ukraine by accident'*, BBC, 26 VIII 2014 r., https://www.bbc.com/news/world-europe-28934213 [dostęp: 8 III 2020].

[66] Zob. *Rasmussen potwierdza wtargnięcie Rosjan. Hollande apeluje do Moskwy*, TVN24, 15 VIII 2014 r., https://tvn24.pl/swiat/rasmussen-potwierdza-wtargniecie-rosjan-hollande-apeluje-do-moskwy-ra459520-348636 [dostęp: 8 III 2020].

sprzętu wojskowego przekazanego przez FR, np. systemów rakietowych Uragan, pojazdów opancerzonych Tigr, wyrzutni Buk oraz czołgów. Sprzęt, uzbrojenie, amunicja, a nawet paliwo miały być dostarczane w ramach przejazdu konwojów wojskowych przez miasto Krosnodon, położone ok. 15 km od granicy rosyjsko-ukraińskiej[67]. Ponadto w czasie, gdy społeczność międzynarodowa była zajęta sprawą przejazdu konwoju humanitarnego, rosyjska artyleria wspierała działania prorosyjskich separatystów, wystrzeliwując ze swojego terytorium rakiety Grad i Urgan[68], a 76 Dywizja Desantowo-Szturmowa dyslokowana w Pskowie brała udział w walkach o Ługańsk.

Dane wywiadowcze posiadane przez NATO świadczyły o niepokojącym wzroście sił lądowych i powietrznych wchodzących w skład SZ FR skoncentrowanych w pobliżu granicy z Ukrainą. Wykryto również duże ilości transferów broni, wyrzutni artyleryjskich, czołgów oraz transporterów opancerzonych. Miały być one dostarczane przez Rosję grupom separatystycznym walczącym na wschodzie Ukrainy[69].

Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE, ang. Organization for Security and Co-operation in Europe) pełniąca misję obserwacyjną OBWE na punktach kontrolnych przejść granicznych w Gukowie i Doniecku poinformowała, że 22 sierpnia 2014 r. 227 rosyjskich ciężarówek mających nieść pomoc humanitarną przekroczyło granicę rosyjsko-ukraińską bez eskorty MKCK. Tylko 34 zostały poddane kontroli dzień wcześniej przez członków misji obserwacyjnej. Reszta konwoju, w tym pojazdy pomocnicze (m.in. karetki pogotowia ratunkowego), nie została skontrolowana[70]. Do wybranych pojazdów pozwolono zajrzeć dziennikarzom. Potwierdzili oni, że w pokazanych im ciężarówkach znajdowały się zapasy świadczące o przewożeniu pomocy humanitarnej, takie jak żywność dla niemowląt, płatki zbożowe, kasze czy śpiwory. Niepokój społeczności międzynarodowej wzbudziło to, że niektóre z przemalowanych na biało Kamazów były prawie puste[71]. Ciężarówki zaczęły wracać na terytorium Rosji dzień później, w sobotę 23 sierpnia 2014 r. W tym samym czasie, gdy białe ciężarówki odwracały uwagę społeczności międzynarodowej, granicę ukraińsko-rosyjską przekroczył inny konwój. Sfotografowano 23 transportery opancerzone, wspierane przez ciężarówki przewożące paliwo oraz inne pojazdy logistyczne

---

[67] *Reporter AP: Rosja przerzuca na Ukrainę broń w rejonie Krasnodonu*, TVN24, 26 VIII 2014 r., https://tvn24.pl/swiat/reporter-ap-rosja-przerzuca-na-ukraine-bron-w-rejonie-krasnodonu-ra462025-3409862 [dostęp: 8 III 2020].

[68] *Bellingcat Report – Origin of Artillery Attacks on Ukrainian Military Positions in Eastern Ukraine Between 14 July 2014 and 8 August 2014*, Bellingcat, 17 II 2015 r., https://www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/ [dostęp: 8 III 2020].

[69] *NATO Secretary General condemns entry of Russian convoy into Ukraine*, NATO, 22 VIII 2014 r., https://www.nato.int/cps/en/natohq/news_112112.htm [dostęp: 8 III 2020].

[70] *Spot report by the OSCE Observer Mission at the Russian Checkpoints Gukovo and Donetsk, 22 August 2014: Russian humanitarian aid trucks departed from the Donetsk Border Crossing Point without ICRC's escort*, OSCE, 22 VIII 2014 r., https://www.osce.org/om/122927 [dostęp: 8 III 2020].

[71] Zob. *Maskirovka' Is Russian Secret War*, War Is Boring, 26 VIII 2014 r., https://medium.com/war-is-boring/maskirovka-is-russian-secret-war-7d6a304d5fb6 [dostęp: 8 III 2020].

oznaczone rosyjskimi tablicami wojskowymi, które późnym wieczorem przemieszczały się w kierunku Doniecka. Konwój wjechał na terytorium Ukrainy po rzadko uczęszczanej drodze gruntowej, w rejonie przejętym przez separatystów[72].

Po sukcesie przejazdu pierwszego białego konwoju od sierpnia 2014 r. do października 2018 r. na południowo-wschodnie terytoria Ukrainy zostały wysłane łącznie 84 konwoje humanitarne. Według danych opublikowanych przez Ministerstwo Obrony Cywilnej, Sytuacji Kryzysowych i Eliminacji Skutków Klęsk Żywiołowych FR na Ukrainę dostarczono ponad 78 tys. ton produktów, takich jak żywność i leki[73]. Należy jednak zauważyć, że ukraińskim i międzynarodowym organizacjom humanitarnym, które chciały udzielić pomocy ludności w obwodzie ługańskim i donieckim, ograniczono niemal całkowicie dostęp. Jedyną organizacją humanitarną mającą możliwość prowadzenia działalności na terenie obydwu republik pozostał MKCK[74]. Stworzyło to idealne warunki do działań propagandowych. Ukazywano władze ukraińskie jako ignorujące problemy ludności, a stronę rosyjską jako jedyną udzielającą realną pomoc i zapewniającą wsparcie.

Burza medialna wokół białego konwoju, skupienie uwagi dziennikarzy na ciężarówkach i spekulacje na temat ich zawartości skutecznie odwróciły uwagę od innych przejść granicznych kontrolowanych przez prorosyjskich separatystów, którymi żołnierze i specjaliści wraz z sprzętem wojskowym mogli bez problemu przedostawać się na terytorium Ukrainy. W ten sposób na chwilę odwrócono również uwagę od zestrzelenia samolotu malezyjskich linii lotniczych nad terytorium zajętym przez separatystów.

Podsumowanie

Współczesne środowisko bezpieczeństwa międzynarodowego dynamicznie się zmienia, czego potwierdzeniem jest m.in. wojna w Gruzji oraz sytuacja na Ukrainie. Przeobrażeniom ulega również charakter wojen i konfliktów zbrojnych. Zmniejsza się prawdopodobieństwo zaistnienia oficjalnie wypowiedzianych wojen pomiędzy państwami, coraz częściej natomiast mamy do czynienia z konfliktami wewnątrz państw podsycanymi przez grupy rebelianckie i separatystyczne. Te grupy niejednokrotnie są inspirowane przez rządy innych państw, dążące do realizacji własnych interesów i celów strategicznych przez zachwianie równowagi politycznej, gospodarczej w atakowanym państwie oraz zdyskredytowanie go na arenie międzynarodowej. Pojawiają się nowe zagrożenia

[72] Por. S. Walker, *Aid convoy stops short of border as Russian military vehicles enter Ukraine*, „The Guardian", 15 VIII 2014 r.,https://www.theguardian.com/world/2014/aug/14/russian-military-vehicles-enter-ukraine-aid-convoy-stops-short-border [dostęp: 8 III 2020].

[73] Zob. *Международное сотрудничество*, МЧС России, https://www.mchs.gov.ru/deyatelnost/mezhdunarodnoe-sotrudnichestvo [dostęp: 8 III 2020].

[74] V. Barbelet, *Humanitariac access and local organisations in Ukraine*, London 2017, s. 1–18.

związane z cyberprzestrzenią, których przejawem może być nie tylko atak na infrastrukturę informatyczną obiektów strategicznych czy zasoby informacyjne administracji publicznej. Coraz większym i poważniejszym zagrożeniem jest wykorzystywanie Internetu do działań propagandowych i dezinformacyjnych. Przestrzeń wirtualna staje się idealnym miejscem do manipulacji mitami, świadomością społeczną oraz do podsycania i wykorzystywania obaw istniejących wśród ludności cywilnej. Działalność tzw. internetowych trolli pokazuje, jak łatwo można posłużyć się mediami społecznościowymi, forami tematycznymi czy sekcjami komentarzy stron informacyjnych, żeby manipulować.

Współcześnie maskirowka, zarówno w zakresie celów, jak i narzędzi, jest coraz szerzej wykorzystywana, zwłaszcza na poziomie strategicznym, w sferze politycznej, gospodarczej i dyplomatycznej. Aby zwiększyć jej skuteczność, konieczne jest ścisłe skoordynowanie wszystkich organizacji i struktur zaangażowanych w wykonanie zadania, które muszą podlegać scentralizowanemu dowództwu i być stale kontrolowane. Efektywne maskowanie wymaga również pokazania swojego zaangażowania w przestrzeganie prawa międzynarodowego. W przypadku braku możliwości zamaskowania udziału sił zbrojnych w konflikcie należy uzasadniać ich działania przez odwoływanie się do konieczności obrony praw człowieka czy zapewnienia bezpieczeństwa własnym obywatelom. Ze względu na szeroki dostęp do informacji, jakim dziś dysponuje opinia publiczna, maskowanie oznacza także konieczność posługiwania się dezinformacją, w tym manipulowanie informacjami w telewizji publicznej, oraz podsycania niepokojów społecznych, zarówno bezpośrednio na miejscu działań, jak i w sieci internetowej, np. przy pomocy internetowych trolli.

Obecnie wykorzystanie maskirowki wydaje się szczególnie skuteczne na szczeblu taktycznym, np. w czasie przemieszczania wojsk, jednak na szczeblu strategicznym może stwarzać problemy, zwłaszcza w środowisku międzynarodowym. Jej nieskuteczność może spowodować utratę zaufania zarówno innych państw, jak i własnego społeczeństwa, izolację na arenie międzynarodowej czy nałożenie sankcji gospodarczych. Najważniejszymi elementami mającymi wpływ na skuteczność maskowania są jednolity scenariusz i linia narracji, z którymi muszą zostać zapoznane wszystkie osoby biorące aktywny udział w tego typu działaniach.

Prognozuje się, że maskirowka będzie coraz częściej wykorzystywana w wojnach, konfliktach zbrojnych oraz działaniach innych niż wojenne do osiągania celów militarnych oraz politycznych i gospodarczych. Dużą rolę będzie ogrywała w maskowaniu działań podmiotu państwowego na arenie międzynarodowej. Rozwój technologii i coraz szerszy dostęp społeczeństwa do informacji sprawiają, że jednym z filarów maskowania stają się działania w cyberprzestrzeni, podejmowane przede wszystkim w celach dezinformacyjnych oraz propagandowych. To zjawisko można zaobserwować już dzisiaj. Aktywność w cyberprzestrzeni będzie ukierunkowana na kreowanie opinii publicznej, wzbudzanie niepokojów i wykorzystywanie społecznych obaw czy mitów. Bardzo dużego znaczenia nabierze zarządzanie refleksyjne, które, co potwierdziła wojna w Gruzji, pozwala na szybkie i skuteczne osiągnięcie celów. Współczesne konflikty

zbrojne pokazują, że efektywnym środkiem maskowania jest również zacieranie różnic pomiędzy konwencjonalnym a niekonwencjonalnym sposobem prowadzenia działań. W przyszłości coraz więcej celów będzie realizowanych za pomocą nowych typów wojen, takich jak wojna pełzająca czy wojna hybrydowa, których cechą charakterystyczną jest stosowanie maskirowki na ogromną skalę. W tego typu wojnach dużą rolę odgrywa przestrzeń wirtualna, która jest wykorzystywana do zdobywania informacji i manipulowania ludnością zamieszkującą terytoria, na których toczą się działania. W działaniach wojennych będzie się unikać bezpośrednich starć, dążyć do rozproszonego funkcjonowania sił oraz korzystać z systemów bezzałogowych i broni precyzyjnego rażenia. Agresor będzie unikał odpowiedzialności za swoje postępowanie, prowadząc działania w sposób skryty, podejmując wielokierunkowe strategie dyplomatyczne, stosując presję ekonomiczną oraz wykorzystując na dużą skalę służby specjalne. Natomiast maskowanie stricte militarne będzie prawdopodobnie ukierunkowane głównie na maskowanie termiczne, radiolokacyjne oraz radiotechniczne sprzętu i uzbrojenia wojskowego oraz będzie obejmować stosowanie makiet wyposażonych w imitatory uniemożliwiające odróżnienie ich od prawdziwego sprzętu wojskowego czy też odbijaczy kątowych w celu przeciwdziałania rozpoznaniu radiolokacyjnemu przeciwnika.

Bibliografia

Barbelet V., *Humanitariac access and local organisations in Ukraine*, London 2017, HBG Working Paper.

Blandy C.W., *Provocation, Deception, Entrapment: The Russo-Georgian Five Day War*, Swindon 2009, Defence Academy of the United Kingdom.

Cheterian V., *The August 2008 war in Georgia: from ethnic conflict to border wars*, „Central Asian Survey" 2019, nr 2, s. 155–170.

Donovan C., *Russian Operational Art In The Russo-Georgian War of 2008*, Carlisle 2009, U.S. Army War College.

Ellison B., *Russian Grand Strategy in the South Ossetia War*, „Demokratizatsiya: The Journal of Post-Soviet Democratization" 2011, nr 19, s. 343–366.

Giles K., Sherr J., House C., *Russian Reflexive Control*, Kingston 2008, Royal Military College of Canada.

Glantz D., *Soviet Military Deception in the Second World War*, New York 2005, Frank Cass.

Gołda-Sobczak M., *Krym jako przedmiot sporu ukraińsko-rosyjskiego*, Poznań 2016, Silva Rerum.

Hurak I., *Rosyjska obecność militarna oraz dyplomacja rosyjska w kontekście konfliktu na wschodzie Ukrainy*, „Wschód Europy" 2015, nr 2, s. 161–182.

Kubiak K., *Wojna w Gruzji w 2008 roku. Geneza i przebieg działań zbrojnych*, „Międzynarodowe Prawo Humanitarne" 2011, t. 2: *Konflikt rosyjsko-gruziński w 2008 r.,* s. 11–38.

Lakomy M., *Przebieg i uwarunkowania konfliktu na wschodzie Ukrainy*, w: M. Stolarczyk, M. Lakomy, K. Czornik, *Implikacje konfliktu ukraińskiego dla bezpieczeństwa Polski. Aspekty polityczne, wojskowe, gospodarcze i społeczne*, Katowice 2015, Wydawnictwo Regionalnego Ośrodka Debaty Międzynarodowej w Katowicach.

Latimer J., *Podstęp na wojnie*, Warszawa 2017, Wydawnictwo Amber.

Maskowanie operacyjne: DD-3.31(A), Bydgoszcz 2018, Centrum Doktryn i Szkolenia Sił Zbrojnych, Ministerstwo Obrony Narodowej.

Maskowanie wojsk i wojskowej infrastruktury obronnej: DD-3.20, Warszawa 2010, Sztab Generalny Wojska Polskiego, Ministerstwo Obrony Narodowej.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno- psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 11–36.

Zawadzki J., *Współczesny rozbiór państwa. Casus Gruzji*, „Nowa Polityka Wschodnia" 2011, nr 1, s. 157–172.

Literatura rosyjska

Королёв А.Ю., Королёва А.А., Яковлев А.Д., *Маскировка. Вооружения, техники и объектов*, Санкт-Петербург 2015, Университет ИТМО.

Мацуленко В.А., *Оперативная маскировка войск*, Москва 1975, Военное издательство Министерства обороны СССР.

Źródła internetowe

Amos H., *Ukraine crisis fuels secession calls in pro-Russian south*, „The Guardian", 23 II 2014 r., https://www.theguardian.com/world/2014/feb/23/ukraine-crisis-secession-russian-crimea [dostęp: 12 III 2020].

Ash L., *How Russia outfoxes its enemies*, BBC, 29 I 2015 r., https://www.bbc.com/news/magazine-31020283 [dostęp: 14 III 2020].

Bellingcat Report – Origin of Artillery Attacks on Ukrainian Military Positions in Eastern Ukraine Between 14 July 2014 and 8 August 2014, Bellingcat, 17 II 2015 r. https://www.bellingcat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/ [dostęp: 8 III 2020].

Captured Russian troops 'in Ukraine by accident', BBC, 26 VIII 2014 r., https://www.bbc.com/news/world-europe-28934213 [dostęp: 8 III 2020].

Crimea, Sevastopol officially join Russia as Putin signs final decree, RT, 21 III 2014 r., https://www.rt.com/news/russia-parliament-crimea-ratification-293/ [dostęp: 12 III 2020].

Demirjian K., Birnbaum M., *Russia escalates tensions with aid convoy, reported firing of artillery inside Ukraine*, „The Washington Post", 22 VIII 2014 r., https://www.washingtonpost.com/world/russian-humanitarian-convoy-enters-ukraine-despite-warnings/2014/8/22/7b14fa8e-29e1-11e4-8593-da634b334390_story.html [dostęp: 8 III 2020].

Direct Line with Vladimir Putin, 17 IV 2014 r., http://en.kremlin.ru/events/president/news/20796 [dostęp: 12 III 2020].

Gregory P.R., *Putin's 'Human Rights Council' Accidentally Posts Real Crimean Election Results*, „Forbes", 5 V 2014 r., https://www.forbes.com/sites/paulroderickgregory/2014/05/05/putins-human-rights-council-accidentally-posts-real-crimean-election-results-only-15-voted-for-annexation/ [dostęp: 12 III 2020].

'Maskirovka' Is Russian Secret War, War Is Boring, 26 VIII 2014 r., https://medium.com/war-is-boring/maskirovka-is-russian-secret-war-7d6a304d5fb6 [dostęp: 8 III 2020].

NATO Secretary General condemns entry of Russian convoy into Ukraine, NATO, 22 VIII 2014 r., https://www.nato.int/cps/en/natohq/news_112112.htm [dostęp: 8 III 2020].

Parfitt T., *Russia exaggerating South Ossetian death toll, says human rights group*, „The Guardian", 13 VIII 2018 r., https://www.theguardian.com/world/2008/aug/13/georgia [dostęp: 25 I 2020].

Putin reveals secrets of Russia's Crimea takeover plot, BBC, 9 III 2015 r., https://www.bbc.com/news/world-europe-31796226 [dostęp: 14 III 2020].

Radyuhin V., *Medvedev, Putin accuse Georgia of genocide*, 11 VIII 2018 r., https://www.thehindu.com/todays-paper/tp-international/Medvedev-Putin-accuse-Georgia-of-genocide/article15279050.ece [dostęp: 25 I 2020].

Rasmussen potwierdza wtargnięcie Rosjan. Hollande apeluje do Moskwy, TVN24, 15 VII 2014 r., https://tvn24.pl/swiat/rasmussen-potwierdza-wtargniecie-rosjan-hollande-apeluje-do-moskwy-ra459520-348636 [dostęp: 8 III 2020].

Reporter AP: Rosja przerzuca na Ukrainę broń w rejonie Krasnodonu, TVN24, 26 VIII 2014 r., https://tvn24.pl/swiat/reporter-ap-rosja-przerzuca-na-ukraine-bron-w-rejonie-krasnodonu-ra462025-3409862 [dostęp: 8 III 2020].

RPT-INSIGHT-How the separatists delivered Crimea to Moscow, Reuters, 13 III 2014 r., https://www.reuters.com/article/ukraine-crisis-russia-aksyonov-idINL6N0M93AH20140313?edition-redirect=in [dostęp: 12 III 2020].

