PAŹDZIERNIK 2015

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

WYDANIE SPECJALNE

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

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

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WYDANIE SPECJALNE

Warszawa 2015

Zespół redakcyjny: dr Zbigniew Nawrocki (redaktor naczelny)
Damian Szlachter (sekretarz Redakcji)
Izabela Laskus, Grażyna Osuchowska,
Anna Przyborowska (redakcja i korekta)
Maciej Śliwiński (skład)

Redaktor tematyczny: Antoni Podolski

Projekt okładki: Katarzyna Głowacka

ISNN 2080-1335

Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

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

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

Numer zamknięto i oddano do druku w październiku 2015 r.

Druk:
Drukarnia ART
ul. Fortuny 5
01-339 Warszawa

Spis treści

Wstęp

Prezentujemy Państwu wydanie specjalne „Przeglądu Bezpieczeństwa Wewnętrznego" poświęcone problematyce dotyczącej tzw. wojen hybrydowych. Termin wojna hybrydowa, który zaczął pojawiać się w publikacjach amerykańskich po roku dwutysięcznym, został szczególnie upowszechniony od momentu anektowania Krymu przez Rosję. Od tej pory w powszechnej opinii stał się słowem kluczem mającym symbolizować nowy typ wojny, rodzaj zagrożenia, który co prawda dotychczas występował, ale obecnie został na nowo zdefiniowany. Rosjanie jednak postrzegają wojny hybrydowe jako skutek… rozwoju amerykańskich technologii mający na celu osłabienie strategicznych oponentów USA (vide: „kolorowe rewolucje").

Już sama definicja „wojny hybrydowej" jest niejasna i budzi spory wśród ekspertów. Trudno precyzyjnie określić, czy jest to kombinacja strategii i taktyki zmierzająca do wymieszania różnych typów działań zbrojnych, czy wynik konwergencji zasad wojny konwencjonalnej i operacji specjalnych. A może jest to kombinacja wojny symetrycznej i asymetrycznej lub tylko nowe pojęcie dla określenia tradycyjnych metod wywoływania i podtrzymywania konfliktów, tyle że rozgrywanych z wykorzystaniem nowoczesnych narzędzi (np. działań w cyberprzestrzeni), często bez użycia środków militarnych?

Jak zatem określić konflikt rosyjsko-ukraiński toczący się w sąsiednim kraju, z którym łączy nas granica o długości ponad pół tysiąca kilometrów? Otóż bez względu na to, czy pojęcie „wojny hybrydowej" to wytwór amerykański, czy na nowo zdefiniowane działania rosyjskie stosowane przez tę stronę od wieków i czy rzeczywiście jest to nowy typ wojny, czy tylko stosowane tu technologie są nowe – wojna jest po prostu wojną albo – jak chce Clausewitz – kontynuacją polityki innymi środkami.

Zagadnienia poruszone w niniejszym wydaniu „Przeglądu Bezpieczeństwa Wewnętrznego" nie wyczerpują tematu wojen hybrydowych. Nie odnieśliśmy się tu m.in. do perspektywy działań hybrydowych prowadzonych przez Państwo Islamskie w sytuacji masowego napływu ludności muzułmańskiej do Europy. Jest to, naszym zdaniem, temat zasługujący na powstanie odrębnej publikacji. Skupiliśmy się natomiast na konflikcie rosyjsko-ukraińskim, który od miesięcy przykuwa uwagę i niewątpliwie zachwiał naszym dotychczasowym poczuciem bezpieczeństwa, stawiając tę kwestię w zupełnie nowym świetle.

Na zakończenie pragnę serdecznie podziękować Panu Ministrowi Markowi Biernackiemu, który był pomysłodawcą, a następnie życzliwym recenzentem niniejszego wydania. Mam nadzieję, że spotka się ono z zainteresowaniem Czytelników.

Szef
Agencji Bezpieczeństwa Wewnętrznego

gen. bryg. Dariusz Łuczak

Michał Wojnowski

Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku

Zaplecze nieprzyjaciela – oto teren, na którym rozgrywają się istotne walki Rosji ze światem zewnętrznym, gdzie Rosja odnosi zwycięstwa lub przegrywa. To co następuje potem, bywa tylko finałem absorbującym uwagę, lecz najmniej ważnym i najmniej istotnym[1].

Włodzimierz Bączkowski

(1905−2000)

Wstęp

Aneksja Półwyspu Krymskiego oraz będąca jej następstwem „wojna noworosyjska" stały się przedmiotem szerokiego zainteresowania zachodnich mediów oraz profesjonalnych ośrodków analitycznych funkcjonujących w państwach członkowskich NATO i na zachodniej Ukrainie. W opinii większości z nich działania rosyjskie stanowią nową formę zagrożenia bezpieczeństwa, którą określono mianem wojny hybrydowej (ang. '*hybrid warfare*')[2].

Mając na uwadze odrębną tożsamość cywilizacyjną państwa rosyjskiego, należy zadać pytanie, czy ocena przebiegu operacji krymskiej i działań prowadzonych przez Federację Rosyjską (dalej: FR) wobec Ukrainy, dokonywana przez pryzmat wykładni zachodniej myśli wojskowej, odzwierciedla rzeczywistą specyfikę rosyjskiej sztuki wojennej?

Celem niniejszego opracowania jest próba udzielenia odpowiedzi na to pytanie przez wskazanie, że pojęcie oraz koncepcja wojny hybrydowej są obce rosyjskiej teorii i praktyce wojskowej, co zostanie omówione w pierwszej części artykułu.

Działania prowadzone przez FR na południowym wschodzie państwa ukraińskiego noszą znamiona praktycznego wykorzystania znanych z przeszłości metod charakterystycznych dla rosyjskiej wojskowości, które obecnie wzbogacono o nowe rozwiązania technologiczne. Aby to ocenić, konieczne jest przedstawienie analogii między teoretycznymi aspektami tych działań a praktyką, co stanowi temat drugiej części opracowania.

---

[1] Cyt. za: W. Bączkowski, *Rosja wczoraj i dziś. Studium historyczno-polityczne*, Jerozolima 1946, s. 40.

[2] Zob. dla przykładu: H. Reisinger, A. Golz, *Hybrider Krieg in der Ukraine. Russlands Intervention und die Lehren für die NATO*, „Osteuropa" 2014, nr 9–10, s. 119–134; O. Tamminga, *Hybride Kriegsführung. Zur Einordnung einer aktuellen Erscheinungsform des Krieges*, „Stiftung Wissenschaft und Politik Aktuell" 2015, nr 27, s. 1–4; C. Major, Ch. Mölling, *Eine hybride Sicherheitspolitik für Europa. Resilienz, Abschreckung und Verteidigung als Leitmotive*, „Stiftung Wissenschaft und Politik Aktuell" 2015, nr 31, s. 1–4; D. Mastriano, D. O'Malley, *A U.S. Army War College Analysis of Russian Strategy in Eastern Europe, an Appropriate U.S. Response, and the Implications for U.S. Landpower*, Carlisle 2015, s. 47–57. Por. V. Usenko, D. Usenko, *Russian Hybrid Warfare: What are Effects-Based Network Operations and how to Counteract Them* [online], http://euromaidanpress.com/2015/01/17/russian-hybrid-warfare-what-are-effect-based-network-operations-and-how-to-counteract-them/ [dostęp: 1 IX 2015].

Antycypując wyniki dalszych rozważań i biorąc pod uwagę ogromny dorobek rosyjskiej myśli wojskowej oraz czynnik mentalnościowy rosyjskiej kultury strategicznej, należy podkreślić, że ocena konfliktu rosyjsko-ukraińskiego przez pryzmat stworzonego na Zachodzie paradygmatu wojny hybrydowej wydaje się niepełna i nieobiektywna. Co więcej, w świetle tych czynników nie wydaje się możliwe stworzenie uniwersalnego wzorca (w opinii zachodnich ekspertów jest nim właśnie wojna hybrydowa), który miałby rzekomo charakteryzować rosyjskie metody prowadzenia konfliktów.