Russia says cannot order Crimean 'self-defense' units back to base, Reuters, 5 III 2014 r., https://www.reuters.com/article/us-ukraine-crisis-lavrov-spain-idUSBREA240NF20140305 [dostęp: 12 III 2020].

Sabak J., *Pół dekady okupacji Krymu i wojny w Donbasie*, Defence 24, 11 III 2019 r., https://www.defence24.pl/pol-dekady-okupacji-krymu-i-wojny-w-donbasie-opinia [dostęp: 14 III 2020].

Słownik języka polskiego PWN, https://sjp.pwn.pl/sjp/maskowac;2481616.html [dostęp: 9 X 2019].

Spot report by the OSCE Observer Mission at the Russian Checkpoints Gukovo and Donetsk, 22 August 2014: Russian humanitarian aid trucks departed from the Donetsk Border Crossing Point without ICRC's escort, OSCE, 22 VIII 2014 r., https://www.osce.org/om/122927 [dostęp: 8 III 2020].

Ukraine crisis: Russia aid convoy 'invades Ukraine', BBC, 22 VIII 2014 r., https://www.bbc.com/news/world-europe-28892525 [dostęp: 8 III 2020].

Walker S., *Aid convoy stops short of border as Russian military vehicles enter Ukraine*, „The Guardian", 15 VIII 2014 r., https://www.theguardian.com/world/2014/aug/14/russian-military-vehicles-enter-ukraine-aid-convoy-stops-short-border [dostęp: 8 III 2020].

Rosyjskie i ukraińskie źródła internetowe

Денисенко В., *Стратегическая маскировка как образ российской политической жизни*, ИноСМИ.RU, 26 VI 2015 r., https://inosmi.ru/russia/20150626/228788387.html [dostęp: 30 X 2019].

Как готовилась война, „Новая газета", 27 VI 2009 r., https://novayagazeta.ru/articles/2009/06/28/42316-kak-gotovilas-voyna [dostęp: 10 II 2020].

Классификация и способы маскировки, http://red-tent.ru/mask/maskirovka [dostęp: 31 X 2019].

Марущенко П., *Идею введения противника в заблуждение необходимо формировать путем группирования отдельных мер обмана противника по выбранным признакам*, Бюро военно-политического анализа, 23 III 2018 r., http://bvpa.ru/обман-противника-процесс-творчески/ [dostęp: 20 XI 2019].

Маскировка, https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=13494 [dostęp: 30 X 2019].

Медведев разъяснил Саакашвили задачи железнодорожных войск России в Абхазии, NEWSru.com, 3 VI 2008 r., http://palm.newsru.com/russia/03jun2008/medsaak.html [dostęp: 10 II 2020].

Международное сотрудничество, МЧС России, https://www.mchs.gov.ru/deyatelnost/mezhdunarodnoe-sotrudnichestvo [dostęp: 8 III 2020].

Монетчиков С., *Маскировка. Искусство быть невидимым*, 8 VI 2013 r., https://topwar.ru/30425-maskirovka-iskusstvo-byt-nevidimym.html [dostęp: 23 X 2019].

Оперативная маскировка, Студопедия, 11 III 2015 r., https://studopedia.info/2-14013.html [dostęp: 30 X 2019].

Премьер-министр Крыма попросил Путина о помощи, Тасс, 1 III 2014 r.; https://tass.ru/mezhdunarodnaya-panorama/1013127 [dostęp: 12 III 2020].

Путин: Россия не планировала присоединять Крым, Тасс, 10 IV 2014 r., https://tass.ru/politika/1111359 [dostęp: 14 III 2020].

Росія збільшила свій контингент в Криму до 16 тисяч військовослужбовців – Тенюх, УНІАН, 4 III 2014 r., https://www.unian.ua/politics/892512-rosiya-zbilshila-sviy-kontingent-v-krimu-do-16-tisyach-viyskovoslujbovtsiv-tenyuh.html [dostęp: 12 I 2020].

Ручкин В., *Вирус вождизма*, „Красная звезда", 13 VIII 2018 r., http://old.redstar.ru/2008/8/13_8/4_06.html [dostęp: 10 II 2020].

Стратегическая маскировка и дезинформация, http://politike.ru/termin/strategicheskaja-maskirovka-i-dezinformacija.html [dostęp: 30 X 2019].

Шляхов В., *Референдум в Крыму: ответ «нет» не предусмотрен,* „Голос Америки", 12 III 2014 r., https://www.golosameriki.com/a/world-ukraine-crisis-referendum/1869197.html [dostęp: 12 III 2020].

В Крыму находятся российские военнослужащие не только из частей ЧФ РФ, утверждают в Генштабе ВСУ, Интерфакс, 4 III 2014 r., https://interfax.com.ua/news/general/194412.html [dostęp: 12 III 2020].

Владимир Путин внёс обращение в Совет Федерации, 1 III 2014 r., http://www.kremlin.ru/events/president/news/20353#sel=2:17:t6V,2:25:991 [dostęp: 12 III 2020].

Abstrakt

Celem artykułu było przedstawienie charakterystyki maskowania operacyjnego stosowanego przez Siły Zbrojne Federacji Rosyjskiej oraz poszerzenie wiedzy na temat ewoluowania działań, w których stosuje się maskirowkę. Szczególną uwagę poświęcono przykładom jej wykorzystania we współczesnych wojnach i konfliktach zbrojnych – przede wszystkim w konflikcie na Ukrainie oraz w wojnie pięciodniowej w Gruzji. Na podstawie przeprowadzonej analizy wskazano tendencje dotyczące posługiwania się maskirowką we współczesnych i przyszłych konfliktach oraz działaniach innych niż wojenne.

Wynika z niej, że maskirowka będzie coraz częściej wykorzystywana do osiągania celów strategicznych oraz kształtowania opinii międzynarodowej. Jednym z najważniejszych obszarów jej stosowania stanie się cyberprzestrzeń, umożliwiająca skuteczniejsze prowadzenie działań dezinformacyjnych i propagandowych, w tym wojny informacyjnej. Ze względu na dynamiczny rozwój technologii, jak również potencjał Sił Zbrojnych Federacji Rosyjskiej do działań z zakresu maskowania operacyjnego należy kontynuować badania dotyczące maskirowki.

Słowa kluczowe: maskowanie, maskowanie operacyjne, dezinformacja, ukrywanie, pozorowanie, imitacja, maskirowka, Siły Zbrojne Federacji Rosyjskiej, wojna w Gruzji, konflikt na Ukrainie.

Operational deception (Maskirovka) as a Russian capability to surprise the enemy

Abstract

The aim of the article was to present the characteristics of operational deception used by the Armed Forces of the Russian Federation and to broaden the understanding of the evolution of operations using Maskirovka. Particular attention was paid to examples of its use in contemporary wars and armed conflicts - primarily in the conflict in Ukraine and in the Five-Day War in Georgia. The analysis led to an identification of trends regarding the use of deception in contemporary and future conflicts and activities other than war. It shows that the maskirovka will be increasingly used to achieve strategic goals and shape international opinion. One of the most important areas of its application will be cyberspace, enabling more effective disinformation and propaganda activities, including information warfare. Considering the dynamic development of technology and capabilities of the Armed Forces of the Russian Federation in the field of operational masking, it is justified to conduct further research in the Maskirovka area.

Keywords: deception, operational deception, disinformation, concealment, simulation, imitation, Maskirovka, The Armed Forces of the Russian Federation, War in Georgia, Conflict in Ukraine.

IV

WYBRANE ARTYKUŁY W JĘZYKU ANGIELSKIM

SELECTED ARTICLES IN ENGLISH

ŁUKASZ SKONECZNY
ORCID: 0000-0003-1612-0915

BOGUSŁAW CACKO
ORCID: 0000-0002-6496-7005

DOI: 10.4467/20801335PBW.21.032.14309

Sharp power – introduction to the issue

Since the development of the first Greek polis, political communities have sought effective tools to influence both their enemies and allies. The result of this centuries-old experience is the emergence of many models of state power in relation with other entities on the international arena. This article focuses on presenting a new kind of state power, namely *sharp power*. An attempt was made to define this phenomenon, present its characteristic manifestations. Moreover, methods to mitigate its negative effects on the security of the Republic of Poland were proposed.

The authors' analysis of the issue related to the state power and its various forms leads to a hypothesis that we are currently witnessing the formation of another type of influence of political regimes on entities of international relations, combining elements of coercion and manipulation. Such a policy defies classification into the categories known so far namely hard, soft and smart power.

There are many different definitions of a state power.[1] The one by John G. Stoessinger is considered classic. According to the American researcher, this term means "(...) the ability of a state to use its resources(...) in a way that will influence the behaviour of other states".[2] This way of understanding, despite being generic, indicates the need for political elites to have an economic, ideological or cultural base that will constitute the foundation for effective influence on other states. At the same time, the author of the aforementioned definition assumes the need for decision-makers to have in-depth knowledge of the possibilities of influencing the activity of other entities

[1] The authors of the article do not analyse the works to date in the theory of state power and its various forms. They only present the most representative theories.

[2] J.G. Stoessinger, *The Might of Nations. World Politics in Our Times*, New York 1969, pp. 26–27.

of international relations. It is worth noting that Stoessinger did not specify what exactly do "resources influencing other states" imply. This lack of precision resulted in the widespread use of the terms soft power and hard power in the literature on the subject. These terms were coined by the American Joseph S. Nye, author of numerous publications on security and international politics. The concept of soft power was to be a response of Western countries to the military threat posed by the USSR. The American scientist came to the conclusion, modifying the earlier idea of Zbigniew Brzeziński, who compared the international policy to the game of chess,[3] that international competition is currently conducted on three planes simultaneously. Namely, military power, economic power and soft power, i.e. the ability to shape the preferences of other entities of international relations.[4] The deployment of soft power is identified mainly with democratic states. Simply put, it is about encouraging - by means of persuasion – the participants in international relations to accept the actions of a given country. According to Nye, a country's soft power rests on three types of resources: its culture, its political values and the foreign policies it implements.[5]

The cultural factor is linked in this case with the attractiveness of the culture of a given country, which is manifested, inter alia, in the held onto and promoted universal values. This does not mean, however, that one can equate soft power with mass culture, which is one of the possible ways of transmitting ideas. For this reason, this aspect of impact should be considered more broadly and include, for example, scientific exchange or business cooperation.[6] Regarding the other two elements of soft power, Nye wrote: "(...) domestic or foreign policies that appear hypocritical, arrogant, indifferent to others' views, or based on a narrow conception of national interests can undermine soft power (…) Government can attract or repel by the influence of its example."[7] Yet it should be emphasized that any attempts by the political regime to take full control of soft power will face serious obstacles - especially in the liberal democracy. This is due to the fact that a large part of soft power is dispersed among various types of social entities (media, NGOs, entertainment industry, artistic environment, etc.) which remain beyond the reach of the authorities.[8]

The opposite of soft power strategy is hard power. Nye defined hard power as the potential resulting from geopolitical and economic factors.[9] It focuses on incentives and threats to use force in international relations. Thus, in this strategy there is no question of an indirect influence through culture or values, but rather of exerting an

---

3 See Z. Brzeziński, *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*, New York 1997.

4 J.S. Nye Jr., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007, pp. 33–34.

5 Ibid., p. 40.

6 Ibid., p. 41.

7 Ibid., pp. 43–44.

8 Ibid., p. 44.

9 Ibid., p. 34.

actual influence on others. For this reason, hard power remains mainly the domain of authoritarian regimes whose institutional and legal solutions as well as the values promoted are not attractive to other countries. It should also be noted that soft power and hard power sometimes enhance each other, but sometimes they collide with each other. However, it cannot be clearly indicated which of the above-mentioned approaches is more effective. Analysing these issues, Nye advanced the thesis that it is possible to combine the effectiveness of actions on the international scene with the ability to benefit from both strategies. Such an approach resulted in the development of the concept of smart power.

Smart power should be understood as the effective integration of soft and hard power elements.[10] This strategy requires the decision-makers to be skilful in using the available foreign policy instruments, adapted both to the existing international situation and the possessed potential for action. This applies in particular to the ability to adapt to current events, coordination of activities between individual state institutions (including a clear demarcation of their competences), the existence of an efficient information flow and appropriate procedures for reacting to potential problems.[11]

What is sharp power?

The end of the Cold War and, above all, the Ukrainian conflict that started in 2014 revealed a new trend in the methods and measures used by countries to pursue their interests in the international community. These activities defy traditional classification into hard power and soft power strategies. American researchers Christopher Walker and Jessica Ludwig were the first to notice this in 2017 in the article "The meaning of sharp power. How authoritarian states project influence."[12] In their publication, they indicated the growing activity of authoritarian countries on the international scene, which differs from the activities hitherto described by Western countries as elements of soft power. Its aim is not to increase the attractiveness of one's own image, but to manipulate public moods - especially in terms of perceiving the values characteristic of a democratic state of law. American researchers coined the term sharp power, which means penetrating the information and political environment of a selected country in order to discredit it in the eyes of the national and foreign public opinion. (The original quote reads: "Authoritarian influence efforts are 'sharp' in the sense that they pierce, penetrate, or perforate the political and information environments in the targeted

[10] *CSIS Commision on smart power: a smarter, more secure America*, R.L. Armitage, J.S. Nye Jr. (ed.), Washington 2007, p. 7.

[11] J. Sadłocha, "Pomiędzy miękką a twardą siłą: smart power", *Wrocławskie Studia Politologiczne* 2012, vol. 13, pp. 38–40.

[12] Ch. Walker, J. Ludwig, "The meaning of sharp power. How authoritarian states project influence", *Foreign Affairs*, 16 XI 2017, foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power [access: 14 VI 2021].

countries.")[13] In the opinion of the authors of the discussed article, examples of authoritarian regimes using sharp power are the Russian Federation and the People's Republic of China. The purpose of their activity is not to "win the hearts and minds" but to induce or fuel animosity among the citizens of Western countries. At the same time, Walker and Ludwig draw attention to the lack of adequate defence mechanisms of the West against the actions taken by authoritarian regimes. The researchers postulate, first of all, to expose hostile information operations and to raise public awareness of this.[14] An important contribution to the sharp power discourse is another article by Nye, namely "How sharp power threatens soft power. The right and wrong ways to respond to authoritarian influence."[15] It was a response to a publication by Walker and Ludwig. In the opinion of the American scientist, sharp power is not a previously unknown phenomenon. In his opinion, it is a new term for information warfare. Nye additionally observes that sharp power is not an activity that is unique to authoritarian regimes. This strategy is also used by democratic countries, an example of which was the US policy towards the USSR during the Cold War. Moreover, the American political scientist warns the West against trying to use sharp power against authoritarian regimes. It puts Western democracies at risk of losing their credibility and lowering their own soft power potential. Therefore, according to Nye, the most important thing in counteracting sharp power is that liberal democracies maintain relative openness in their contacts with autocratic states. In this context, primarily civil society institutions have an important role to play (including the mass media, academia, non-governmental organizations), which should disseminate knowledge about information warfare techniques.

There are also critical opinions in the debate devoted to sharp power. The author of one of them is Xin Liu, who in the article "What sharp power? It's nothing but 'unsmart' power" disagrees with Walker and Nye's viewpoint that it is a completely qualitatively new phenomenon.[16] In her mind, sharp power is the result of unsuccessful implementation of smart power, i.e. unskilled combination of soft and hard power elements.

Summarizing the perceptions on sharp power so far, it should be stated that the view according to which this is purely a new term, defining an already recognised threat, which is information warfare, may raise serious doubts. It is true that information manipulation is the main component of sharp power, but it is not the only tool used in this strategy. Later in the article, other methods of this concept will be discussed, which are not only limited to moves made in the information space.

---

[13] Ibid.

[14] Ibid.

[15] J.S. Nye Jr., "How sharp power threatens soft power. The right and wrong ways to respond to authoritarian influence", *Foreign Affairs*, 24 I 2018, foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power [access: 14 VI 2021].

[16] Xin Liu, "What sharp power? It's nothing but 'unsmart' power", *USC Center on Public Diplomacy*, 15 XI 2018, uscpublicdiplomacy.org/blog/what-sharp-power-it's-nothing-"unsmart"-power [access: 10 V 2021].

One should agree with Nye's stance that sharp power is not the exclusive domain of authoritarian regimes. As the American scientist rightly pointed out, this strategy is also used by the democratic authorities. However, it is worth considering why countries with authoritarian tendencies decide more on this strategy. According to the authors of this article the nature of the liberal socio-political system bears the greatest significance. Its openness is used by authoritarian regimes to carry out sharp power intrusions. Openness should be understood as such features of liberal democracy as: freedom of speech, free media market, political pluralism, meaning the possibility of establishing political parties not under the influence of authorities, the existence of an independent sector of non-governmental organizations, etc. Due to the lack of these elements or their strict supervision in autocratic regimes, governments in democratic countries have significantly limited opportunities to undertake similar sharp power initiatives. An additional factor preventing liberal democracies from applying this strategy is the fear of sparking off a serious political crisis. Supposing the mass media discloses such activities carried out by a democratic government it could cause strong public criticism of the authorities and in an extreme case even necessitate snap elections.

To sum up, sharp power can therefore be defined as **aggressive actions of the state carried out with the use of methods imitating soft power elements in order to manipulate the image of a given country (or other entities of international relations) or to destabilize its socio-political system, or to force certain actions by its authorities.**[17]

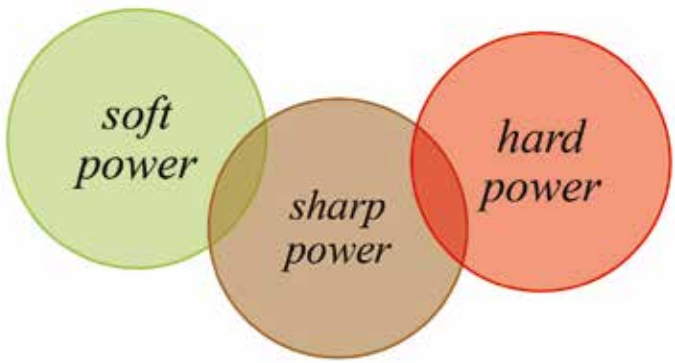


Fig. 1. The position of sharp power with regard to soft power and hard power.

Source: Own elaboration.

[17] Extracts in bold have been highlighted by the authors (ed.).

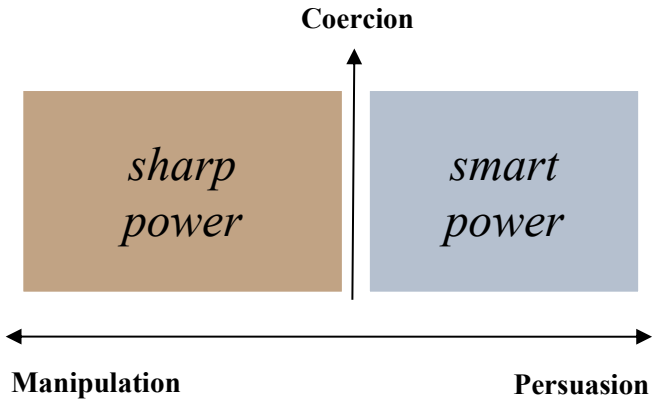


Fig. 2. The position of sharp power with regard to smart power.

Source: Own elaboration.

Methods of exercising sharp power

Countries use various economic, political, military and diplomatic instruments characteristic of soft and hard power to pursue sharp power strategy. The list presented below is not a complete catalogue. However, these methods are currently predominantly chosen by countries that decide to undertake this type of action.