Wojna hybrydowa na Zachodzie i w Rosji

Koncepcja wojny hybrydowej w wojskowości krajów członkowskich NATO

Po raz pierwszy pojęcie „wojna hybrydowa" pojawiło się w amerykańskiej myśli wojskowej. Zyskało ono popularność dzięki narracji dotyczącej kryzysu izraelsko-libańskiego, czyli konfliktu między Izraelem a organizacją Hezbollah, który trwał od 12 lipca do 14 sierpnia 2006 r.[3] Zaczęto je także stosować w kontekście kryzysu rosyjsko-ukraińskiego. Początkowo, podejmując próby scharakteryzowania rosyjskich działań na Ukrainie, posługiwano się takimi określeniami, jak „wojna nieliniowa" (ang. '*non-linear war*') i „wojna specjalna" (ang. '*special war*'). Do połowy lata 2014 r. termin „wojna hybrydowa" nie pojawiał się w oficjalnych wypowiedziach przedstawicieli NATO ani w rezolucjach sojuszu. Po raz pierwszy w odniesieniu do rosyjskiego sposobu prowadzenia działań na Ukrainie nieoficjalnie użył tej nazwy holenderski generał Frank van Kappen, który 26 kwietnia 2014 r. nazwał rosyjskie operacje „hybrydowymi". W dniu 3 lipca 2014 r. władze Paktu Północnoatlantyckiego oficjalnie ogłosiły, że wojna na południowym wschodzie państwa ukraińskiego to wojna hybrydowa[4].

Należy podkreślić, że definicja wojny hybrydowej jest niejasna i budzi spory wśród ekspertów. Zakres jej desygnatów nie jest stały i ulega ciągłym zmianom. Opinię tę potwierdza analiza kilku definicji zaczerpniętych z aktów normatywnych oraz opracowań autorstwa zachodnich i ukraińskich badaczy. Według nich pojęcie wojny hybrydowej należy rozumieć jako:

- syntezę środków charakterystycznych dla walki zbrojnej prowadzonej metodami konwencjonalnymi i działań o charakterze nieregularnym[5],
- działania polegające na wykorzystaniu środków militarnych i niemilitarnych zintegrowanych w operacji, która ma zaskoczyć nieprzyjaciela, a potem umożliwić przejęcie inicjatywy i osiągnięcie korzyści przez oddziaływanie psychologiczne. W tym celu na dużą skalę są wykorzystywane działania dyplomatyczne, informacyjne i radioelektroniczne. Prowadzi się także operacje w cyberprzestrzeni, ukrywając jak najdłużej działania wojskowe i wywiadowcze, co następuje w połączeniu z wywieraniem silnej presji ekonomicznej[6].

[3] T. McCulloh, R. Johnson, *Hybrid Warfare. JSOU Report 13-4*, Florida 2013, s. 1–19.

[4] A. Rácz, *Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, Helsinki 2015, s. 41.

[5] *Hybrid Warfare. Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee of Armed Services, House of Representatives, GAO Report 10 – 1036 R, September 10, 2010*, w: *Terrorism. Commentary of Security Documents. Volume 127: The Changing Nature of War*, K.E. Boon, A. Huq, D.C. Lovelace (red.), Oxford 2012, s. 45–46.

[6] *Hybrid Warfare. Challenge and Response*, „The Military Balances" 2015, nr 115, s. 18–19. Por. F.G. Hoffman, *Conflicts in the 21th Century: The Rise of Hybrid Wars*, Virginia 2007, s. 17–35; T. McCulloh, R. Johnson, *Hybrid*

- zespół różnorodnych działań prowadzonych przeciwko nieprzyjacielowi według określonego algorytmu czyli skończonego ciągu precyzyjnie zdefiniowanych czynności, koniecznych do wykonania określonych zadań. Cechą charakterystyczną wojny hybrydowej jest przewaga środków niemilitarnych nad walką zbrojną. Z tego powodu nie jest możliwe uznanie wojny hybrydowej za wojnę w klasycznym rozumieniu tego słowa, dlatego też postuluje się określanie działań dla niej charakterystycznych terminem agresja hybrydowa, który znacznie dokładniej definiuje specyfikę tego typu konfliktu. Głównymi desygnatami agresji hybrydowej są działania o charakterze informacyjno-propagandowym, wywiadowczo-dywersyjnym, polityczno-dyplomatycznym oraz ekonomicznym z elementami lobbingu i korupcji. Ponadto w ramach tego rodzaju konfliktu przewiduje się możliwość prowadzenia działań zbrojnych przy pomocy regularnej armii, sił partyzanckich oraz ograniczonego zastosowania taktycznej broni jądrowej[7].

Należy uznać, że główną cechą charakterystyczną wojny hybrydowej jest dążenie do maksymalnej zbieżności i synchronizacji metod, środków oraz sposobów prowadzenia operacji militarnych i pozamilitarnych w celu zwiększenia efektu synergii. Pozwala on bowiem na osiągnięcie względnie trwałej przewagi nad przeciwnikiem. Rezultatem tej praktyki jest niwelowanie różnic istniejących między różnorodnymi środkami i sposobami prowadzenia walki na rzecz ukształtowania uniwersalnego paradygmatu czyli wzorca „organizacji różnorodności"[8]. To podejście metodologiczne charakteryzuje zachodnie koncepcje wojny hybrydowej, co odzwierciedlają opinie cywilnych i wojskowych ekspertów. Według Franka G. Hoffmana wojna hybrydowa (…) *charakteryzuje się zbieżnością* (...) *fizyczną i psychologiczną, kinetyczną i niekinetyczną, wojskowych i cywilów* (…) *sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone*[9]. Na czynnik zbieżności parametrów konfliktu zwraca również uwagę płk Daniel T. Lasica. Według niego „hybrydowość" to logiczna kombinacja strategii i taktyki zmierzająca do wymieszania różnych typów działań zbrojnych[10]. Z kolei Robert G. Walker traktuje wojnę hybrydową jako wynik konwergencji zasad wojny konwencjonalnej i operacji specjalnych, płk John J. McCuen zaś definiuje ją jako kombinację wojny symetrycznej i asymetrycznej[11]. Tak więc wojna hybrydowa w ujęciu zachodnich badaczy stanowi próbę sformułowania nowego paradygmatu badawczego przyczyn, przebiegu i skutków konfliktów rozpatrywanych w kontekście współczesnych problemów bezpieczeństwa, asymetrii działań militarnych, przewlekłości konfliktów regionalnych, podziałów kulturowych i negatywnych skutków globalizacji[12].

Warfare…, s. 35–41.

[7] E. Магда, *Гибридная война: выжить и победить*, Харьков 2015, s. 29–30.

[8] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, s. 12–13. Szerzej na ten temat zob. A. Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, New York 2009, s. 163–215.

[9] F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly" 2009, nr 52, s. 34.

[10] D.T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth 2009, s. 11.

[11] R.G. Walker, *SPEC FI: The United States Marine Corps and Special Operations*, Monterrey 1998, s. 4–5; J.J. McCuen, *Hybrid Wars*, „Military Review" 2008, nr 2, s. 108. Por. A. Gruszczak, *Hybrydowość*…, s. 13–14.