Information warfare

The basic method used within sharp power is information warfare. Its major significance is connected with the global revolution of information and communication technology and the development of network societies. The result of these processes is a rapid increase in the role of the Internet in gaining information and in interpersonal communication. Information warfare makes it possible to reach a large audience with a specific message (e.g. via social media, online television and message board). At the same time, the aggressor remains anonymous (due to the multitude of entities operating in the information space, it is difficult to indicate the true author). Moreover, it allows to conceal the real intentions of the sender under the guise of providing reliable data or a different point of view on a specific topic. An important feature of information warfare is also the relatively low cost of its waging (this is related, inter alia, to the fact that currently the main area of information warfare is the Internet). Additionally, it constitutes the main backing for other activities used within sharp power, significantly increasing their effectiveness.

In this article, the authors adopt the definition of information warfare formulated by Robert Rajczyk, as a long-term, multistranded communication process, the purpose of which is to gain an information advantage over the opponent, e.g. by influencing national and foreign public opinion, lowering morale and cultivating conformism among a hostile society, as well as exercising public diplomacy.[18]

The term "information warfare" should be understood broadly. It does not mean generating propaganda and disinformation only during an armed conflict, but may also include aggressive informational undertakings carried out during peace time.[19] Information warfare might involve:

- making public (e.g. via WikiLeaks copycat websites) sensitive information, captured from private PCs and mobile phones belonging to politicians, government or military officials, and officers of uniformed services;
- conducting disinformation activities on the Internet, e.g. on social networking sites by fictitious groups of users (so-called trolls);
- using agents of influence to manipulate the views of political decision-makers, pressure groups and opinion-makers;
- creating media (radio, television, newspapers, web portals) friendly to the manipulating country;
- projecting a negative image of a given country by the mass media of the manipulating country (including the mass media of neighbouring countries for the purpose of hostile information activities);
- blocking state websites or replacing published content;
- discrediting the ideology, social values or system of governing solutions functioning in a given country;
- destroying optical-fiber or telecommunications networks in order to prevent the transmission of information.

Since the Ukrainian crisis which began in 2014, the information warfare waged by the Russian Federation towards the countries of Central and Eastern Europe, including Poland, has been escalating. Russia's main goals include creating a negative image of the region and inflaming tensions in its relations with partners from the European Union and the North Atlantic Alliance. Poland, as a close ally of the USA and an important member of the EU and NATO, is perceived by the Kremlin as one of the key masterminds of international initiatives aimed against the interests of the Russian Federation. Moscow may engage pro-Russian Polish journalists, scientists, politicians and social activists in information campaigns directed against the Republic of Poland. In addition, Moscow benefits from the support of entities responsible for promoting Russia's interests abroad, as well as representing the Russian minority.

---

[18] See R. Rajczyk, *Nowoczesne wojny informacyjne*, Warszawa 2016, p. 29.

[19] For more on the differences in defining information warfare by NATO and by the Russian side, see K. Giles, *Handbook of Russia information warfare*, Rome 2016, pp. 3–13.

Providing support to political entities and social organizations that fit into the sharp power strategy of the manipulator-state

Another important sharp power objective is to support the activity of political organizations and social environments that lobby for the manipulator-state or that may destabilize the situation in a given country. The most frequently used methods include:

- **multidirectional pressure** - consisting in exerting political, economic, military or diplomatic pressure on the authorities of a given country in order to force them to make concessions to entities acting in the interest of the manipulator-state (this may include introducing legal solutions favourable to the activity of such organizations, e.g. entry in the register of political parties);
- **economic aid** - including both legal and bound by law possibilities of supporting such entities (e.g. donations, research grants, real estate rental), as well as illegal methods used by the manipulator-state. Most often - as in the case of money laundering crime - they involve the use of straw persons, i.e. natural or legal persons who are to cover the real origin of financial resources. In order to make it impossible to trace the sources of financing, accounts are also often created in banks operating in the territory of the manipulator-state, in which money is transferred to a given entity and then paid by its representatives;
- **propaganda and disinformation activity** - i.e. all information activities carried out by the manipulator-state in order to create positive opinions about the supported entity or discredit the image of the authorities of the country in which it operates (e.g. information campaigns on the Internet, black PR, maintaining official contacts by diplomatic representatives of the manipulator-state with the given entity).

An example of a type of sharp power discussed above could be the information indicating that Russia and China might have been supporting Catalan separatists. According to media reports, the Spanish police were to investigate the involvement of Russian intelligence in inspiring Catalan nationalists to protest and resist the central government in Madrid. An officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU) was to contact Victor Terradellas in 2017, who, as an advisor to the then Prime Minister of Catalonia, Carles Puigdemont, exerted pressure on him to proclaim independence by this region. On the basis of digital correspondence, the Spanish law enforcement agencies were to establish that Terradellas assured the Catalan politician of Vladimir Putin's support and of the possibility of granting financial aid allegedly promised by China.[20] The aim of Russia's actions might have been an attempt to destabilize the situation inside the EU, which would indirectly weaken its position in relations with Russia.

[20] M. Kucharczyk, "Czy Rosja wspierała katalońskich niepodległościowców?", *Euractiv*, 28 XI 2011, euractiv.pl/section/demokracja/news/czy-rosja-wspierala-katalonskich-niepodlegloscowcow [access: 15 V 2021].

History politics

Sharp power strategy employs more and more often history politics. Yet, it is not solely about the promotion of a certain vision of history by the authorities of a given country, as historical issues have always been used for political games on the international arena. In the case of sharp power, politics of history does not involve popularization of a specific interpretation of history, but its deliberate falsification and denial of facts that are commonly accepted in historiography.

An example of this type of activity is the present history politics of the Russian Federation concerning the outbreak and the events of World War II. One of its elements is the so-called "monument war" waged against Poland. The pretext for starting it by Moscow was the introduction of the so-called decommunization act by the Polish parliament on 1 April 2016, especially its amendment from June 2017. As a consequence of these resolutions, Russia accuses Poland of destroying the cemeteries of Soviet soldiers who fought with Nazi Germany during World War II. The Kremlin's goal is to slander the image of the Republic of Poland in the eyes of international opinion, which results in the loss of credibility of the authorities in Warsaw and the weakening of the unity of NATO and the EU. It is also about increasing hostility towards Poland among the Russian society. The reason for this animosity is the alleged lack of gratitude of the Polish nation for the sacrifices made by the Russians during the liberation of our country from German occupation.

Another priority of the Russian politics of history is the attempt to attribute the responsibility for the outbreak of World War II to Poland. In this context, the Russian side points to the allegedly pugnacious policy of the Republic of Poland between 1918 and 1939 and the refusal of the Polish authorities to cooperate with the USSR. Simultaneously, it diminishes the role of the Ribbentrop-Molotov Pact in defining the Soviet and Nazi spheres of influence in Central and Eastern Europe. Moreover, the Kremlin holds Poland responsible for the Holocaust. The Russian side considers an argument which supports the later stance is the fact that the German extermination camps were built in the occupied territory of the Polish Republic by the Third Reich. All these examples serve to whitewash the history of the USSR and at the same time create a negative image of Poland as a Nazi and anti-Semitic country.[21]

Manipulation of the conduct and outcome of elections in a given country

An important tool of the sharp power strategy is to convince the citizens of a given country that the political regime in power is deprived of adequate social legitimacy.

[21] For more on the topic of Russian politics of history, see J. Darczewska, "'Wojny pamięci': historia, polityka i służby specjalne Federacji Rosyjskiej", *Przegląd Bezpieczeństwa Wewnętrznego* 2019, no. 11, pp. 13–41.

The most effective method of achieving this goal is to undermine the credibility of the election process itself and to convince people that its outcomes were fabricated. Such activities may include, inter alia, mass dissemination of fake news regarding the interference of a foreign country in the election process, anomalies in the vote count, etc. The manipulator state may also, for example, inspire social protests denying the results of the presidential or parliamentary elections.

Direct influence on the outcome of elections, is also possible e.g. by means of actions targeted at specific candidates or political parties. These may include:

- cyberattacks targeting election infrastructure with the aim of tampering with the number of votes cast;
- using the so-called proxies (e.g. NGOs) which disseminate critical opinions about specific candidates or political parties;
- spreading fake news on the Internet (social media, message board, news portals);
- media attacks carried out by the mass media of the manipulator-state.

The presidential campaign in the USA in 2016 might be an example of interference in the election process, which is an element of the sharp power strategy. There are indications that Russia was trying to create a negative media coverage about the American political system, undermining the credibility of Hillary Clinton - the Democratic party presidential candidate and to support Donald Trump in achieving victory.[22]

Scientific cooperation

Scientific cooperation is another tool used by countries to pursue sharp power strategy. Most often it will be used to perform influence operations in the academic environment of a given country. The strategic goal is to create an expert lobby which will promote the interests of the manipulator-state, e.g. among representatives of the political elite, or to publicly criticize the actions taken by state authorities. The implementation of this plan may consist in organizing study trips to the manipulator-state or awarding scholarships for young people and university employees. In this way, future agents of influence can be selected who after having achieved social and professional position can be used to manipulate the views of opinion-leading environments.

Another example of such pursuit might be the invitation of representatives of academia to participate in cultural and scientific events with undertones of propaganda. They can be organized by the manipulator-state both abroad and in the territory of the country being the target of foreign sharp power. The invited guests include politicians, scientists and social activists who make provocative speeches. These types of events are then used as part of the information warfare. It should be noted that

[22] Cf.: R.S. Mueller, III, "Report on the investigation into Russian interference in the 2016 presidential election", *U.S. Department of Justice*, vol. 1–2, Washington 2019.

the representatives of the scientific community invited to such events are often unaware of their real purpose.

The manipulator-state may also invite scientists of a given country to participate in controversial scientific projects, concerning, for example, history, the political situation in the world, membership in international organizations. In exchange for the attendance scholars might be offered attractive compensation or assistance in conducting research (including access to archives of documents located in the territory of the manipulator-state). The aim of this type of initiatives is to question the foreign and internal policy of a selected country or increase tensions in its relations with neighbouring countries.

The system of research grants might be another objective of sharp power strategy. Entities (e.g. state-owned foundations and enterprises, private donors) associated with the manipulator-state may obtain, in return for financial support, the possibility of locating their representatives, e.g. on supervisory boards and boards of universities or research institutes in a given country. In this way, they gain the opportunity to decide, for example, on the research projects carried out by them. In order to prevent the loss of funding, the scientific institutions subsidized in this way might intend to avoid taking initiatives incompatible with the interests of the manipulator-state or engaging in undertakings that are unfavourable for.[23]

International economic undertakings

Sharp power also involves international initiatives which - under the guise of ensuring economic benefits to the participating countries - destabilize the political situation in a given region and subordinate its economy to the manipulator-state. Examples of such activities include the Russian Nord Stream 2 and the Chinese New Silk Road.

The aim of the gas investment implemented by the Kremlin is, apart from bypassing the territory of transit countries (including Poland, Ukraine, the Baltic states), to undermine the EU's energy policy in the field of solidarity and cooperation between EU countries, and to increase tension in relations between the Federal Republic of Germany and the countries of Central and Eastern Europe. It should be noted that, in the opinion of many economists, the construction of one more gas connection to Germany is unprofitable for Gazprom and its shareholders.[24]

The New Silk Road project promoted by Beijing, i.e. a network of transport infrastructure enabling relatively fast trade between China and Europe, is of a similar

---

[23] For more examples of using scientific cooperation as a sharp power tool, see: A. Foxall, "Russian sharp power in European academia", in: *The Art of Deceit: How China and Russia Use Sharp Power to Subvert the West*, A. Foxall, J. Hemmings (ed.), London 2019, pp. 31–35.

[24] See A. Becker, "Nord Stream 2 w oczach niemieckich ekspertów: 'Zbędny, szkodliwy, nierentowny'", *Deutsche Welle*, 10 IX 2020, dw.com/pl/nord-stream-2-w-oczach-niemieckich-ekspertów-zbędny-szkodliwy-nierentowny/a-54870406 [access: 23 VI 2021]; J. Rutkowski, "Nord Stram 2 – wszystko przemawia przeciw temu projektowi", *Forsal*, 27 II 2021, forsal.pl/gospodarka/artykuly/8106480,nord-stream-2-wszystko-przemawia-przeciw-temu-projektowi.html [access: 23 VI 2021].

nature. The aim of this initiative is to strengthen China's geopolitical position in the world, as well as to create a pro-China lobby among EU members, which will have the task of influencing the politics of Brussels in line with Beijing's expectations in return for the possible benefits of this venture. As early as in 2012, China made the first attempt to create a group of favourable states in the Central European region under the format of the "16 + 1 Initiative" (now "17 + 1", since Greece joined in 2019). However, the attempt turned out to be ineffective due to, inter alia, absence of serious economic offers from Beijing for its participants.

Hybrid conflict

The last and, at the same time, the most aggressive method the state may decide to use within the sharp power strategy, is the hybrid conflict. This concept denotes a crisis situation in which one of the parties (the state or non-state actors) refrains from using the armed forces directly and undertakes other means of influencing the opponent, i.e. economic, political, diplomatic, or military. Moreover, a characteristic feature of a hybrid conflict is the inability to identify the aggressor precisely, thus declaring a formal state of war (the so-called aggression below the threshold of war).[25]

The ability to conduct a hybrid conflict effectively is the highest form of exercising sharp power, which means that a given country achieves the maximum potential in this area. The hybrid conflict is the result of the synergy effect, obtained through the skilful use of particular methods of sharp power, appropriate coordination of the activities of state institutions, and the ability to adapt to the dynamically changing international environment. An example of this type of threat is Russia's policy towards Ukraine that has been pursued since 2014 which through territorial destabilization and disintegration keeps Ukraine under Russian influence and prevents its integration with NATO and the EU.

How to counter sharp power?

An important issue related to the problem of sharp power is the development by the state authorities of an appropriate strategy that would effectively prevent the negative effects of such actions. This is especially important in the case of liberal democracies, including Poland, which - as mentioned earlier - are particularly susceptible to this type of activity on the part of authoritarian states.

Increasing public awareness of the risks related to information manipulation on the Internet should be first priority of the protection strategy. The efforts of

[25] See Ł. Skoneczny, "Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia", *Przegląd Bezpieczeństwa Wewnętrznego* 2015, special edition, pp. 39–50.

private individuals or public benefit organizations to disseminate knowledge about disinformation and unmask fake information should be viewed positively. An example from Poland worth mentioning is the initiative called "Rosyjska V kolumna w Polsce" (Russian fifth column in Poland)[26] or the activity of the Center for Propaganda Analysis and Disinformation. These are, however, insufficient actions, and the magnitude of the problem requires the involvement of the state. This means the need to establish an entity responsible for programming, supervising, analysing, and coordinating the activities of state institutions in the field of counteracting hostile information operations aimed at discrediting the image and international position of the Republic of Poland. Currently, these tasks are scattered among various state authorities, which has a negative impact on the effectiveness of their undertaking. It also gives rise to the hazard of power disputes and duplication of tasks.

The possibility of introducing legislative solutions modelled on the American law from 1938 on the Foreign Agents Registration Act (FARA) should also be considered. It regulates the activity of entities operating under the authority of a foreign principal, which may involve, including:

- participation in various initiatives of a political nature;
- acting as a political advisor, PR consultant, information services employee;
- granting financial loans or other types of material resources;
- representing a foreign principal in front of US government institutions.

The primary goal of FARA is to identify foreign influences in the United States and the resulting threats to the national security. The act is also intended to provide the American authorities with a possibility to determine whether the given information does not constitute an attempt to influence American public opinion by other countries. It is worth mentioning that, on the basis of the provisions of this legal act, the Russian television RT and the Sputnik news agency were entered into the register of foreign agents in November 2017. These entities were also obliged, inter alia, to inform recipients that they are operating as foreign agents, and to provide the US Department of Justice with data on their funding sources.

It is also important that democratic states adopt effective measures against autocratic regimes that use sharp power. On the one hand, liberal democracies must intensify their influence on the societies of these countries by means of soft power (e.g. by organizing mass programs of scientific and cultural exchange, facilitating travel, promoting democratic values, etc.). On the other hand, they should limit the possibility of spreading fake news and undermining trust in a democratic state of law. In this context, perhaps it is worth considering the solution adopted by the Latvian authorities, which in February 2021 decided to ban Russia- RTR television for one year due to inciting hatred. Participants in a current affairs program aired on RTR

[26] *Rosyjska V kolumna w Polsce* is a Facebook profile administered by a blogger Marcin Rey where he presents the activities of pro-Russian environments in Poland (ed.).

channel described Ukraine as a terrorist state and called for the Russian troops to enter its territory.[27]

To sum up, the problem of counteracting sharp power efficiently will become increasingly vital, especially in the globalizing world. This means, as indicated above, the necessity for the state authorities to undertake, above all, appropriate educational and legislative measures. At the same time, the governments of democratic countries cannot passively observe attempts to destabilize their socio-political systems, but must launch initiatives aimed at counteracting this type of aggression.

Bibliography

Brzeziński Z., *The grand chessboard: American primacy and its geostrategic imperatives*, New York 1997, Basic Books.

CSIS Commision on Smart Power: A smarter, more secure America, R.L. Armitage, J.S. Nye Jr. (ed.), Washington 2007, Center for Strategic & International Studies.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, Ośrodek Studiów Wschodnich.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, Ośrodek Studiów Wschodnich.

Darczewska J., "'Wojny pamięci': historia, polityka i służby specjalne Federacji Rosyjskiej", *Przegląd Bezpieczeństwa Wewnętrznego* 2019, no. 20, pp. 13–41.

Gallarotti G., "Soft power: what it is, why it's important, and the conditions under which it can be effectively used", *Journal of Political Power* 2011, no. 1, pp. 25–47.

Giles K., *Handbook of Russia information warfare*, Rome 2016, NATO Defense College.

Krzak A., "Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego", *Przegląd Bezpieczeństwa Wewnętrznego* 2018, no. 18, pp. 11–39.

Kuźniar R., *Polityka i siła. Studia strategiczne – zarys problematyki*, Warszawa 2005, Scholar.

Materski W., "Polityka historyczna Federacji Rosyjskiej po 2000 r.", *Dzieje Najnowsze* 2014, no. 4, pp. 93–115.

Mueller R.S., III, *Report on the investigation into Russian interference in the 2016 presidential election,* U.S. Department of Justice*,* vol. 1–2, Washington 2019.

Nye J.S. Jr., *Bound to lead. The changing nature of American power*, New York 1991, Basic Books.

Nye J.S. Jr., *Przyszłość siły*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Nye J.S. Jr., *Soft Power. Jak osiągnąć sukces w polityce światowej*, Warszawa 2007, Wydawnictwa

[27] See "Łotwa zakazała na rok emisji rosyjskiej telewizji państwowej 'Rosja RTR'", *Studium Europy Wschodniej* UW, 9 II 2021, studium.uw.edu.pl/lotwa-zakazala-na-rok-emisji-rosyjskiej-telewizji-panstwowej-rosja-rtr/ [access: 11 VI 2021].

Akademickie i Profesjonalne.

Rajczyk R., *Nowoczesne wojny informacyjne*, Warszawa 2016, Difin.

Sadłocha J., "Pomiędzy miękką a twardą siłą: smart power", *Wrocławskie Studia Politologiczne* 2012, vol. 13, pp. 37–46.

Skoneczny Ł., "Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia", *Przegląd Bezpieczeństwa Wewnętrznego* 2015, special edition, pp. 39–50.

Stoessinger J.G., *The Might of Nation. World Politics in Our Times*, New York 1969, Random House.

The Art of Deceit: How China and Russia Use Sharp Power to Subvert the West, A. Foxall, J. Hemmings (ed.), London 2019, The Henry Jackson Society.

Tomaszewska P., Pohl A., "Dylematy związane z uczestnictwem Polski w chińskiej inicjatywie Belt and Road", *Przegląd Strategiczny* 2019, no. 12.

Tromblay D.E., *Political Influence Operations: How Foreign Actors Seek to Shape US Policy Making*, Lanham–Boulder–London–New York 2018, Rowman and Littlefield.