[12] Tamże, s. 25. Por. A. Bousquet, *Chaoplexic Warfare or the Future of Military Organization*, „International Affairs" 2008, nr 84, s. 915–929. Por. P.R. Mansoor, *Introduction: Hybrid Warfare in History*, w: *Hybrid*

Zachodni politycy, wojskowi i dziennikarze są przekonani, że tego rodzaju wykładnia ma swoje odzwierciedlenie w poglądach rosyjskich strategów. W ośrodkach decyzyjnych, mediach i społeczeństwach krajów członkowskich NATO i Unii Europejskiej panuje opinia, że w Federacji Rosyjskiej funkcjonuje obecnie „nowy model nowoczesnej wojny", który nazywa się „rosyjską wojną hybrydową" (ang. '*Russian hybrid warfare*'). Genezy tego „nowego" sposobu prowadzenia wojny stosowanego przez Rosję niektórzy zachodni eksperci upatrują rzekomo w *strategii działań pośrednich*, którą opisał brytyjski wojskowy Basil Liddell Hart, *strategii totalnej* Ericha Ludendorffa oraz w koncepcji zastosowania nieograniczonych środków walki propagowanych przez chińskich wojskowych Qiao Lianga i Wanga Xiangsui. „Rosyjska wojna hybrydowa" polega zatem na wykorzystaniu całej gamy środków politycznych, dyplomatycznych, militarnych, informacyjnych, gospodarczych i kulturowych, które odpowiednio dobiera się i łączy w taki sposób, aby ich zsynchronizowane wykorzystanie przyniosło zamierzone efekty. Jak podkreślono, w tym „nowym rosyjskim modelu" wojna nie ma początku ani końca, następuje zatarcie podziału na żołnierzy i cywilów. Działań militarnych nie poprzedza polityczna deklaracja wszczęcia wojny, są one prowadzone z zaskoczenia, a inicjują je niewielkie pododdziały wojsk regularnych i nieregularne oddziały zbrojne, w czasie pokoju (grupy partyzanckie, wojska specjalne, „zielone ludziki" itp.). Głównym polem walki tej nowoczesnej wojny prowadzonej przez Rosję na Ukrainie nie jest już dłużej przestrzeń fizyczna, lecz przede wszystkim nieograniczona sfera oddziaływania psychologicznego. Działania te nie zmierzają do fizycznego unicestwienia nieprzyjaciela i zajęcia jego terytorium, ale ich celem jest złamanie woli walki przeciwnika i ograniczenie jego możliwości oporu[13].

Percepcja zachodnich koncepcji wojny hybrydowej w Federacji Rosyjskiej

Analizując kontekst zastosowania zachodniej terminologii w Federacji Rosyjskiej, należy pamiętać, że Rosjanie, adaptując obcy aparat pojęciowy, kierują się własnymi założeniami i logiką, przystosowując go do swoich potrzeb, tradycji i kultury[14]. Opinia ta dotyczy również zachodniej koncepcji wojny hybrydowej. Do momentu wybuchu konfliktu rosyjsko-ukraińskiego termin „wojna hybrydowa" (ros. '*гибридная война*') pojawiał się w rosyjskiej literaturze sporadycznie, przeważnie w kontekście działań zbrojnych prowadzonych przez USA w Iraku i Afganistanie. „Wojna hybrydowa"

Warfare. Fighting Complex Opponents from the Ancient World to the Present, W. Murray, P.R. Mansoor (red.), Cambridge 2012, s. 1–18. Paradygmat – termin ten został wprowadzony do nauki przez Thomasa Kuhna. Oznacza określony wzorzec uporządkowanych desygnatów, model oraz zbiór metod lub matrycę badania określonych problemów. Paradygmat stanowi także pogląd na świat, teorię lub grupę teorii mających wspólną wizję świata lub wspólny przedmiot badań. Zob. J. Czaputowicz, *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa 2007, s. 40.