Walker Ch., "What Is 'Sharp Power'?", *Journal of Democracy* 2018, no. 3, pp. 9–23.

Internet sources

Becker A., "Nord Stream 2 w oczach niemieckich ekspertów: 'Zbędny, szkodliwy, nierentowny'", *Deutsche Welle*, 10 IX 2020, dw.com/pl/nord-stream-2-w-oczach-niemieckich-ekspertów-zbędny-szkodliwy-nierentowny/a-54870406 [access: 23 VI 2021].

Kucharczyk M., "Czy Rosja wspierała katalońskich niepodległościowców?", *Euractiv*, 28 XI 2011, euractiv.pl/section/demokracja/news/czy-rosja-wspierala-katalonskich-niepodlegloscowcow [access: 15 V 2021].

Liu Xin, "What Sharp power? It's nothing but 'unsmart' power", *USC Center on Public Diplomacy*, 15 XI 2018, uscpublicdiplomacy.org/blog/what-sharp-power-it's-nothing-"unsmart"-power [access: 10 V 2021].

"Łotwa zakazała na rok emisji rosyjskiej telewizji państwowej 'Rosja RTR'", *Studium Europy Wschodniej UW*, 9 II 2021, studium.uw.edu.pl/lotwa-zakazala-na-rok-emisji-rosyjskiej-telewizji-panstwowej-rosja-rtr/ [access: 11 VI 2021].

Nye J.S. Jr., "How sharp power threatens soft power. The right and wrong ways to respond to authoritarian influence", *Foreign Affairs*, 24 I 2018, foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power [access: 14 VI 2021].

Przychodniak M., "Chiny wobec kryzysu inicjatywy 17+1", *Polski Instytut Spraw Międzynarodowych,* pism.pl/publikacje/Chiny_wobec_kryzysu_inicjatywy_171_ [access: 8 VI 2021].

Rutkowski J., "Nord Stram 2 – wszystko przemawia przeciw temu projektowi", *Forsal*, 27 II 2021, forsal.pl/gospodarka/artykuly/8106480,nord-stream-2-wszystko-przemawia-przeciw-temu-projektowi.html [access: 23 VI 2021].

"Sharp power. Rising authoritarian influence: new forum report, *National Endowment for Democracy*, 5 XII 2017, https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

Walker Ch., Ludwig J., "The meaning of sharp power. How authoritarian states project influence", *Foreign Affairs*, 16 XI 2017, foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power [access: 14 VI 2021].

Walker Ch., "The point of sharp power", *Project Syndicate*, 1 II 2018, https://www.project-syndicate.org/commentary/soft-power-shortcomings-by-christopher-walker-2018-02 [access: 14 VI 2021].

Abstract

The aim of the article is an attempt to define the sharp power strategy, present characteristic ways of its employment and propose methods of minimizing its negative consequences for the security of the Republic of Poland. The analysis of the issues related to the types of state power (soft power, hard power, smart power) is followed by a coherent definition of sharp power formulated by the authors of the publication. The consecutive section of the article describes examples of methods of implementing the aforementioned strategy of influencing participants of international relations. Finally, the authors presented proposals for institutional and legal solutions, which are to counteract potential sharp power moves aimed at undermining the security and international position of the Republic of Poland.

Keywords: state power, sharp power, soft power, hard power, smart power, information warfare, hybrid conflict

KRZYSZTOF IZAK
ORCID: 0000-0001-9815-6035

DOI: 10.4467/20801335PBW.21.033.14310

Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA

Al-Qaeda, by conducting a spectacular terrorist attack on the United States 20 years ago, indirectly caused changes in the domestic and foreign policies of the United States and many other countries in the world. 11 September 2001 was a turning point in the fight against terrorism, which became global in scale. Never before had the governments of so many countries in the world given at least verbal support to a party attacked by terrorists, in this case the US. However, this international unanimity can be justified by the categorical statement of President George W. Bush: "Who is not with us, is against us." No country could officially afford to claim support for terrorism, with an exception of the so-called Axis of Evil. This phrase was used by President Bush in his famous speech on 29 January 2002 and addresses the governments of Iraq, Iran and North Korea. There was no mention of Afghanistan, which the Americans entered in October 2001, and none of Saudi Arabia, which had been supporting Islamic extremists for many years (15 citizens of this country were among the group of 19 who attacked selected targets in New York and Washington). A consequence of the 9/11 attacks was the US invasion of Afghanistan, and then Iraq. This in turn resulted in the escalation of Islamic terrorism that continues to this day. Terrorism threat level can vary now and then, but it is still present and will not simply disappear. In the United States, in order to justify the unintended negative effects of the government's policies, the reality was described using the economic term: *black swan*, which refers to an unexpected and impossibly difficult to predict event that has potentially severe consequences. In reality, however, the fallout of the so-called war on terror were highly predictable. The Taliban takeover in Kabul on 15 August 2021 and the withdrawal of the last American soldiers

from Afghanistan, 20 years after their entry into the country, can be seen as a return to the previous situation, i.e. the reactivation of the Islamic Emirate of Afghanistan.[1]

The purpose of the article is to present the complex process of preparations for the attack on the United States on 11 September 2001, the precise execution of the plan and the consequences that led to irreversible changes in global politics. The suicide hijackers who completed U.S. piloting courses belonged to a new generation of Islamic fighters. Most of them were educated representatives of the middle class with a stable financial situation. So, answering the question, what prompted them to perform a suicide operation and kill several thousand innocent people, would be purposeful. Al-Qaeda would not be able to plan and organize these attacks if it did not have the financial resources, the means to communicate with each other and, above all, a shelter where it was possible to conduct training and adequately inspire young people. Undoubtedly, it was this organization that initiated the course of events that led to the greatest terrorist attack in history. It is particularly significant to present the events and the surrounding circumstances that could have hindered or even partially halted the 9/11 attacks. Therefore, the author will try to answer the question whether it was possible to prevent these almost simultaneous attacks at all. The harbinger of the 9/11 attacks was the assassination carried out just two days earlier of Ahmed Shah Masud, the leader of the United Islamic Front for the Salvation of Afghanistan and the most reliable leader of anti-Taliban opposition, who was trusted by the West.[2] The elimination of Masud was part of the preparations for the US invasion of Afghanistan in retaliation against the 9/11 attacks, which al-Qaeda had correctly predicted.

Osama bin Laden and the Taliban leader Mullah Mohammad Omar probably had no doubts that, like the Afghan mujahideen destroyed the Soviet army after ten years of war, their militants would also cope with US forces if invaded. The author points out that the al-Qaeda forecast turned out to be fully correct, but the administration at the White House was not so clear-cut about sending troops to Afghanistan in the first moment after the attack. The author also raises the issue of conspiracy theories regarding the 9/11 attacks, which were propagated in the media, films and books for

---

1 The Taliban offensive, which started in May 2021, accelerated at the turn of July and August 2021. The soldiers of the Afghan National Army almost without a fight handed over the main cities of Afghanistan. On 15 August, the Taliban took over Kabul. The pace at which this happened came as a surprise to many observers. President Ashraf Ghani fled to the UAE. Thousands of people, NATO staff, family members, representatives of the Afghan administration, international organizations and security forces occupied the Kabul airport, attempting to board Western planes that conducted a delayed evacuation. For many of these people, staying in Afghanistan is a death sentence at the hands of the Taliban.

2 The murder of Ahmed Shah Masud was carried out by two young Moroccans holding Belgian passports. Passing off as journalists, they came to the Panjshir Valley in north eastern Afghanistan, which was the base of Masud and his militants, which was being unsuccessfully attacked by the Taliban for five years. They had a hidden bomb on the camera that exploded as one of the bombers was recording the interview conducted by another alleged journalist. Masud died several hours later as a result of his injuries.

several years. These had a significant impact on the consciousness of the American society, a large part of which recognized an alternative version of events.

The author of this article used a historical method that enables to show the chronological course of events that had led to the four attacks on 11 September 2001. The author also employed a behavioural method, consisting in analysing the behaviour of the participants in the anti-American plot, both at the time of preparations for the attacks and aircraft hijacking. The last method adopted for the purpose of this paper is a statistical one that allows to present in numbers the effects of the terrorist attack on the USA – the victims and material losses.

Planning for the 9/11 operation

The mastermind of the spectacular terrorist 9/11 plot was Kuwait-born Khalid Sheikh Mohammad[3], the uncle of Ramzi Yousef[4], who was responsible for the 1993 WTC bombing.[5] Two years later they both devised a plan to bomb 12 American planes flying from Asia to the USA.[6] In 1996, Mohammed met Osama bin Laden in Afghanistan, to whom he presented various ideas for attacking the United States, including an air operation. Over the next three years, al-Qaeda analysed the possibilities of attacking the United States. One of the plans by Khalid Sheikh Mohammad involved the hijacking of two groups of planes: five from the US East Coast and five from Asia to the US. Nine of them were to be flown into previously selected targets, including buildings of the CIA, FBI and nuclear power plants. Mohammed intended to take the controls of the tenth plane, kill all adult male passengers on board, then make a statement condemning US policy in the Middle East and land in an undefined location, freeing

[3] Khalid Sheikh Mohammad was arrested in March 2003 in Pakistan. He is currently in an American prison. In 2019, Mohammad made an offer to the families of the 9/11 victims, claiming that he would testify in their favour in their civil lawsuit against the government of Saudi Arabia. Mohammad, wanting to avoid the impending death penalty, made an offer of cooperation to the families of the victims. He promised to testify in their favour in the trial against Saudi Arabia. His trial is not over yet.

[4] Ramzi Yousef was arrested in February 1995 in Pakistan. In 1998, the US court gave him a life sentence for the attack on the WTC of 26 February 1993 and the planting of a bomb on flight 435 Philippines Airlines on 11 December 1994.

[5] On 26 February 1993, a truck filled with explosives was detonated in the underground garage of the WTC. Six people were killed and several hundred injured. After the attack, Ramzi Yousef left the USA.

[6] As part of preparations for the terrorist plot known as "Bojinka" on 11 December 1994, Ramzi Yousef planted a bomb of his own construction on a plane flying from Manila to Tokyo. As a result of the explosion, one person was killed and 10 were injured. The plane was seriously damaged, but thanks to the experience of the crew and the short distance from Okinawa, it landed safely. The size of the explosive was several times smaller than the size of the ones planned for consecutive attacks on planes. The "Bojinka" plot was disrupted by an accidental fire in a hotel room rented by terrorists.

the women and children. The latter part of the hijack plot was firmly rejected by Osama bin Laden, but in the Spring of 1999, he gave approval for such an operation. Later that year in Kandahar, the head of al-Qaeda, Khalid Sheikh Mohammad and Mohammed Atef, alias Abu Hafs al-Masri met.[7] The purpose of the secret meeting was to select the objects of the attack that would cause not only the greatest possible material damage, but most of all image damage, of symbolic importance for the United States. No one but these three attended the conference, but among Osama bin Laden's closest associates there was talk of the "plane operation".[8]

The al-Qaeda leader envisioned that an attack on such targets could lead to the collapse of the federal state. No wonder he wanted to destroy the White House and the Capitol. The Pentagon building was also on the list of targets. If these facilities had been destroyed, the collapse of the US would not have been such an unreal fantasy. Khalid Sheikh Mohammad also proposed the WTC skyscrapers, which his nephew Ramzi Yousef had not managed to demolish in 1993. There were also discussions about the Sears Tower in Chicago and the Library Tower in Los Angeles. Bin Laden assumed that attacks on these targets could be carried out later. As mentioned, Bin Laden took into account the probability that, in retaliation against the attack, the United States would sooner or later strike Afghanistan, where they would suffer severe losses, just like the USSR in the 1980s. He also did not rule out the possibility that after the attacks the USA would eventually withdraw all their Middle Eastern forces, as they did in Somalia after the failed attempt to capture Mohammed Farah Aidid in early October 1993. Nineteen American soldiers were killed in this operation.

Al-Qaeda did not have much money at the time, but in its ranks there was a significant number of young people ready to die a martyr's death. If the plan was aimed at only blowing up hijacked planes in the air, there would be no need to involve people trained as pilots. The concept of the attack was more complicated, and its implementation required a disciplined group of people, some of whom would be able to fly planes. Bin Laden assigned Mohammed four of his most reliable men. There were two Saudis in this group: Nawaf al-Hazmi, Khalid al-Mihdar and two Yemenis: Zuhail Abdo Anam Said al Sharabi alias Abu Bara and Tawfiq bin Attash alias Khallad. The group was joined by: Yemeni Ramzi bin al-Shibh (bin al-Shaibah), Egyptian Muhammad Atta al-Sayed, Lebanese Ziad Jarrah and Emirati Marwan al-Shehhi, who at the end of 1999 came from Germany to Afghanistan to meet Bin Laden. He informed them that they would be martyrs, and ordered them to return to Germany and enrol in flight schools in the USA.[9] The "plane operation" plans involved two teams, each of which was to carry out an attack severe to the enemy. The group of men from Germany

[7] Former Egyptian policeman, member of the Egyptian Islamic Jihad, one of the al-Qaeda commanders and one of Osama bin Laden's most trusted advisers. He was killed in a U.S. airstrike in Afghanistan in November 2001.

[8] S. Coll, *Rodzina Bin Ladenów. Arabskie losy w amerykańskim stuleciu*, Warszawa 2015, pp. 435–436.

[9] L. Wright, *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, pp. 432–435.

reported stolen or missing passports so that attention was not paid to their stay in Afghanistan. The members of the later so-called Hamburg Cell came from well-to-do families and studied at technical universities in Europe. Jarrah and Al-Shehhi were engineers, Muhammad Atta was an architect (he studied town planning in Hamburg in 1992–1999), thanks to which they could easily blend in with American society during pilot training. Only Al-Shibh, who came from a disadvantaged background and without a specific profession, didn't fit in with the rest, yet, he knew the Koran well. However, none of them had an upbringing in a madrasa, which before 9/11, was often considered a source of Muslim terrorism. They all attended secular schools, and Jarrah was not even a practicing Muslim before joining the group.[10] Atta was the operational leader of the group. After graduating, he rented an apartment at Marienstraβe 54. This is where the future hijackers used to gather. It was typical for the Hamburg cell to conduct activities in a way that was imperceptible to outsiders. None of the soon-to-be hijackers came to notice as fanatical followers of Islam. Although the Federal Criminal Police Office wanted to investigate members of the Atta group who were interrogated in connection with suspected incidents, the Prosecutor General's Office did not agree to their detention as there was no justification for any legal action or for the issuing of an arrest warrant. Thus, Muhammad Atta lived a normal life, without hiding, he travelled a lot and made contacts from Hamburg to Afghanistan, which made it easier for him to carry out a large-scale terrorist attack on 11 September.[11]

The abovementioned Saudis, Nawaf al-Hazmi and Khalid al-Mihdar, had no problems with obtaining US visas, and from Kuala Lumpur via Bangkok they flew to Los Angeles, where they arrived on 15 January 2000. Yemenis, Abu Bara and Khallad, did not receive US visas. Khallad was the mastermind behind the attack on the destroyer USS *Cole* on 12 October 2000.[12] Saudis enrolled in the US flight school and were aided by a San Diego-based Saudi scholar, Omar Bajumi. Three members of the Hamburg group arrived in the US. Marwan al-Shehhi flew first in May and was followed by Muhammad Atta with Ziad Jarrah in June 2000. Ramzi bin Al-Sibh did not receive a US visa, so he became a liaison between the attackers in the US and al-Qaeda (he is currently in an American prison). Al-Shehhi and Jarrah pretended to be bodyguards of Atta, who in turn played the role of a member of the Saudi royal family. All three travelled to Florida and took flight lessons there in the city of Venice. Future terrorists spent many hours in a Boeing 727 flight simulator and flew small planes in Florida and

[10] K. Armstrong, *Pola krwi. Religia i przemoc*, Warszawa 2017, pp. 532–533.

[11] W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm*, Warszawa 2009, p. 150; A. Lichtenberg, B. Dudek, "Zamachy 11 września: historia 'Grupy Hamburskiej'" *Deutsche Welle*, https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [access: 12 IX 2011].

[12] A motor boat filled with explosives detonated at the side of the ship moored in the port of Aden. The explosion caused a hole 12 m in diameter and many other serious damages. 17 sailors were killed and 39 were injured. The attack on the USS *Cole* followed a similar, unsuccessful attack on the destroyer USS *The Sulivans*, which was moored off the coast of Yemen. It happened on 3 January 2000. The boat was so overladen with explosives it sank before reaching its destination.

other states. The greatest progress was made by Jarrah, who obtained a license to pilot small aircrafts in August 2000. At the end of that year, he began training in piloting large jets. The training fees were paid by Pakistani Ali Abdul Aziz Ali alias Amar al-Baluchi through Emirates Bank International. The money was wired into the Sun Trust Bank, where Atta, al-Shehhi and Jarrah had opened their accounts.

At the end of January 2001, all three had to fly even more hours, do more exercises on flight simulators of large passenger planes (Boeing 747 and 767), and learn about security measures at airports. They broke their stay in the USA with trips to Europe, Africa and the Middle East. Jarrah left the United States six times, more often than any other conspirator. He visited, among others his girlfriend in Germany. Muhammad Atta, al-Shehhi and Jarrah also flew as passengers on American airlines, which allowed them to learn about the security at the airports. During one of these reconnaissance flights from New York to California, Al-Shehhi and Jarrah aroused the interest of airport security, but were not detained.[13]

On the other hand, the flight training of Saudi friends Nawaf al-Hazmi and Khalid al-Mihdar was problematic. In 1995, they had fought together in the Balkans on the side of Bosnian Muslims, and then in Afghanistan, they supported the Taliban fighting against the Northern Alliance of Ahmed Shah Masud. In San Diego, where they lived since January 2000, they attended a mosque whose imam was Anwar al-Awlaki.[14] In San Diego, they also took flying lessons, but due to their poor command of English, they did not cope with practical classes. Instructor Rick Garza gave them six lessons on the ground before allowing them to fly together with him in a single-engine Cessna. Although Garza found them completely incapable of learning to fly, the Saudis were only interested in flying large airliners. They offered extra money for the course, which aroused the instructor's suspicions, but he did not inform the authorities about it. It was evident that neither of them had sufficiently mastered the flying skills.[15] On 10 June 2000 al-Mihdar flew to Yemen to visit his wife, angering Khalid Sheikh Mohammad, who did not want al-Hazmi to be left alone in California. Mohammad even intended to remove al-Mihdar from the planned operation, but Bin Laden reportedly refused to do so. The Saudi man returned to the US. In September, al-Mihdar and al-Hazmi changed their address. They moved to the home of an FBI informant Abdusattar Sheikh, who did not provide the security service with any information about the suspects living in his home. After the attack on the USS *Cole* on 12 October 2000, the Prime Minister of Yemen, Abdul Karim al-Iryani, informed that al-Mihdar was one of the key planners

[13] P.L. Bergen, *Osama bin Laden. Portret z bliska*, Warszawa 2007, p. 319.

[14] Anwar al-Awlaki was a US citizen of Yemeni descent. In the United States, he become religiously radical and reportedly provided spiritual support to the operatives of the 9/11 attacks. He popularized his teachings on the website www.anwar-awlaki.com. Expelled from the US, he went to Yemen. There he became the spiritual leader of the Al-Qaeda Organization in the Arabian Peninsula. He died on 30 September 2001 as a result of a raid by an American unmanned aircraft.

[15] J. Elsässer, *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007, p. 232.

of the attack and was in Yemen at that time.[16] At the end of 2000, al-Mihdar went to Saudi Arabia, and in early 2001, to Afghanistan, where he stayed for several months. It was here where he presumably met Bin Laden. He was appointed the organizer and coordinator of a group of suicide hijackers who were to terrorize the aircrews and passengers. In June 2001, al-Mihdar returned to Saudi Arabia and, apparently, gathered the remaining operatives there and prepared them for the trip to the USA. They travelled in pairs. Al-Mihdar easily obtained an American visa at the US consulate in Jeddah and on 4 July 2001 he landed in New York.[17]

While al-Mihdar was in the Middle East, in December 2000 Al-Hazmi met his compatriot Hani Hanjour. He was the only one of the future terrorists who stayed in the US with no connection to the attack. He first came to the USA in 1991 for a several-month-long English language course. After returning to Saudi Arabia, where he stayed for five years, he applied for a job with Saudi Arabian Airlines, but was rejected due to poor ratings. The airline offered to consider his application if he obtained a commercial pilot's license in the United States. Thus, he returned to the USA where he gained his pilot's license (with a poor rating) in April 1999, after three years of training. His application with Saudi Arabian Airlines was again rejected due to low grades in his pre-admission exam. In late 1999, he was to inform his family that he was going to the UAE to search for a job. In fact, he went to Afghanistan, but by December 2000 he was already in the US. He moved to Abdusattar Shaikh's house in San Diego. There he began his flying training again, but he turned out to be a poor pilot, and his poor knowledge of specialized English in the field of aviation disqualified him from obtaining a professional pilot certificate. Nevertheless, he began advanced training in a flight simulator in Mesa, Arizona, where he arrived with al-Hazmi. At the beginning of April 2001, they both settled in Falls Church, Virginia, in the Washington metropolitan area. At that time, the already mentioned al-Awlaki[18] was appointed the new imam of the Dar al-Hijra mosque in Washington. Here they were joined by compatriots Majed Moqed and Ahmed al-Ghamdi, who came from Saudi Arabia. The four travelled to Patterson, Virginia, and rented an apartment there. From Virginia, they flew to various cities, checking airport security systems. They also travelled to Las Vegas on several occasions to have fun. In Paterson, they were joined by al-Mihdar, who had returned from the Middle East. In July, Hanjour obtained a US driving license on the basis of a false address certificate. In late June 2001, two more Saudis arrived in New York: Abdulaziz al-Omari and Salem al-Hazmi. For several days, the two were with other future hijackers in Paterson. There, al-Omari and al-Mihdar acquired false identity documents. They presumably bought them from All Services Plus in Passaic County,

[16] "Piecing together the terrorist jigsaw", *The Guardian*, of 15 X 2001, https://www.theguardian.com/world/2001/oct/15/worlddispatch.brianwhitaker [access: 17 I 2001].

[17] L. Wright, *Wyniosłe wieże*…, p. 478.

[18] https://en.wikipedia.org/wiki/Hani_Hanjour [access: 1 VI 2021].

New Jersey, a company that sold fakes.[19] According to other opinions, Mohammad al-Atris[20], a US citizen of Egyptian descent, sold false documents to them. He was the leader of a criminal group engaged in the production and sale of false American identity cards.[21] To get false documents, al-Omari went to Florida, there he rented a flat, where he stayed until September. Other Saudis were already in Florida at that time: Satam al-Suqami and the brothers Walid and Wail al-Shehri. Al-Sukami and Walid al-Shehri were among the nine people who opened SunTrust bank accounts with a cash deposit.[22] Money was withdrawn from these accounts for current expenses. In May 2001, Mohand al-Shehri, Hamza al-Ghamdi and Ahmed al-Nami[23] arrived in Florida, followed by the Emirati Fayez Banihammad and Saudi Saeed al-Ghamdi at the end of June. Two al-Ghamdi: Hamza and Ahmed were brothers, while Saeed al-Ghamdi was not related to them. All three came from the same tribe in the Saudi province of Al-Baha to which Ahmed al-Haznawi also belonged. In 2000, all three Al-Ghamdi fought in Chechnya. They were also very religiously observant.[24] Saeed flew to Miami, Florida with Wail al-Shehri. The information concerning the nineteenth hijacker, Salem al-Hazmi, Nawaf's brother, is contradictory. He was first due to arrive in the US on 29 June 2001, according to both the FBI and the 9/11 Commission report, although there were numerous unconfirmed reports that he had previously lived in San Antonio, Texas with Satam al-Suqami. Al-Hazmi, like other Saudis, used the Visa Express program to enter the US. He then moved to Paterson, New Jersey, to live with Hani Hanjour. Both were among the five terrorists who submitted ID applications in Arlington, Virginia, even though al-Hazmi already had a New Jersey ID.[25]

By the end of June 2001, all participants of the 9/11 attacks were already in the United States. Among them were 15 Saudis, two Emiratis, a Lebanese and an Egyptian. Three of the four forming the Hamburg cell: Marwan al-Shehhi, Ziad Jarrah and Muhammad Atta were the key operatives of the entire plot. Atta was supposed to be the operational leader. On 7 July 2001, he set out via Zurich to Spain. He travelled to various locations in the province of Tarragona in the north-east of the country, where a summit meeting was held. There is no doubt that it was attended by Ramzi bin al-Shebh, a member of the Hamburg cell who did not receive a visa to the US and remained al-Qaeda's liaison.[26] Imad Eddin Barakat Yarkas alias Abu Dahdah, born in Syria, and

---

[19] https://en.wikipedia.org/wiki/Abdulaziz_al-Omari [access: 1 VI 2021].

[20] Mohammed al-Atris was arrested in August 2002 at John F. Kennedy Airport. During the search of his apartment, 75 false documents were found.

[21] K. Izak, "Fałszywe dokumenty w rękach terrorystów", *Człowiek i Dokumenty* 2014, no. 32, p. 10.

[22] https://en.wikipedia.org/wiki/Satam_al-Suqami [access: 1 VI 2021].

[23] https://en.wikipedia.org/wiki/Ahmed_al-Nami [access: 1 VI 2021].

[24] https://en.wikipedia.org/wiki/Ahmed_al-Ghamdi [access: 1 VI 2021].

[25] https://en.wikipedia.org/wiki/Salem_al-Hazmi [access: 1 VI 2021].

[26] The investigation carried out after September 11 showed that Moroccans, Said Behaji, Zakariya Essabar, Abdelghani Mzoudi and Mounir al-Motassadeq, also belonged or could have belonged

the Moroccan Amar al-Azizi helped organize this meeting. It is also suggested that the meeting was attended by Khalid Sheikh Mohammad and Said Behaji, and later joined by Marwan al-Shehhi and two others, possibly the brothers Wail and Waleed al-Shehri, who stayed at a hotel in Salou, Costa Dorada on 16 July. During the meeting, Al-Shibh gave instructions from Osama bin Laden, including his appeal for the air operation to be carried out as soon as possible and to keep its goals secret. The al-Qaeda leader was concerned about the safety of the operation, as the real threat was the presence in the USA of a large number of participants in the planned attack. Atta informed that all participants of the plot, who were supposed to terrorize the crews and passengers of the hijacked planes, had already reached the United States without any problems. He claimed he needed another five to six weeks to finalize the details of the operation. Bin al-Shibh handed him the ultimate list of targets set by Bin Laden. These were the symbols of America: The United States Capitol, the Pentagon and the World Trade Center. The Twin Towers were two of the most recognizable buildings in the world and shaped the New York skyline. If any of the hijacker pilots would not be able to reach the target, they were supposed to crash the plane. Atta communicated his personal problems he had with Ziad Jarrah. He suspected that he might abandon preparations for the attack. If such a situation did occur, he would be replaced by Zacarias Moussaoui, who was trained as the next pilot.[27]

French citizen Zacarias Moussaoui alias Abu Khalid al-Sahrawi from the end of February till the end of May 2001, completed approximately 60 hours of piloting in Norman, Oklahoma. Despite this, he never flew by himself and for unknown reasons left further training. Muhammad Atta and Marwan al-Shehhi were also in the same pilot school. From Oklahoma, Muossaoui travelled to Minnesota to continue his training at Eagan, for which he received money from Düsseldorf and Hamburg sent by Bin al-Shibh. On 13 August he paid 6,800 USD to train on a Boeing 747 flight simulator at Pan-Am International Flight Academy. However, he aroused the suspicions of

to the Hamburg cell. The latter was the only member of the Hamburg cell who was sentenced to imprisonment in Germany. In January 2007, Motassadeq was sentenced to 15 years in prison for membership in a terrorist organization and for helping to murder 246 people. That's how many people flew on four US airline planes on 11 September 2001. In October 2018, Motassadeq left the Hamburg prison and was deported to Morocco without the right to return to Germany within 46 years. Abdelghani Mzoudi was arrested along with Motassade, but was acquitted in 2004. The other two Moroccans left Germany after 9/11 and went to Afghanistan. According to German law, the Hamburg cell was not an independent terrorist organization, as it was not able to carry out attacks in the USA neither financially nor personally (that was the reasoning then). According to the Federal Office for the Protection of the Constitution, the attacks were not planned in Hamburg, but in Afghanistan. "Zamachy 11 września: historia Grupy Hamburskiej", *Deutsche Welle*, 11 IX 2011, https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [access: 12 IX 2011]; N. Werkhäuser, "Hamburg: pomocnik zamachowców z 11 września wydalony do Maroka", *Deutsche Welle*, 15 X 2018, https://www.dw.com/pl/hamburg-pomocnik-zamachowców-z-11-września-wydalony-do-maroka/a-45895869 [access: 16 X 2018]; *The 9/11 Commission Report*, https://govinfo.library.unt.edu/911/report/911Report.pdf, pp. 160–164 [access: 6 VI 2021].

[27] https://en.wikipedia.org/wiki/Mohamed_Atta [access: 1 VI 2021].

the instructor Clarence Prevost, who contacted the FBI field office on 15 August because he was concerned about the student's questions. Moussaoui asked questions about the air routes around New York and inquired if the cockpit door could be opened during the flight. The FBI quickly determined that Moussaoui was an Islamic radical who had previously lived in Pakistan and possibly Afghanistan as well. It was suspected that he might become a suicide hijacker in the future. As he was a French national who overstayed his visa, the Immigration Office issued a detention warrant. On 16 August Moussaoui was arrested in Eagan and charged with immigration violation.[28] After 9/11, it was hypothesized that Moussaoui was probably preparing for the second series of al-Qaeda attacks, which were to take place on the west coast of the USA.[29] He was the only participant of the preparations for the attack to be arrested before 11 September and was later called the twentieth hijacker. Ramzi bin al-Shibh was called by the same name, but wrongly because he never reached the United States.

On his return from Spain, Muhammad Atta met on 25 July with Jarrah, whom he drove to the Miami airport to depart for Germany. The next day he travelled to Newark, New Jersey by Continental Airlines. The purpose of the trip was probably to eet the participants of the attack who were there. He returned to Florida on 30 July. In August, he travelled again to New Jersey and twice to Las Vegas on observation flights, independent of the other members of the group. He met monthly with Nawaf al-Hazmi to discuss the state of preparation for the operation. On 10 September Atta picked up Abdul Aziz al-Omari from the Milner Hotel in Boston, Massachusetts (where other hijackers had checked in as well) and the two terrorists travelled in a rental car to the Comfort Inn Hotel in Portland, Maine, where they spent the last night. In the morning they boarded a flight from Portland to Boston. Before seven at the Logan airport in Boston, Atta received a call from Marwan al-Shehhi, most likely with the information that he and his companions were already at the same airport.[30] The operation entered its final phase.

The attacks

Boeing 767 aircraft American Airlines 11 flight from Boston to Los Angeles

At 7.59 a.m. Boeing 767 aircraft American Airlines Flight 11 took off from Boston to Los Angeles, California. There were 81 passengers on board, including Muhammad Atta, Abdulaziz al-Omari, the brothers Wail and Waleed al-Shehri, and Satam al-Suqami. 15 minutes into the flight, when passengers were served drinks, the hijacking operation began. Probably, the terrorists threatened to detonate an explosive. During

[28] https://en.wikipedia.org/wiki/Zacarias_Moussaoui [access: 1 VI 2021].

[29] L. Wright, *Wyniosłe wieże*…, p. 490.

[30] https://en.wikipedia.org/wiki/Mohamed_Atta [access: 1 VI 2021].

this time, the pilots stopped responding to air traffic control signals. They were forced to leave the cockpit, and Atta took over the controls. The plane began to deviate from the planned route. At 8:18 a.m. two flight attendants: Betty Ong and Madeline Sweeney managed to establish a few minutes' contact from the rear of the plane via SBC Communications radio with the American Airlines office and flight attendants at Logan airport in Boston. The women informed about the hijacking of the plane, provided the numbers of the first-class seats taken by the hijackers after boarding the plane (in the following order: 2A, 2B, 9A, 9C and 9B). On this basis, their identity was quickly established. They also reported that a passenger, a female flight attendant and a male flight attendant had been injured with a knife. The perpetrators were the Al-Shehri brothers.[31] Exactly at 8.23 a.m. Muhammad Atta tried to make an announcement to the passengers from the cockpit, but pressed the wrong switch and thus sent a message to the air traffic control service. He said: "(...) have some planes, just stay quiet and you'll be ok. We're returning to the airport." A minute later he added: "Nobody move. Everything will be okey. If you try to make any moves, they will endanger yourself and the airplane. Just stay quiet." The air traffic control service obtained confirmation that the plane was hijacked and informed the Federal Aviation Agency of this fact. At 8.33 a.m. Muhammad Atta announced: "Nobody move, please. We're going back to the airport. Don't try to make any stupid moves." Five minutes later, the Boston Air Traffic Control Service informed NORAD[32], which in turn called on two F-15 Eagle planes from Otis base to take control of the flight. However, the order to take off the F-15 fighters was issued too late. The analysis of the time of informing the controllers indicates that the right decisions were not made on time, as NORAD was informed at 8:38, i.e. 20 minutes after the first hijack signal given by the flight attendant. The plane was already over New York's Manhattan.[33] At. 8:46 a.m. terrified Sweeney said over the phone to manager Michael Woodward: "I can see water. I can see buildings. I can see buildings! We're flying low. We're flying very, very low. We're flying too low. Oh my God, we're going way too low. Oh my God!"[34] At that moment, the plane piloted by Atta hit the North Tower of the WTC at a speed of about 750 km/h (there were about 40,000 litres of jet fuel in the tanks).[35] The plane struck between the 93rd and 99th floor

[31] https://pl.melayukini.net/wiki/Betty_Ong [access: 1 VI 2021]; https://pl.melayukini.net/wiki/Wail_al-Shehri [access: 1 VI 2021].

[32] North American Aerospace Defence Command – a combined organisation of the United States and Canada that exists since 12 May 1958., https://pl.wikipedia.or/wiki/North_American_Aerospace_Defense_Command (editor's footnote).

[33] https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks#American_Airlines_Flight_11:_One_World_Trade_Center,_North_Tower [access: 3 VI 2021]; *National Commission on Terrorist Attacks Upon the United States*, "We have some planes", https://www.9-11commission.gov/report/911Report_Ch1.htm [access: 3 VI 2021].

[34] https://pl.melayukini.net/wiki/Madeline_Amy_Sweeney [access: 1 VI 2021].

[35] The flight from Portland to Boston was delayed, so Atta's luggage did not make it onto Flight 11. It was retrieved later at Logan Airport. The luggage included airline uniforms, flight manuals, as well

of the building. Due to the massive destruction of the tower, people from the 92nd floor and above could not escape. 1,344 people were trapped because all stairs and elevators were impassable. Hundreds of people were killed by the impact, others died from fire or smoke, and still others died by jumping out of the building's windows. The first reports spoke of a mishap, but the narrative changed when the second plane, Flight 175, flew into the South Tower.[36]

Boeing 767 aircraft United Airlines flight 175 from Boston to Los Angeles

On 9 September, Marwan al-Shehhi, Fayez Banihammad, Mohand al-Shehri and Satam al-Suqami departed from Florida to Boston. The next day, they rented a room at the Milner Hotel in Boston. So, al-Suqami shared a room with the hijackers of another plane, because he himself boarded flight 1137.[37] The brothers Hamza and Ahmed al-Ghamdi flew from Florida to Boston on 7 September. They checked into the Days Hotel, where they stayed until the day of the attack. On the morning of 11 September, they arrived by taxi at Logan International Airport. There a few minutes before seven Marwan al-Shehhi made a phone call to Atta, with whom he talked for about three minutes. Around 7.30, the hijackers: al-Shehhi, Banihammad, al-Shehri and the al-Ghamdi brothers took their places on the Boeing 767 aircraft United Airlines flight 175 to Los Angeles. There were 46 passengers and nine crew members on board. Approximately 30 minutes into the flight, between 8.42 and 8.46, the plane was hijacked. The al-Ghamdi brothers pushed passengers and the crew to the rear of the plane, threatening with an explosive. Banihammad and Shehri killed the pilots Victor Saracini and Michael Horrox. This allowed al-Shehhi to take control of the plane. One of the female flight attendants was stabbed. The plane piloted by al-Shehhi almost collided with the Delta Airlines aircraft Flight 2315. Several passengers called their relatives, informing them of the hijacking. At the same time, they found out about the Flight 11, which had already hit the North Tower of the WTC. At 9.03 a.m. the plane - flying at a speed of 950 km/h, which was faster than the plane piloted by Muhammad Atta - crashed into the southeast corner, striking through floors 77 and 85. There were about 38,000 litters of jet fuel. The impact of the crash into the building in such a place caused the South

as other items and a farewell letter, which was a kind of instruction from the martyr. The document consisted of three parts: instructions for the last night of a martyr, instructions for the time before boarding the plane and the last gave instructions about the flight until martyrdom. These instructions were supported by quotations from the Koran for future suicide bombers like him. Everything in the context of spiritual preparation with prayers and quotations from the scriptures. There is an interesting passage from Atta's will: "The people who will clean my body should be good Muslims. The person who will wash my body around my genitals should wear gloves so he won't touch them". The terrorist was unaware that his body would be atomized in the blast. P.L. Williams, *Al-Qaida - the brotherhood of terror*, Warsaw 2002, pp. 168–175.

[36] https://pl.wikipedia.org/wiki/Katastrofa_lotu_American_Airlines_11 [access: 1 VI 2021].

[37] https://pl.melayukini.net/wiki/Satam_al-Suqami [access: 1 VI 2021].

Tower to collapse at 10.28 which was earlier than the North Tower.[38] It is estimated that 637 people were killed or trapped in the building at the time of the disaster. Part of the fuselage and landing gear broke off the plane which hit the south tower and fell on the 47-story 7 WTC building (the twin towers are 1 WTC and 2 WTC), setting it on fire, and causing its collapse at 17.20.[39]

Boeing 757 aircraft American Airlines flight 77 from Washington to Los Angeles

On 10 September, all hijackers of the Boeing 757 aircraft American Airlines Flight 77 to Los Angeles: Hani Hanjour, Khalid al-Mihdar, Majed Moqed and brothers Nawaf and Salem al-Hazmi checked into the Marriott Residence Inn in Herndon, Virginia, located nearby Dulles International Airport in Washington, DC. At the same time, Saleh ibn Abdul Rahman Hussayen, a prominent representative of the Saudi Arabian government, was staying at the hotel, but there is no evidence that he met or even knew about any of the future hijackers. The next day at approximately 6.20 a.m., the whole group left the hotel for the above airport. At 7:20 a.m. al-Mihdar and Moqed were selected for extra screening during security checks because of a metal object being detected. However, they both boarded the plane without problems, as did the other three members of the group. At 7.50 a.m. they took their seats on the plane. They were armed with plastic knives and wallpaper cutters. Besides the hijackers, there were 53 passengers and six crew members on board. The plane took off at 8:20 a.m. with a 10-minute delay. Exactly 30 minutes later, the pilots communicated via radio with air traffic controllers for the last time. In the next four minutes, the plane must have been in the hands of the hijackers as it deviated from its intended direction of flight. Hani Hanjour assumed control over the plane. In contrast to the hijackings of the remaining aircrafts, in the case of Flight 77, there was no information about a bomb threat and attack with sharp tools. Pilots Charles Burlingame and David Charlesbois were forced to take their seats in the rear of the plane. Using the intercom, Hanjour announced that the plane had been hijacked. The passenger Barbara Olson informed her husband Theodor Olson, the US attorney general, about the hijacking of the plane by phone. At 9.37 the plane crashed into the west facade of the Pentagon. 64 people in the plane and 125 people in the building were killed.[40]

Boeing 757 aircraft United Airlines Flight 93 from Newark to San Francisco

On 7 September, Ziad Jarrah, Ahmed al-Haznawi, Ahmed al-Nami and Saeed al-Ghamdi were the first to leave Florida. They flew to Newark near New York. It is not

[38] https://pl.melayukini.net/wiki/Marwan_al-Shehhi [access: 4 VI 2021]; https://pl.melayukini.net/wiki/Hamza_al-Ghamdi [access: 4 VI 2021].