[13] Oprac. na podst. M. Fryc, *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, „Bezpieczeństwo Narodowe" 2015, nr 33, s. 62–66; H. Reisinger, A. Golz, *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, „NATO Research Paper" 2014, nr 105, s. 3–11; O. Jonsson, R. Seely, *Russian Full-Spectrum Conflict: An Appraisal After Ukraine*, „The Journal of Slavic Military Studies" 2015, nr 28, s. 1–22; M. Wrzosek, *Konflikt rosyjsko-ukraiński a zmiany w teorii prowadzenia działań militarnych*, „Kwartalnik Bellona" 2014, nr 4, s. 11–23; B. Perry, *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, „Small Wars Journal" 2015, nr 1 [online], http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-operations [dostęp: 1 IX 2015].

[14] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, s. 15.

stanowiła wówczas synonim określenia „partyzanckie metody prowadzenia działań wojennych" (ros. '*партизанские методы ведения боевых действий*'), które odnosiło się zarówno do oddziałów partyzanckich typu wojskowego, jak i powstańczego[15].

W miarę rozwoju wydarzeń na południowym wschodzie państwa ukraińskiego zachodnia koncepcja wojny hybrydowej stała się w FR narzędziem kremlowskiej, antyzachodniej propagandy. W tym kontekście szczególnie interesująca jest rozprawa autorstwa Rusłana Puchowa – dyrektora Centrum Analiz Strategii i Technologii w Moskwie, opublikowana na łamach czasopisma „Niezawisimoje wojennoje obozrienije" z 29 maja 2015 r. Główna teza R. Puchowa sprowadza się do stwierdzenia, że strona rosyjska zarówno na Krymie, jak i we wschodnich obwodach Ukrainy nie stosowała żadnych nowych sposobów walki i rozwiązań taktycznych, które Zachód określa jako wojnę hybrydową. Tymczasem według NATO Rosja, wykorzystując tę „nową taktykę", stała się znacznie groźniejsza dla Zachodu niż ZSRR. Jako dowód panującego na Zachodzie przekonania R. Puchow przywołuje wypowiedź Sekretarza Generalnego NATO Andersa Rasmussena oraz zachodnie definicje wojny hybrydowej. Dziwi się opiniom wyrażanym na Zachodzie, zgodnie z którymi w okresie od lutego do kwietnia 2014 r. siły rosyjskie miałyby w jakiś nowatorski sposób wykorzystać piechotę morską, wojska powietrznodesantowe i siły specjalne, łącząc ich działania z operacjami informatycznymi i radioelektronicznymi oraz z wykorzystaniem cyberprzestrzeni i mediów do prowadzenia szerokiej kampanii informacyjnej, skierowanej do odbiorców wewnętrznych i zewnętrznych. Rosyjski analityk jest zaskoczony poglądami, według których na wschodniej Ukrainie Rosjanie mieliby inspirować działania grup nacisku złożonych z miejscowej ludności, a także tworzyć tego typu grupy i kierować nimi. R. Puchow stwierdza, że definicje wojny hybrydowej są całkowicie oderwanymi od rzeczywistości fantazjami. Odpiera m.in. zarzut, że strona rosyjska prowadziła operacje w cyberprzestrzeni, co jego zdaniem w przypadku armii ukraińskiej nie było konieczne ze względu na jej niewielki stopień zinformatyzowania i archaiczny sprzęt, którym dysponowała na Krymie. Analityk stara się również udowodnić, że działania propagandowe wobec ludności Półwyspu Krymskiego były bardzo ograniczone, ponieważ prawdziwego zamiaru i gotowości do przeprowadzenia ataku w danym miejscu nie głosi się publicznie. Zdaniem R. Puchowa, mając na uwadze zaskoczenie społeczności międzynarodowej po sprawnym zajęciu Krymu, zamysł ten został zrealizowany. Ponadto aneksja półwyspu spotkała się z entuzjastycznym przyjęciem w Federacji Rosyjskiej, gdzie wszyscy i tak uważali Krym za „rosyjską ziemię". W związku z tym wszelkie działania propagandowe byłyby po prostu bezcelowe. Zdaniem R. Puchowa, zachodni analitycy, którzy starają się udowodnić, że sukces Rosji był wynikiem wojny hybrydowej, ignorują unikatowy charakter krymskiej operacji oraz starają się ukryć swoją „błędną" ocenę tych wydarzeń. Według niego, wyjątkowość aneksji Krymu przejawiała się w tym, że Moskwa wykorzystała przede wszystkim bezwzględne poparcie miejscowej ludności, która umożliwiła paraliż ukraińskich jednostek wojskowych stacjonujących na Krymie. Jak przekonuje rosyjski analityk, trudno sobie wyobrazić pojawienie się „zielonych ludzików" w innym państwie, np. w Polsce lub w Stanach Zjednoczonych. W tym przypadku nie byłoby żadnego logicznego wytłumaczenia takiej akcji i żadnych szans na jej powodzenie. Dodatkowym czynnikiem sprzyjającym Kremlowi był fakt, że na półwyspie znajdowały się rosyjskie bazy wojskowe,