[39] https://pl.xcv.wiki/wiki/United_Airlines_Flight_175 [access: 4 VI 2021].

[40] https://pl.melayukini.net/wiki/Hani_Hanjour [access: 4 VI 2021]; https://pl.melayukini.net/wiki/Nawaf_al-Hazmi [access: 4 VI 2021].

known what they were doing till the plane hijacking. On 10 September, Jarrah wrote a letter to his fiancée in Germany, but she did not receive it. The parcel returned to the US and was seized by the FBI. It was a suicide terrorist letter containing phrases such as: "I did what I had to. It is a great honour. You will see the result and everyone will be celebrating."[41] On 11 September, between 7:39 a.m. and 7:48 a.m., all hijackers boarded Boeing 757 aircraft United Airlines Flight 93 from Newark to San Francisco. They took their seats in business class in the front part of the plane. Excluding the hijackers, there were 33 passengers and seven crew members on board. The plane was supposed to take off at 8.00, but due to delays in other flights, it did not take off until 8.42 a.m. At 9.24, the crew was informed of two planes that had crashed into the WTC and warned against cockpit intrusion. Two minutes later, the pilot asked for confirmation of this information. Meanwhile, one of the hijackers, possibly al-Ghamdi, attacked one of the female flight attendants, and Al-Haznawi, the passenger, and showed a cardboard dummy bomb that he had attached to the body. At 9.28 a.m. a female flight attendant was forced to open the cockpit door. There, al-Ghamdi and al-Namni cut the throats of the pilots: Jason Dahl and LeRoy Homer, and killed the flight attendant. The air traffic controller heard the scream of the woman being killed and the voice of the terrorist shouting "Allah Akbar!". As the plane began to descend abruptly, Jarrah who was at the controls, tried to stabilise the flight and turn the plane towards Washington. Passengers were forced to sit in the rear of the plane. At 9.32 one of the hijackers ordered them to remain calm. Jarrah was instructing passengers from the cockpit, but because he pressed the wrong button, his voice was not heard on the plane, but in air traffic control. At 9.31 Jarrah gave the message:

Ladies and gentlemen, here the captain. Please sit down. Keep remaining seating. We have a bomb on board. So, sit. Eight minutes later he repeated: Here's the captain. I would like you all to remain seated. We have a bomb aboard and we are going back to the airport to have our demands. So, please remain quiet.

However, the passengers were not prohibited from using mobile phones. Thanks to this, they learned from their families about the attack on the WTC. The passenger, Jeremy Glick, told the family that the hijackers were Arabs and they had red bands tied around their heads. Together with the other passengers he concluded that their plane could also be used to attack an important object. As a result of a vote, they reached a decision to try to seize the plane from the hands of terrorists. The sight of the pilots' bodies lying in front of the cockpit probably helped confirm such a conclusion. They decided to attack with the use of weapons made of cutlery from the on-board kitchen and dishes with boiling water. The passenger attack caused the hijackers to lose control of the situation. Ziad Jarrah had serious problems with controlling the Boeing, but he tried to make it difficult for passengers to approach the cockpit door by rolling the machine left and then right. This caused passengers to lose their balance in the narrow aisles of the aircraft interior, but still they managed to near to the

[41] https://pl.melayukini.net/wiki/Ziad_Jarrah [access: 4 VI 2021].

front of the aircraft. Most likely using a food cart, they rammed one of the terrorists standing in front of the cockpit door. The passengers managed to incapacitate or kill him. Meanwhile, the three other hijackers locked themselves in the cockpit. They were not prepared for this turn of events. When passengers began to force down the cockpit door, Jarrah most likely made the decision to crash the plane with the ground. For unknown reasons, he prolonged the moment of the catastrophe. As soon as the flight speed increased, the passengers managed to force the door open. They got into a fight with terrorists. The plane turned upside down with the landing gear up and at 10.03 (according to other sources, at 10.06 or 10.10), it crashed to the ground at a speed of 930 km/h. The disaster occurred near Shanksville, Pennsylvania.[42] Because of the Flight 93 delay of more than 40 minutes passengers became aware of earlier attacks, which the terrorists had not taken into account. The passengers' resistance surprised them too. The target of the attack was the White House or the Capitol. The latter, however, seems more likely as Osama bin Laden wished to destroy it.

The aftermath of the attacks

In the events of 9/11, 2,996 people were killed, including 19 terrorists, and 6,291 were injured.[43] Six Poles were among the fatalities. 343 firefighters died in the rescue operation. Most of the rescuers, firefighters and policemen who were the first to come to the rescue and survived, began to develop cancer because of inhaling harmful substances. For some people, symptoms didn't appear until 10 years or even later. By 2017, 142 officers had died as a result of diseases related to the service in Ground Zero.[44] The media started writing about the 9/11 attack and talking about "mega-terrorism" because this incident had been the most successful attack of any terrorist organization until then. Psychologically, the United States and much of the world were undeniably shocked. In the US, in the period of several days after 9/11, the sale of weapons and ammunition for personal use increased by 10%, while in six months the number of weapons sold increased by 450,000 pieces more than in the same period before the attack. Patriotic spirit was mobilised. On the day of the attack, sales of US flags in Walmart stores increased by two thousand percent, and the next day by a further four thousand percent. At the beginning of October, 80 percent of Americans had flags displayed in front of their houses. When President George W. Bush announced "a monumental struggle of good versus evil" on 12 September, the crowd chanting "Kill all Arabs!" surrounded one of the largest mosques in Chicago, frequented mainly by

[42] https://pl.wikipedia.org/wiki/Katastrofa_lotu_United_Airlines_93 [access: 4 VI 2021]; https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks [access: 4 VI 2021].

[43] https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [access: 7 VI 2021].

[44] "Nieśli pomoc po ataku na WTC, po latach ciężko zachorowali. Śmierć strażaków - ojca i syna - w wyniku nowotworów", *Polsat News*, 19 VIII 2017, https://www.polsatnews.pl/wiadomosc/2017-08-19/niesli-pomoc-po-ataku-na-wtc-smierc-strazakow-w-wyniku-nowotworow/ [access: 6 VI 2021].

Arabs. Across the United States, anti-Muslim sentiment, acts of hatred and aggression directed at culturally alien residents increased. Police advised to close Muslim schools for a week, and Muslims not to participate in Friday prayers for their safety. Among the victims, including fatalities, were both Muslims, Hindus and Sikhs.[45]

The attacks caused enormous material losses. Particularly high costs were incurred by insurance and reinsurance companies, airlines and aircraft manufacturers, as well as the tourism industry. The enormous damage connected with the destruction of the New York City World Trade Center and the disruption of the financial system had to be covered by insurance companies linked with the lucrative American market. The airlines whose planes were hijacked and then destroyed during the terrorist attacks were also due compensation. Swiss reinsurance company Swiss Re estimated that the total losses of the insurance sector related to the 9/11 attacks amounted to 90 billion USD, of which 19 billion USD were direct costs. The insurance sector in order to secure itself for the future revised the policy and raised rates significantly, from 20 to 80 percent, mostly where the risk was particularly high. For airlines, the hijacking and destruction of several planes meant a sharp decline in travel interest. Fears of new terrorist attacks caused passenger traffic to decrease dramatically, which meant a considerable reduction in financial inflows for carriers. An even more severe blow turned out to be that the increase in insurance rates substantially raised the costs of air transport. As air transport struggled with the effects of a general downturn in the global economy, the 9/11 events plunged this service area into the deepest crisis since World War II. Total losses were estimated at 12–13 billion USD. Under these conditions, airlines had to suspend some connections, decommission hundreds of aircrafts and reduce personnel. Ticket prices were also lowered, in some cases by as much as 80 percent. Two companies that had been in financial difficulties for a long time - Swissair and Sabena - had to file for bankruptcy. After 9/11, the overall number of flights in the US, including private flights, decreased by 22.7 percent. In 2001, European airlines recorded a decrease in passenger traffic by 5%, and a year after the terrorist attack, it was lower by 11%. Domestic and international airports around the world handled 3 percent fewer passengers. Freight traffic also decreased. The crisis in the air transport had an impact on the situation of aircraft manufacturers. The airlines had largely limited orders, especially for Boeing and Airbus aircrafts. The entire tourism industry felt a decline in travel interest, involving both tour operators, hotels, gastronomy and various types of commercial and service companies. One example was the decline of the luxury goods trade, which basically took place at airports. As a consequence, the production of such articles also decreased.[46]

However, the most critical were the international repercussions. By launching attacks on the WTC and the Pentagon, al-Qaeda influenced world politics by prompting

[45] D. Streatfeild, *Świat po 11 września*, Warszawa 2011, pp. 42–44.

[46] A. Krzemirski, "Rocznica 11 września. Olbrzymie odszkodowania i strach przed podróżami", *Parkiet* of 11 IX 2002, https://www.parkiet.com/artykul/260530.html [access: 6 VI 2021].

Washington to declare a "war on terror". In a speech to the nation on 20 September 2001, President George W. Bush revealed the plans for this war. The United States demanded unconditional support from its people, allies and all nations for the war against terrorism, and the principle of "either with us or against us" resulted in the condemnation of neutral states and their recognition as enemies of the United States. In America itself, opposition to this war was viewed as a betrayal of those killed in Manhattan, Washington, and Pennsylvania, as well as a betrayal of the nation and the "values of civilization".[47] At the same time, Washington devised a list of strategic goals. Among them, the possibility of an attack on Iraq was considered, although there was no indication of the country's involvement in the terrorist act. Ultimately, Secretary of State Colin Powell's moderate line of conduct prevailed, and after the Taliban's refusal to hand over Osama bin Laden, on 7 October 2001, the US Operation Enduring Freedom began with a volley of 50 missiles fired from American warships in the Arabian Sea. One of the missiles hit the residence of Mullah Mohammed Omar, a Taliban leader, in Kandahar, killing his stepfather and a 10-year-old son. Another fell on the small village of Kuram, killing 100 civilians, and another destroyed a mosque in the outskirts of Jalalabad. By 9 November U.S. backed-Afghan Northern Alliance forces, fighting the Taliban had gained control of the strategic city of Mazar-i-Sharif, the capital of Balkh Province in northern Afghanistan. Thus, they put an end to Taliban rule. Two days later, the city of Herat, in the west of the country, surrendered almost without a shot. On 12 November, coalition forces entered Kabul, where they were greeted by cheering crowds of Taliban opponents. Contrary to all expectations, the first stage of the war of revenge against the Taliban turned out to be an undeniable success of the US Army. While the new Vietnam or the remake of the Soviet defeat of the 1980s was being announced, the US military, thanks to its air force and special forces and the help of troops hostile to the Taliban, crushed the Islamic Emirate of Afghanistan in a matter of weeks. Al-Qaeda had to relinquish its close-knit structure in Afghanistan and remained a network structure and political ideology. The Americans did not manage to capture Osama bin Laden in Afghanistan, who for many Muslims became a symbol of the fight against the US and a living legend.

The US war on terrorism was followed by the US invasion of Iraq on 20 March 2003. The dual threat of terrorism and weapons of mass destruction was only a pretext to eliminate an enemy that had long been on the target of the United States, especially of the so-called neoconservatives, politicians around Vice President Dick Cheney and Assistant Secretary of Defence Paul Wolfowitz. Cheney took up the old concept of Reagan's preventive war and made it the centrepiece of a new strategy to prompt a government change in Iraq. Prevention was replaced by deterrence. Since then, the theoretical notion of preventive war mixed in practice with the war on terror. It was a way of imposing American supremacy over the next decades and transforming

[47] *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, P. Scraton (ed.), Warszawa 2003, pp. 14–15.

the United States into a hegemonic undisputed power by, inter alia, overthrowing the regime in Iraq and planning a US-style democracy there. In the longer term, it was supposed to change the system of government in other countries around the Persian Gulf and contribute to the resolution of the Palestinian-Israeli conflict. The rest of the events are well known. On 20 March 2003, coalition forces, mostly American and British (with the participation of Australians and Poles), quickly overthrew the government of Saddam Hussein, who was detained a few months later. American forces, however, remained stuck in both Afghanistan and Iraq for many years, did not solve any problems, but contributed to the development of Islamic terrorism on an unprecedented scale. Moreover, the invasion of Iraq turned out to be one of the most spectacular and deadly strategic mistakes in military history.

The terrorist attack on the USA was an impulse for the reform of the American secret services, the most far-reaching since 1947. Washington made a decision regarding the need to create a system that would adequately counteract terrorist threats and effectively warn about their occurrence. This involved strengthening of the structures with operational and reconnaissance powers, increasing the scope of their tasks and improving their ability to coordinate. According to some experts and FBI agents, it was the lack of cooperation between this federal service and the CIA, which did not provide them with important information, that prevented the detection of a terrorist plot in the US before the largest attack in history took place. The question that remains unanswered is whether the attack could have been prevented under different circumstances? It seems rather not. The American secret services had too little information to be linked into a logical sequence leading to the hijackers.

In addition to the secret service reform, new legal regulations were also introduced. They were included in the document of 26 October 2001, commonly known as the USA Patriot Act.[48] This law allowed the government to access private information, even if there was no proof that the person was involved in terrorist activities, with all the possible abuses that resulted from it. Numerous security measures were introduced on the territory of the US, with particularly strict controls at airports and public buildings. Border controls were tightened up, especially towards people from countries subject to visa requirements. Immigrants found to be suspects were arrested. The counterterrorism management apparatus was centralized. The Intelligence Community, which was internally divided with struggles for influence, competence and line of duty, underwent a process of reform. Washington granted the US judiciary the highest prerogatives. It is difficult to assess to what extent the actions taken on the basis of these decisions helped to eliminate the terrorist threat. They certainly contributed to some extent to the restriction of civil liberties and human rights, as symbolized by the internment of prisoners suspected of terrorist activity at the US military base in Guantánamo. Internationally, the new course in US foreign policy

[48] M. Szymańska, "Eksplozja terroryzmu w USA a przekształcenia w amerykańskich służbach specjalnych po 11 września 2001 r.", *Przegląd Bezpieczeństwa Wewnętrznego* 2014, no. 10, p. 186.

distorted by the sympathies and provisional goals of the neocons who blacklisted Iraq for al-Qaeda support (even though there was no evidence for this), while omitting Saudi Arabia and Pakistan, which are known to be supporting many terrorist organizations, including al-Qaeda.[49] Much controversy in the United States was sparked by 28 secret pages (out of 838) of the 2002 report by the US Congress on the 9/11 attacks, to which the author already referred. Saudi Arabia flatly rejected accusations that it had anything to do with the attacks on New York and Washington. The basis for such allegations, made by some of the victims' families and American politicians, was precisely the classification of a part of the US Congress report. It was speculated that there is evidence of Saudi Arabia's ties to the attacks, and it was not just because 15 of the 19 terrorists were Saudis who belonged to al-Qaeda led by another wealthy Saudi - Osama bin Laden. After the document was declassified in July 2016, it was noted that there was no information in it indicating any links between the Saudi authorities and the attackers. At the same time, former Florida Senator Bob Graham, who co-chaired the Congressional investigation, found that it was very clear from the disclosed pages that Saudi Arabia was the main source of financing the attacks. Thus, doubts about Saudi Arabia's role in the 9/11 attacks still remained and gave rise to compensation claims by the families of the victims against Riyadh.[50]

9/11 conspiracy theories

A large number of supporters of the 9/11 conspiracy theories suggests that the then US government stood behind the attacks which were planned and organized by the secret services. In a 2006 poll on the fifth anniversary of the attacks, more than a third of respondents said the Washington administration either had helped carry out the attacks or had not deliberately done anything to prevent them. In a telephone poll conducted in the same year, half of Americans replied that for President George W. Bush, the 9/11 attacks had been a pretext for a war with Iraq. Two years later, the number of people recognizing an alternate version of the 9/11 events increased even more. As much as 46 percent of Americans did not believe the government's version of the incidents, and nearly half of the American population, including many scientists and politicians, demanded a re-investigation of the attacks.[51] Not surprisingly, the 9/11 Truth Movement,

[49] G. Chaliand, A. Blin, *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020, pp. 372–373.

[50] "USA: Kongres ujawnił tajną część raportu o zamachach z 11 września", *Dziennik Gazeta Prawna*, 15 VII 2016, https://www.gazetaprawna.pl/wiadomosci/artykuly/960454,usa-kongres-ujawnil-tajna-czesc-raportu-o-zamachach-z-11-wrzesnia.html [access: 16 VII 2016]; "Rodziny ofiar zamachów na WTC z 11 września pozywają Arabię Saudyjską", *Bankier.pl*, 21 III 2017, https://www.bankier.pl/wiadomosc/Rodziny-ofiar-zamachow-na-WTC-z-11-wrzesnia-pozywaja-Arabie-Saudyjska-3668756.html [access: 22 III 2017].

[51] "Spisek World Trade Center", *Laif*, 9 V 2008, https://web.archive.org/web/20090615224350/http://laif.co.uk/art,spisek_world_trade_center,1496.html [access: 9 VI 2021].

which supported the production of documentaries exposing Washington's alleged lies and neglect, and the publication of books, often written by recognized authorities, grew in power. However, the driving force for the movement was the Internet, which spread information that the government was jointly responsible or directly responsible for the attacks. A special role was played by the families of the victims, who could not understand "(...) why President Bush, after the news about the plane crash into the second WTC tower, sat idle with a thoughtless face among six-year-olds at a school in Florida."[52]

In 2014, 2,300 architects and engineers affiliated with Architects & Engineers for 9/11 Truth (AE911Truth) demanded an independent re-investigation into the collapse of three WTC buildings. Currently, this organization already has 3,300 members.[53] In September 2019, a team of scientists from the University of Alaska Fairbanks published the results of a four-year study on the behaviour of the 7 WTC building structure at the time of the disaster. Based on, inter alia, computer simulations it was identified that the cause of the collapse of the 47-story building could not be a fire, but only the almost simultaneous damage to all columns inside the building. In the 1 WTC and 2 WTC buildings, the fire from the crash of the planes did not last long and did not result in a long-term rise in temperature, as all the fuel from the aircraft tanks burned out immediately after the crash. Computer simulations were to show that the temperature of the fires was over 1000°C, while steel and iron in this type of structures begin to melt only at a temperature of about 1500°C. According to the conspiracy theory, Twin Towers and 7 WTC were destroyed by the use of controlled detonation of explosives. The official report of the National Institute of Standards and Technology avoided any discussion about the possibility of planting explosives, as the possibility of using them was arbitrarily ruled out at the beginning of the investigation.[54]

Even more questions arose in connection with the attack on the Pentagon. The giant Boeing that hit it was piloted by Hani Hanjour, who was rated low by instructors as a pilot of an only two-person plane. Meanwhile, on 11 September, he was piloting a large plane, with incredible composure and accuracy, steering the machine at the speed of almost 1000 km/h into a building at the height of only a few meters above the ground. No remains of the plane were found, and in addition, the damage found in the building after the accident was too small for the size of the plane. Although many eyewitnesses described the crash, the authorities were unable to show any video of the incoming plane silhouette, despite the fact that several dozen cameras were installed in the vicinity of the Pentagon. All but one of the victims' bodies were identified

[52] M.A. Velez, "11 września: władza spisków", *Wirtualna Polska*, 7 IX 2006, https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [access: 11 IX 2006].

[53] M. Kucharczyk, "Wybuch, który miał zatrzeć ślady wielkiego spisku. Ta teoria o zamachach na WTC wciąż ma się dobrze", *gazeta.pl*, 11 IX 2020, https://wiadomosci.gazeta.pl/wiadomosci/7,114881,26286855, kontrolowany-wybuch-ktory-mial-zatrzec-slady-ta-teoria-o-zamachach.html [access: 12 IX 2021].

[54] Ibid.

by DNA analysis. It was unclear how the human remains were preserved since no significant fragments of the plane were found because they had "evaporated" due to high temperatures (information on the remains of the plane was included in the official version of the Commission report on September 11). These doubts arouse due to the emergence of a theory that a missile hit the Pentagon. It was thus another piece of evidence of a neoconservative conspiracy to fabricate an excuse to invade Iraq.[55]

Other conspiracy versions were based on the alleged prior knowledge of certain people about the September 11 attacks. This issue, concerning profitable financial operations carried out before the attack, was raised, among others, by in Michael Moore's *9/11 Fahrenheit*. In turn, the British BBC and the Reuters agency reported the collapse of the WTC 7 building more than 20 minutes before this event, which, according to supporters of conspiracy theories, was supposed to indicate prior knowledge about the attacks. On YouTube, you could find an excerpt of the BBC news in which the anchor reports the collapse of WTC 7, while in the background one could see a live panorama of Manhattan with the building still standing there. According to the BBC, it was a mistake of a reporter who had just arrived at the scene and the fault of misinformation from Reuters. The news agency released a statement that the information about the collapse of the 7 WTC building was reported by the local agency and passed on without verification. According to another conspiracy theory, Jews were allegedly warned about the attack earlier, because none of them died in the WTC, despite the fact that many of them worked there. This theory was supported by the fact that there was only one Israeli on the list of victims. Meanwhile, not every Jew is a citizen of Israel, and about 400 American Jews were killed in the attack on the WTC. In Muslim countries, however, the theory spread widely about the plot being prepared by Israel, as evidenced by the fact that on 11 September 2001 four thousand Jews did not come to work at the WTC because they had been warned by text message.[56]

According to the testimony of Colin Powell, then secretary of state, part of the so-called war hawks around President Bush immediately wanted to use these events as a way to solve the problem with Iraq. In other words, 9/11 was to become a pretext for a war with Saddam Hussein. That is the crux of the 9/11 conspiracy theories. Paul Wolfowitz, Donald Rumsfeld, Dick Cheney, brother of the President Jeb Bush co-founded in 1997 the Project for the New American Century - PNAC - an organization preparing the intellectual background of the future neoconservative administration. In the autumn of 2000, at the time of the election campaign, the authors of the project published a report entitled *Rebuilding America's Defences*. It was a call to strengthen the US military domination in the world and for a kind of remilitarization after years

[55] P. Łepkowski, "11 września 2001 roku: Dzień, który zmienił świat", *Rzeczpospolita*, 11 IX 2020 r., https://www.rp.pl/Historia/309099993-11-wrzesnia-2001-roku-Dzien-ktory-zmienil-swiat.html [access: 12 IX 2020].

[56] R. Nogacki, "World Trade Center – Czy Żydzi wiedzieli wcześniej?", *Nasza Witryna*, 6 VI 2013, https://web.archive.org/web/20130606091550/http://www.naszawitryna.pl/przewodnia_sila_19.html [access: 9 VI 2021].

of relaxation caused by the end of the Cold War. The authors expressed the opinion that without a new Pearl Harbor, such remilitarization would be a difficult and slow process. Without war, undisciplined Americans would not want to provide for a global empire. According to this logic, war is necessary, and in order to persuade the society to it, a "second" Pearl Harbor is required. The World Trade Center towers, America's icons, were perfect for the "new" Pearl Harbor. The war in Iraq was supposed to be a milestone in the implementation of "Pax Americana" in the oil-bearing Persian Gulf.[57]

The most incredible interpretations of the events of 9/11 have many supporters and dismiss some of the arguments of the more balanced conspiracy theoreticians. The respected politicians Thomas H. Kean and Lee H. Hamilton - chairman and co-chairman of the 9/ 11 Commission did not believe in any conspiracy theories, but they were also unsatisfied with the attitude of the government. Two years after the Commission's official report, they jointly wrote the book *Without Precedent: The Inside Story of the 9/11 Commission*. Using moderate wording they wrote about the constant struggle with the Bush administration and about the constantly new obstacles that prevented the Commission from conducting an independent investigation. The Commission report condemned the lack of decisive action by the White House in response to the CIA information that had appeared long before the attacks that suspected people were planning to hijack passenger planes. "The system was blinking red" - this is the title of the chapter in the report on signs that the administration ignored, that a serious attack on the United States was looming. However, when the attacks were over, it was surprisingly quickly established who had done them, and for what purpose. Surprisingly efficiently and quickly, the scrap metal from the WTC wreckage was disposed. Straight from Manhattan, New York, it was shipped to Chinese steelworks. The American philosopher David Ray Griffin noted that it was the official version of the events of 9/11, promoted by the government, that bore the hallmarks of a conspiracy theory.[58]

Conclusion

Both before and after 2001, terrorist attacks took place in the US and other parts of the world, but never on the scale of the 9/11 attacks. Its root causes lie in the spread of Islamic fanaticism, whose representatives usurp the right to present only themselves as "true believers" and call others "unbelievers" with whom they must fight. This was overlapped by the conviction, common in the Muslim world, that the USA was engaged on the side of Israel in the unresolved Palestinian-Israeli conflict. On top of that, the attack and the sanctions imposed on Iraq in 1991 as well as Washington's support

[57] M.A. Velez, "11 września: władza spisków", *Wirtualna Polska*, 7 IX 2006 r., https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [access: 11 IX 2006].

[58] Ibid.

for regimes in Muslim countries. Last but not least, facing the world socio-economic problems and the process of globalization, which Muslims are trying to counter, by exposing their religious distinctiveness and attachment to tradition. The United States, the richest and most economically powerful country in the world, is blamed by many communities, including Muslims, for the economic problems that have arisen in various regions of the globe. On the one hand, due to the expansion of American companies, and on the other, according to some, insufficient economic and technological aid for poor regions. Critics assume that the problem of poverty in the world is also an American problem in the sense that the United States, as a superpower, should feel even more responsible for the fate of the modern world, for example by providing aid in solving the aforementioned social and economic problems.[59] The attack on the WTC, a symbol of the economic power of the United States, was a kind of revenge for the lack of adequate US involvement in helping the poor regions of the world, primarily the Muslim one, and the attack on the Pentagon, a symbol of the US military power, was a revenge for military interventions in the Middle East.

The above comments should be followed by an explanation by Ayman az-Zawahiri, al-Qaeda ideologist and Osama bin Laden's deputy. In December 2001, in an Arabic-language newspaper issued in London, *Asharq al-Awsat* (*Middle East*), he published a manifesto entitled "Fursan taht rayat al-Nabi" ("Knights under the Prophet's Banner"). He stated, inter alia, that in the 1990s the hopes that had arisen from the victorious jihad in Afghanistan were not fulfilled. Supporters of jihad then faced a complete defeat in the entire Muslim world, as they failed to mobilize masses of Muslims to jointly overthrow the rulers in Muslim countries, described as "near enemy". Only a radical change of strategy, a devastating blow to the United States, could bring success. The boldness and scale of this attack were to convince masses of undecided Muslims of the potent power of jihadist forces and the weakness of "great America", patron of "apostates" in the Middle East and North Africa. The worldwide media coverage of the attack on the US was to mobilize Muslims who would join al-Qaeda as a vanguard leading thousands of brothers in faith to a victorious jihad against both the "near" and "distant enemy", that is, the West.[60]

The events on 11 September 2001 had a negative impact on the economy, primarily of the United States, but not only. As a result of the terrorist threat, for example, the number of tourists in the USA decreased. It was mainly the states that live off tourism, such as Florida, which - as estimated - only at the turn of 2001/2002 lost about 30 billion USD due to the decline in the number of tourists. Airlines and insurance companies also lost billions of dollars. The former owing to the reduced number of passengers, the latter due to the payment of compensation. There were numerous difficulties in international transport because of the tightening of security measures. Closer control

[59] However, it is rarely specified how this should be done. Financial aid from the US is most frequently expected. The lack of it in most cases has been the cause of anti-American riots.

[60] G. Kepel, *Fitna. Wojna w sercu islamu*, Warszawa 2006, pp. 11–12.

of international financial flows was exerted in order to identify and eliminate sources of terrorist organization financing. The 9/11 events made many countries aware that no one - even the most powerful state - can feel safe, and therefore close international cooperation is necessary in combating terrorism and in solving urgent problems of the modern world, the conflicts and tensions in the international arena.

September 11 attacks commenced a new period in the fight against international terrorism. It showed the previously unknown scope of threats posed by terrorist organizations, including the possibility of using weapons of mass destruction. The response to this type of terrorism had to be adjusted to the scale of the emerging danger. The events on 9/11 led to a breakthrough in American politics. The United States declared a war on terrorism. The first act was the attack on the Islamic Emirate of Afghanistan, i.e. the seat of the al-Qaeda ally. The US Operation Enduring Freedom complied with the United Nations Charter, which does not restrict the right to self-defence until the matter is taken over by the Security Council. The participation of other countries, including Poland, in this operation was an aid granted to the USA, as allowed by the UN Charter. In September 2002, a doctrine was adopted in the United States allowing for a preventive strike in the face of imminent threats of terrorists or possession of weapons of mass destruction by the so-called rogue states. The new doctrine was applied the following year against Iraq. However, the war on terror exposed major differences between Europe and the United States. It was not so much about the divergence in military potential and in the way of conducting warfare, but about a diverse perception of the role of international institutions and multinational forces, as well as different assessments of measures and scenarios of possible actions in the fight on terrorism.

The attack on the United States was so unexpected and shocking to both the Americans and the entire international community. Existing international security structures and organizations proved ineffective. The military force and the whole arsenal of the most advanced types of weapons were not able to ensure internal security. The United States and the world faced new threats. Many steps were taken to ensure security and eliminate international terrorism. The fight against it certainly became the main focus of the international community's activity, leading to a change in US foreign policy priorities, and intensifying the tendency towards unilateral preventive actions.

It should also be remembered that the war on terror brought enormous financial benefits to the US military-industrial complex. Already in September and October 2001, there was an increase in the share prices of such companies as Lockheed Martin, Northop Grumman and Rytheon. Military equipment manufacturers also benefited unexpectedly, not only because the West took decisive action against countries, organizations and individuals suspected of terrorism, but also from the launch of aid packages for developing countries. Every major corporation benefited from President Bush's "stimulus" package to help revive the economy. Of the 100 billion USD spent

from this package in November 2001 alone, 75 percent was allocated to subsidies covering the taxes of enterprises, especially the largest corporations.[61]

The success of 9/11 backfired on Al-Qaeda. US forces in Afghanistan failed to eliminate the leaders of this organization, who escaped to Pakistan with the help of allied Afghans. Getting hold of al-Qaeda documents and videotapes in its safe houses made it possible to better understand the structure and dynamics of this organization, and to thwart the attack in Singapore in December 2001. US forces dispersed al-Qaeda leadership, liquidated training camps and greatly reduced the possibilities of mutual communication between its members and commanders and the headquarters providing logistic support to local operations. Osama bin Laden was not eliminated until 10 years later.

The attack of Islamic terrorists on the United States showed the true colours of the societies of Muslim countries. The collapse of the WTC towers was greeted with delight of millions of Muslims in Indonesia, Malaysia, Bangladesh, India, Egypt, Sri Lanka, Oman, Yemen, Sudan, Bosnia and Herzegovina, Afghanistan, Pakistan and the United Kingdom.[62] The cheering residents on the streets of Arab cities became, in common perception, a symbol of undisguised hatred for the United States. These were shocking pictures for the Westerners, but they showed the impulsive and genuine attitude of a large part of Muslims towards America. The future has shown that Muslims who live in Europe also have a similar hatred for the whole of Western civilization. After 9/11 interest in Islam increased significantly. It was observed that many young people in Europe (and also in Poland) converted to Islam. More attention was paid to radical Islam, the ideology which gave rise to the existence and activity of extremist organizations in Muslim countries. Many of them, including al-Qaeda, had carried out bloody terrorist attacks before 2001, but it was the attack on New York and Washington that marked the turning point in the recent history of terrorism. Much of the attention of scientists and the media focused on the fundamentalist trend of Islam flooding the West with more or less reliable information. By the end of 2001 alone, about 800 books devoted to this issue had appeared in the English-language literature. The 2003 US attack on Iraq and the resurgence of the Taliban movement in Afghanistan reinforced these trends. NATO's intervention in both countries contributed to an increase in the terrorist threat in Europe, and its inhabitants became the target of Islamic extremists in Africa and Asia.

---

[61] D. Whyte, "Interesy po staremu? Moralność wielkich korporacji i 'wojna z terroryzmem'", w: *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, P. Scraton (ed.), Warszawa 2003, pp. 193–194.

[62] P.L. Williams, *Al-Kaida– bractwo*…, pp. 96–97.

Bibliography

11 września. Przyczyny i konsekwencje w opiniach intelektualistów, Scraton P. (ed.), Warszawa 2003, Dialog.

Armstrong K., *Pola krwi. Religia i przemoc*, Warszawa 2017, Wydawnictwo W.A.B.

Bergen P.L., *Osama bin Laden. Portret z bliska*, Warszawa 2007, PIW.

Chaliand G., Blin A., *Historia terroryzmu. Od starożytności do Da'isz*, Warszawa 2020, PIW.

Coll S., *Rodzina Bin Ladenów. Arabskie losy w amerykańskim stuleciu*, Warszawa 2015, Kurhaus Publishing.

Dietl W., Hirschmann K., Tophoven R., *Terroryzm*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Elsässer J., *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007, MUZA.

Izak K., "Fałszywe dokumenty w rękach terrorystów", *Człowiek i Dokumenty* 2014, no. 32, p. 7–20.

Kepel G., *Fitna. Wojna w sercu islamu*, Warszawa, Warszawa 2006, Dialog.

Streatfeild D., Świat po 11 września, Warszawa 2011, Oficyna Wydawnicza ŁośGraf.

Szymańska M., "Eksplozja terroryzmu w USA a przekształcenia w amerykańskich służbach specjalnych po 11 września 2001 r.", *Bezpieczeństwa Wewnętrznego* 2014, no. 10, pp. 186–210.

Whyte D., "Interesy po staremu? Moralność wielkich korporacji i 'wojna z terroryzmem'", w: *11 września. Przyczyny i konsekwencje w opiniach intelektualistów*, Scraton P. (ed.), Warszawa 2003, Dialog, pp. 187–194.

Williams P.L., *Al-Kaida – bractwo terroru*, Warszawa 2002, Studio Emka.

Wright L., *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, Wydawnictwo Czarne.

Internet sources

https://en.wikipedia.org/wiki/Abdulaziz_al-Omari [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Ahmed_al-Nami [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Ahmed_al-Ghamdi [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Hani_Hanjour [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Mohamed_Atta [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Salem_al-Hazmi [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Satam_al-Suqami [access: 1 VI 2021].

https://en.wikipedia.org/wiki/Zacarias_Moussaoui [access: 1 VI 2021].

https://pl.melayukini.net/wiki/Betty_Ong [access: 1 VI 2021].

https://pl.melayukini.net/wiki/Hamza_al-Ghamdi [access: 4 VI 2021].

https://pl.melayukini.net/wiki/Hani_Hanjour [access: 4 VI 2021].

https;//pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks [access: 4 VI 2021].

https://pl.melayukini.net/wiki/Hijackers_in_the_September_11_attacks#American_Airlines_Flight_11:_One_World_Trade _Center,_North_Tower [access: 3 VI 2021].

https://pl.melayukini.net/wiki/Madeline_Amy_Sweeney [access: 1 VI 2021].

https://pl.melayukini.net/wiki/Marwan_al-Shehhi [access: 4 VI 2021].

https://pl.melayukini.net/wiki/Nawaf_al-Hazmi [access: 4 VI 2021].

https://pl.melayukini.net/wiki/Satam_al-Suqami [access: 1 VI 2021].

https://pl.melayukini.net/wiki/Wail_al-Shehri [access: 1 VI 2021].

https://pl.melayukini.net/wiki/Ziad_Jarrah [access: 4 VI 2021].

https://pl.wikipedia.org/wiki/Katastrofa_lotu_American_Airlines_11 [access: 1 VI 2021].

https://pl.wikipedia.org/wiki/Katastrofa_lotu_United_Airlines_93 [access: 4 VI 2021].

https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [access: 7 VI 2021].

https://pl.xcv.wiki/wiki/United_Airlines_Flight_175 [access: 4 VI 2021].

Krzemirski A., "Rocznica 11 września. Olbrzymie odszkodowania i strach przed podróżami", *Parkiet*, 11 IX 2002, https://www.parkiet.com/artykul/260530.html [access: 6 VI 2021].

Kucharczyk M., "Wybuch, który miał zatrzeć ślady wielkiego spisku. Ta teoria o zamachach na WTC wciąż ma się dobrze", *Gazeta.pl*, 11 IX 2020, https://wiadomosci.gazeta.pl/wiadomosci/7,114881,26286855,kontrolowany-wybuch-ktory-mial-zatrzec-slady-ta-teoria-o-zamachach.html [access: 12 IX 2020].

Lichtenberg A., Dudek B., "Zamachy 11 września: historia 'Grupy Hamburskiej'", *Deutsche Welle* https://www.dw.com/pl/zamachy-11-września-historia-grupy-hamburskiej/a-15379511 [access: 12 IX 2011].

Łepkowski P., "11 września 2001 roku: Dzień, który zmienił świat", *Rzeczpospolita*, 11 IX 2020, https://www.rp.pl/Historia/309099993-11-wrzesnia-2001-roku-Dzien-ktory-zmienil-swiat.html [access: 12 IX 2020].

"Nieśli pomoc po ataku na WTC, po latach ciężko zachorowali. Śmierć strażaków - ojca i syna - w wyniku nowotworów", *Polsat News*, 19 VIII 2017, https://www.polsatnews.pl/wiadomosc/2017-08-19/niesli-pomoc-po-ataku-na-wtc-smierc-strazakow-w-wyniku-nowotworow/ [access: 6 VI 2021].

Nogacki R., "World Trade Center – Czy Żydzi wiedzieli wcześniej?", *Nasza Witryna*, 6 VI 2013, https://web.archive.org/web/20130606091550/http://www.naszawitryna.pl/przewodnia_sila_19.html [access: 9 VI 2021].

"Piecing together the terrorist jigsaw", *The Guardian*, 15 X 2001 https://www.theguardian.com/world/2001/oct/15/worlddispatch.brianwhitaker [access: 17 I 2001].

"Rodziny ofiar zamachów na WTC z 11 września pozywają Arabię Saudyjską", *Bankier.pl*, 21 III 2017, https://www.bankier.pl/wiadomosc/Rodziny-ofiar-zamachow-na-WTC-z-11-wrzesnia-pozywaja-Arabie-Saudyjska-3668756.html [access: 22 III 2017].

"Spisek World Trade Center", *Laif*, 9 V 2008, https://web.archive.org/web/20090615224350/http://laif.co.uk/art,spisek_world_trade_center,1496.html [access: 9 VI 2021].

"USA: Kongres ujawnił tajną część raportu o zamachach z 11 września", *Dziennik Gazeta Prawna*, 15 VII 2016, https://www.gazetaprawna.pl/wiadomosci/artykuly/960454,usa-kongres-ujawnil-tajna-czesc-raportu-o-zamachach-z-11-wrzesnia.html [access: 16 VII 2016].