[15] О.В. Валецкий, В.М. Неелов, *Особенности партизанских и противопартизанских действий в ходе Иракской войны (2003–2011)*, Москва 2015, s. 25–26.

co stwarzało możliwość skrytego wzmacniania rosyjskiej obecności militarnej na Krymie przez dostarczanie oddziałów wojskowych i sprzętu, czego nie był w stanie dostrzec wywiad NATO. Puchow podkreśla, że wykorzystanie regularnych sił zbrojnych bez oznaczeń przynależności państwowej w działaniach specjalnych ma długą historię i nie można tego uznawać za nowatorskie, a tym bardziej rosyjskie, rozwiązanie. Co więcej, podczas każdej wojny domowej, a taka w opinii rosyjskiego analityka trwa przecież na Ukrainie, dochodzi do sytuacji, w której jedna ze stron wspiera siły sojuszniczego ruchu powstańczego lub partyzanckiego biorące udział w konflikcie. Zdaniem R. Puchowa wojny hybrydowe, postrzegane jako nowy sposób prowadzenia współczesnych konfliktów, toczyły się wielokrotnie na przestrzeni wieków. Autor konkluduje, że trudno sobie wyobrazić użycie sił zbrojnych bez jednoczesnego zabezpieczenia wywiadowczego i informacyjnego, bez sankcji ekonomicznych, bez dywersji prowadzonej tajnymi i jawnymi kanałami oraz próby osłabienia przeciwnika przez wykorzystanie antagonizmów etnicznych, społecznych, ekonomicznych i politycznych istniejących w jego państwie[16]. Warto odnotować, że ta opinia w dużej mierze jest podzielana przez znaczną część korpusu oficerskiego sił zbrojnych FR[17].

Rozważania R. Puchowa stanowią doskonały przykład zyskującej w Rosji na popularności tzw. analityki informacyjnej, której celem jest diagnozowanie i wartościowanie rzeczywistości z perspektywy interesów Federacji Rosyjskiej[18]. Wiarygodna teza, która zakłada, że opierając się na wydarzeniach historycznych można podważyć koncepcje wojny hybrydowej jako novum w dziedzinie wojskowości, a wojna na Ukrainie stanowi przykład zastosowania konkretnych sposobów działania od dawna już wykorzystywanych w konfliktach i wojnach, została przez R. Puchowa wykorzystana jako narzędzie dezinformacji dysymulacyjnej. Dzięki temu stara się on udowodnić, że termin „wojna hybrydowa" jest stosowany na Zachodzie tylko po to, aby wyolbrzymić rolę czynnika zewnętrznego, tj. Rosji, co w oczach opinii międzynarodowej przedstawia ją jako agresora, a jednocześnie zniwelować znaczenie czynników wewnętrznych (np. zagrożenie ludności rosyjskiej ze strony nacjonalistów ukraińskich). To natomiast automatycznie sytuuje Rosję w roli „obrońcy" praw własnych obywateli, a nie inicjatora konfliktu. W ten sposób kremlowska propaganda tłumaczy własnemu społeczeństwu i opinii

[16] Oprac. na podst. Р. Пухов, *Миф о «гибридной войне». Никаких принципиально новых действий наша армия в Крыму и на Украине не вела*, „Независимое военное обозрение" 2015, nr 19 (855), s. 1. Por. П. Топычканов, *«Гибридная война» – научный термин или пропагандистский штамп?* [online], http://russiancouncil.ru/inner/?id_4=6340#top-content [dostęp: 1 IX 2015].