Velez M.A., "11 września: władza spisków", *Wirtualna Polska*, 7 IX 2006, https://wiadomosci.wp.pl/11-wrzesnia-wladza-spiskow-6036234217149057a [access: 11 IX 2006].

Werkhäuser N., "Hamburg: pomocnik zamachowców z 11 września wydalony do Maroka", *Deutsche Welle*, 15 X 2018, https://www.dw.com/pl/hamburg-pomocnik-zamachowców--z-11-września-wydalony-do-maroka/a-45895869 [access: 16 X 2018].

"We have some planes", *National Commission on terrorist attacks upon the United States*, https://www.9-11commission.gov/report/911Report_Ch1.htm [access: 3 VI 2021].

The 9/11 Commission Report, https://govinfo.library.unt.edu/911/report/911Report.pdf, [access: 6 VI 2021].

Abstract

The series of terrorist attacks on 11 September 2001 in the USA, the largest in the history of the world, was carried out by 19 people. Among them were 15 Saudis, two UAE nationals, a Lebanese and an Egyptian. Three of the four formed the Hamburg cell, which was the backbone of the entire plot. It was led by the Egyptian Muhammad Atta el-Sayed. He flew Boeing 767 aircraft American Airlines Flight 11, which first struck the North Tower of the WTC. Marwan al-Shehhi was the pilot of Boeing 767 aircraft United Airlines Flight 175, which crashed into the South Tower of the WTC. Hani

Hanjour sat at the controls of the Boeing 757 aircraft American Airlines flight 77. It was the third machine to target the Pentagon. The pilot of the fourth plane - Boeing 757 aircraft United Airlines Flight 93 - Ziad Jarrah failed to reach his destination, possibly the Capitol, because the passengers decided to take over the control of the plane from the terrorists. The machine crashed in Pennsylvania. In the events of 9/11, a total of 2,996 people were killed, including 19 terrorists, and 6,291 were injured[63]. Six Poles were among the fatalities. 343 firefighters died in the rescue operation.

The attacks caused enormous material losses. Particularly high costs were incurred by insurance and reinsurance companies, airlines and aircraft manufacturers, as well as the tourism industry. The huge losses related to the destruction of the New York City World Trade Center and the disruption of the financial system had to be covered by insurance companies involved in the operations on the American market.

The terrorist attack on the USA was the impetus for the largest reform of the American secret services since 1947. Washington made a decision regarding the need to create a system that would effectively counteract terrorist threats and effectively warn in the event of their occurrence. This was related to the strengthening of structures with operational and reconnaissance powers, increasing the scope of their tasks and improving their ability to coordinate. Most of the legal regulations were expressed in the document commonly known as the USA Patriot Act of 26 October 2001. The most critical, however, were the international repercussions. By the attacks on the WTC and the Pentagon, al-Qaeda influenced world politics by prompting Washington to declare a "war on terror". Within its framework, American forces, supporting the so-called Northern Alliance led to the collapse of the Islamic Emirate of Afghanistan, and then entered Iraq, which in the long run turned out to be one of the most spectacular and deadly strategic mistakes in the history of the military.

At the same time the September 11 attacks sparked many conspiracy theories. Their propagation in the media, in documentaries, as well as in articles, contributed to undermining trust in the American government. An organization called Architects and Engineers for 9/11 Truth which boasts 3.3 thousand architects and engineers from all over the United States, is still very active in researching the case of 7 WTC. Its mission is to establish the truth that the twin towers did not collapse due to the impact of terrorist-piloted planes, as well as the destruction of WTC 7 was not a result of the detachment of a fragment of the second plane. In the opinion of members of this organisation, the damage caused by the planes was far from sufficient to lead to such a catastrophe. They believe someone must have planted explosives.

Keywords: Al-Qaeda, terrorist attack, Hamburg cell, Pentagon, WTC.

[63] https://pl.wikipedia.org/wiki/Zamach_z_11_września_2001_roku [access: 7 VI 2021].

O autorach

Robert Borkowski – doktor habilitowany, profesor nadzwyczajny Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Członek Rady Naukowej Centrum Badań nad Terroryzmem.

Bogusław Cacko – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Izabela Dąbrowska – absolwentka Akademii Sztuki Wojennej, laureatka X edycji ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Paweł Gacek – doktor nauk prawnych, funkcjonariusz Komendy Głównej Policji.

Dariusz Gradzi – adwokat, kancelaria adwokacka AKGK Adwokaci Kostański Gradzi Kuczara s.c.

Maciej Gurtowski – doktor nauk społecznych w dziedzinie socjologii. Pracownik Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej w Warszawie. Ekspert ds. bezpieczeństwa Centrum Analiz Klubu Jagiellońskiego.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Daniel Damian Kasprzycki – doktor nauk o bezpieczeństwie, Dolnośląska Szkoła Wyższa we Wrocławiu. Ekspert w dziedzinie bezpieczeństwa międzynarodowego, współczesnych konfliktów zbrojnych i zagrożeń hybrydowych, ze szczególnym uwzględnieniem Europy Wschodniej i Bliskiego Wschodu.

Rafał Jerzy Kruszyński – doktor nauk prawnych, radca prawny, wykładowca akademicki. Ekspert w dziedzinie krajowego i międzynarodowego prawa gospodarczego oraz praw człowieka.

Remigiusz Lewandowski – doktor, ekspert w dziedzinie bezpieczeństwa ekonomicznego, identyfikacyjnego i cyberbezpieczeństwa. Naukowo związany z Wydziałem Nauk Ekonomicznych i Zarządzania Uniwersytetu Mikołaja Kopernika w Toruniu oraz Wydziałem Bezpieczeństwa Narodowego Akademii Sztuki Wojennej w Warszawie.

Piotr Mickiewicz – profesor zwyczajny w Instytucie Politologii Uniwersytetu Gdańskiego, wiceprezes ds. naukowych Polskiego Towarzystwa Geopolitycznego (kadencja 2020–2023). Redaktor naczelny „Rocznika Bezpieczeństwa Międzynarodowego".

Łukasz Skoneczny – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Jan Waszewski – doktor nauk społecznych w dziedzinie socjologii. Pracownik Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej w Warszawie. Zajmuje się naukowo systemami zautomatyzowanego nadzoru.

Rafał Wądołowski – doktor nauk prawnych, radca prawny, Kancelaria Radcy Prawnego Rafał Wądołowski.

Jacek Michał Wojciechowski – doktor, laureat X edycji ogólnopolskiego konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych. Obecnie naukowo związany z Państwową Uczelnią Zawodową we Włocławku.

About the authors

Robert Borkowski – PhD with post-doctoral degree, associate professor of the Andrzej Frycz Modrzewski Krakow University, member of the Scientific Board of the Terrorism Research Center.

Bogusław Cacko – officer of the Internal Security Agency.

Izabela Dąbrowska – graduate of the War Studies University, laureate of the 10th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats.

Paweł Gacek – PhD in law. Police officer in the Police Headquaters.

Dariusz Gradzi – Attorney at law, AKGK law firm.

Maciej Gurtowski – PhD in Social Sciences. Employed at Security Research Centre at the War Studies University in Warsaw. Expert in security at the Centre for Analysis at the Jagiellonian Club.

Krzysztof Izak – retired officer of the Internal Security Agency.

Daniel Damian Kasprzycki – PhD in security studies at the University of Lower Silesia in Wrocław. Expert in international security, contemporary military conflicts and hybrid threats especially in Eastern Europe and Middle East.

Rafał Jerzy Kruszyński – PhD in law, legal counsel, university lecturer. Expert in domestic and international economic law and human rights.

Remigiusz Lewandowski – PhD, expert in economy, identity and cyber security. A scholar cooperating with the Faculty of Economic Sciences and Management at the Nikolaus Copernicus University in Toruń and with the Faculty of Internal Security at the War Studies University in Warsaw.

Piotr Mickiewicz – professor at the Institute of Political Sciences at University of Gdańsk, vice-president for science of the Polish Geopolitical Society (term of office 2020–2023). Editor-in-chief of the annual Rocznik Bezpieczeństwa Międzynarodowego devoted to international security.

Łukasz Skoneczny – officer of the Internal Security Agency.

Jan Waszewski – PhD in social sciences. He is employed at Security Research Centre at the War Studies University in Warsaw. He pursues research in automated surveillance systems.

Rafał Wądołowski – PhD in law, attorney-at-law, Law Firm of Attorney-at-Law Rafał Wądołowski.

Jacek Michał Wojciechowski – PhD, laureate of the 10th edition of the Head of the Internal Security Agency national contest for the best doctoral, master's or bachelor's thesis on state security in the context of intelligence, terrorist and economic threats. Currently academic at the Higher Vocational School at Włocławek.

Informacje dla autorów

I. Zasady przyjmowania prac.

1. Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego przyjmuje do publikacji w półroczniku „Przegląd Bezpieczeństwa Wewnętrznego" (PBW) artykuły naukowe dotyczące bezpieczeństwa wewnętrznego i porządku konstytucyjnego państwa.
2. Materiały do PBW należy składać przez elektroniczny Panel Redakcyjny dostępny pod adresem: https://ojs.ejournals.eu/PBW/about/submissions.
3. Materiały należy przesłać w terminach: do 30 września (wydanie kwietniowe) oraz do 30 marca (wydanie listopadowe).
4. Przesyłając tekst do wydawnictwa ABW, autor wyraża zgodę na jego opracowanie redakcyjne, tj. na wykonanie redakcji merytorycznej, językowej, technicznej i korekty, zgodnie z normami językowymi oraz na podstawie polskich norm wydawniczych. Wyraża także zgodę na opublikowanie informacji o artykule w naukowych bazach danych i na stronie internetowej Agencji Bezpieczeństwa Wewnętrznego.
5. Autorzy artykułów, które zostaną opublikowane w PBW, podpisują umowę o przeniesieniu na wydawcę autorskich praw majątkowych.
6. Autorzy artykułów opublikowanych w PBW otrzymują honoraria.
7. W przypadku utworu stworzonego przez kilka osób każda z nich jest zobowiązana do wypełnienia *Oświadczenia o wkładzie poszczególnych autorów w powstanie publikacji* (wzór oświadczenia jest dostępny na stronie wydawnictwa ABW, pod adresem: https://abw.gov.pl/wyd/przeglad-bezpieczenstwa/materialy-do-pobrania/1763,Materialy-do-pobrania.html) i przesłania go w wersji elektronicznej (skan) na adres e-mail: wydawnictwo@abw.gov.pl.
8. Autorzy są zobowiązani do wypełnienia *Formularza zgody autora na publikację artykułu w czasopiśmie PBW* (wzór formularza jest dostępny na stronie wydawnictwa ABW, pod adresem: https://abw.gov.pl/wyd/przeglad-bezpieczenstwa/materialy-do-pobrania/1763,Materialy-do-pobrania.html) i przesłania go w wersji elektronicznej (skan) na adres e-mail: wydawnictwo@abw.gov.pl.
9. Autorzy przesyłający artykuły do PBW są zobowiązani do podawania numerów ORCID.
10. Wydawnictwo nie zwraca autorom nadesłanych artykułów oraz zastrzega sobie możliwość odmowy ich publikacji bez podania przyczyny.

II. Przygotowanie tekstów.

1. Wszystkie teksty należy przesyłać w postaci elektronicznej (Word).
2. Do artykułu należy dołączyć:
   a) bibliografię załącznikową,
   b) abstrakty w języku polskim i angielskim nieprzekraczające 15 wierszy wydruku komputerowego,
   c) słowa kluczowe w języku polskim i angielskim.
   d) notkę o autorze (zawód lub tytuł naukowy, miejsce pracy).
3. Wszelkie grafiki, zdjęcia oraz schematy powinny być dołączone w oddzielnych, oryginalnych plikach. Ich wymiary powinny być nie mniejsze, niż te, które mają być uzyskane po wydruku, oraz możliwie jak najlepszej jakości (rozdzielczość 300 dpi w skali 1:1). W przypadku dostarczenia ilustracji złej jakości redakcja zastrzega sobie prawo do ich niezamieszczania.

III. Normalizacja tekstu.

1. Marginesy: 2,5 cm z każdej strony.
2. Czcionka tekstu głównego: Times New Roman 12 pkt; interlinia 1,0.
3. Czcionka przypisów: Times New Roman 10 pkt; interlinia 1,0.
4. Objętość artykułu zgłaszanego do publikacji (wraz z bibliografią, abstraktami i słowami kluczowymi) nie może przekraczać 15 stron wydruku komputerowego w formacie A4, recenzji – 10 stron.
5. Tekst powinien być wyjustowany.
6. Tytuł, podtytuł i śródtytuły: Times New Roman, bold.
7. Rysunki i fotografie należy lokalizować w tekście głównym za pomocą podpisów.
8. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itp.).
9. Nie należy stosować tzw. twardych spacji i miękkich enterów.

Cytaty i wyróżniki.

1. Cytaty o długości do 5 wersów należy zapisywać kursywą, dłuższe należy wyróżniać wcięciem z obu stron, czcionka prosta, 11 pkt.
2. Cytaty obcojęzyczne powinny być przetłumaczone w przypisie (tłumaczy autor tekstu).
3. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie półokrągłym.
4. Uzupełnienia i komentarze odautorskie w cytacie należy podawać w nawiasie kwadratowym.
5. Jeśli w obrębie jednego cudzysłowu występuje drugi cudzysłów, do jego wyodrębnienia należy stosować znak «».

Zapis nazwisk.

1. W tekście głównym nazwiska osób przywoływanych po raz pierwszy należy podawać w pełnym brzmieniu (rozwijać inicjały imion, jeśli to możliwe); później należy podawać samo nazwisko.
2. Jeśli dwie postaci noszą to samo nazwisko (np. Jan i Jędrzej Śniadeccy), w przypadku gdy nie jest oczywiste, o której z nich mowa, należy powtórzyć imię lub wskazać tę osobę za pomocą omówienia.

Skróty.

1. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp. przy ich pierwszym pojawieniu się w tekście (w nawiasie należy podać skrót nazwy, jeśli będzie przywoływana w dalszej części tekstu). Należy wprowadzać jeden skrót dla jednej nazwy.
2. Skróty należy stosować konsekwentnie – jeśli skrót został wprowadzony, od tego miejsca zastępuje on w tekście daną nazwę za każdym razem, gdy ona się pojawia.

IV. Przypisy.

1. Przypisy należy umieszczać na dole strony.
2. Przypisy w tabelach mają numerację oddzielną od przypisów w tekście głównym.
3. Tytuły prac cytowanych po raz pierwszy należy podawać w przypisie w pełnym brzmieniu. Zawsze należy podawać podtytuł publikacji. Przy kolejnym przywołaniu tytuł należy skrócić do czytelnej postaci, dodając wielokropek i rezygnując z podawania ponownie miejsca i roku wydania. W przypadku cytowania publikacji obcojęzycznej – tytuł i dane bibliograficzne podajemy w języku publikacji.
4. W przypisach konsekwentnie należy stosować następujące oznaczenia: tenże/taż, tamże, tłum., wstęp, posł., (red.), oprac., i in., t., cz., z., nr, [bmw] – brak miejsca wydania, [bdw] – brak daty wydania, [bmdw] – brak miejsca i daty wydania, zob., por., zob. szerzej: (z dwukropkiem), za: (z dwukropkiem), i nast.
5. W przypadku większej niż trzech liczby autorów (redaktorów, tłumaczy) należy podać inicjał (inicjały) imienia i nazwisko alfabetycznie pierwszego z nich i dodać do niego skrót: i in.
6. W przypadku dwóch lub trzech miejsc wydania (miejscowości), należy je zapisywać z myślnikami (np. Wrocław–Kraków).
7. Jeśli imię zaczyna się dwuznakiem (np. Sz, Cz), należy zapisać tylko pierwszą literę; wyjątkiem jest Ch.
8. Nie należy stosować skrótów: op. cit., lok., cit., ibidem.

Struktura przypisów.

1. **Przypis archiwalny:**
   pełna nazwa archiwum (gdy pojawia się po raz pierwszy) i w nawiasie formułka „dalej:" oraz proponowany skrót tej nazwy do stosowania za każdym kolejnym razem, 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:

   Archiwum Instytutu Pamięci Narodowej, Oddziałowe Biuro Udostępniania i Archiwizacji Dokumentów w Krakowie (dalej: AIPN, OBUiAD w Krakowie), IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57.

   APK, UWSl. (skrót, gdy wcześniej pojawiła się pełna nazwa miejsca przechowywania źródła), sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r., 5 I 1929 r., k. 57.

2. **Książka:**
   inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, miejsce i rok wydania, strona (ew. zakres stron). W przypadku książki pod redakcją po tytule książki podajemy inicjał imienia i nazwisko redaktora, następnie: miejsce i rok wydania, strona.

   PRZYKŁADY:

   B. Prus, *Lalka*, Wrocław 1998, s. 100–200.
   Polszczyzna na *co dzień*, M. Bańko (red.), Warszawa 2006, s. 420.

3. **Publikacja w pracy zbiorowej:**
   inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), w: *tytuł pracy zbiorowej* (kursywą), numer tomu (jeśli jest), inicjał imienia i nazwisko redaktora, miejsce i rok wydania, strona.

   PRZYKŁAD:

   W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, s. 36.

4. **Artykuł w zbiorze tego samego autora:**
   inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), w: tenże/taż, *tytuł zbioru* (kursywą), numer tomu, miejsce i rok wydania, strona.

PRZYKŁAD:

M. Janion, *Apokalipsa bez zbawienia. Tematy jeanpaulowskie*, w: taż, *Żyjąc, tracimy życie. Niepokojące tematy egzystencji*, Warszawa 2001, s. 15, 17.

5. **Artykuł w czasopiśmie:**
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), „Tytuł Czasopisma", rok wydania, numer w danym roku, zeszyt ew. część (w opisie należy stosować cyfry arabskie), strona.

PRZYKŁAD:

W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13.

5. **Artykuł w dzienniku:**
inicjał imienia i nazwisko autora artykułu, *tytuł* (kursywą). *Podtytuł* (kursywą), „Tytuł Dziennika" , data dzienna.

PRZYKŁAD:

J. Kowalski, *Energia wiatrowa. Nowe możliwości*, „Rzeczpospolita", 2 III 2020 r.

6. **Artykuły lub dokumenty zamieszczone na stronach internetowych:**
inicjał imienia i nazwisko autora, *tytuł artykułu* (*dokumentu*) (kursywą). *Podtytuł* (kursywą), ew. nazwa portalu, data publikacji na stronie, adres internetowy, w nawiasie kwadratowym informacja o dacie dostępu.

PRZYKŁAD:

B. Sajduk, *Chiński krok w stronę bałkanizacji Internetu*, Nowa Konfederacja, 14 IX 2020 r., https://nowakonfederacja.pl/chinski-krok-w-strone-balkanizacji-internetu/ [dostęp: 29 III 2021].

V. Bibliografia załącznikowa.

1. Przy sporządzaniu bibliografii załącznikowej kolejne pozycje należy szeregować w porządku alfabetycznym.
2. Rekomendowany format bibliografii załącznikowej:

Kowalski W., *Służba 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, s. 32–47.

Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014.

3. Należy podać osobno: pozycje zapisywane alfabetem niełacińskim (np. literatura rosyjska), źródła internetowe, materiały archiwalne, akty prawne i orzecznictwo.
4. Akty prawne należy szeregować według hierarchii przyjętej dla tego typu dokumentów, tj. w porządku:
   – konstytucja,
   – ratyfikowane umowy międzynarodowe,
   – rozporządzenia, dyrektywy i decyzje UE,
   – ustawy i rozporządzenia z mocą ustawy,
   – rozporządzenia,
   – akty prawa miejscowego.