[17] Б.В. Андрианов, В.В. Лойко, *Вопросы применения ВС РФ в кризисных ситуациях мирного времени*, „Военная мысль" 2015, nr 1, s. 68.

[18] Propaguje ją m.in. „Rosyjska Szkoła Analityki" (zob. www.analitika-kurnosov.ru), której pomysłodawcą i twórcą jest emerytowany płk FSB Jurij Kurnosow. Założenia projektu zaprezentował m.in. w wydanej w 2012 r. książce pt. *Analityka jako broń intelektualna*. Jest on oparty na metodologii, która umożliwi (...) *połączenie wysiłku analitycznego i skuteczne przeciwdziałanie obcej ekspansji cywilizacyjnej*. Celem autora jest stworzenie nowej, współczesnej rosyjskiej szkoły analitycznej, która ułatwi wychowanie (…) *zdrowo myślących obywateli, zdolnych do przeciwstawienia się ekspansji obcych struktur i kultur, działających zgodnie z formułą „dziel i rządź", podstawową formułą wojny informacyjnej prowadzącej do informacyjnego spustoszenia świadomości, tj. mentalnego ludobójstwa Rosjan.* Należ podkreślić, że tego rodzaju instytucje będące rzekomym wytworem rosyjskiego „społeczeństwa obywatelskiego" są sterowane odgórnie, stanowiąc element sieci umożliwiającej multiplikacje kierowanego przez państwo przekazu. Oprac. na podst. J. Darczewska, *The Information War on Ukraine. New Challenges*, „Cicero Foundation Great Debate Papers" 2014, nr 14/08, s. 12–13. Por. Ю.В. Курносов, П.Ю Конотопов, *Аналитика: методология, технология и организация организационно-аналитической работы*, Москва 2004; Ю.В. Курносов, *Аналитика как интеллектуальное оружие*, Москва 2012.

międzynarodowej, dlaczego Zachód stosuje w swojej narracji pojęcie „nowatorskiej wojny hybrydowej", którą Rosja rzekomo prowadzi przeciwko państwu ukraińskiemu[19].

Zachodnie koncepcje wojny hybrydowej stały się przedmiotem wnikliwych badań prowadzonych przez zastosowanie paradygmatu geopolitycznego[20]. W ich świetle wojna hybrydowa uzyskuje niedostrzegalny na Zachodzie wymiar przestrzenny. W Rosji termin przestrzeń (ros. '*пространство*') bardzo często odnosi się do zjawisk, których wymiar przestrzenny nie jest oczywisty, a które w innych krajach (np. w Polsce) najczęściej są one postrzegane jako „system", „struktura" lub „logika społeczna". Oznacza to, że zjawiska, które są na ogół postrzegane jako strukturalne, w Rosji zyskują nieznany nigdzie indziej sens horyzontalny. W Rosji termin „przestrzeń" występuje w dwóch różnych znaczeniach: jako synonim ściśle przestrzennych komponentów Związku Radzieckiego, które po 1991 r. mogły odgrywać pewną rolę samodzielną (np. *оборонное пространство*), lub były ważnym polem polityki (np. *таможенное*, *экономическое*, *единое правовое пространство*), oraz w odniesieniu do hierarchicznej struktury władzy państwowej (np. *правовое*, *конституционное пространство*)[21].

Geopolityczną interpretację wojny hybrydowej zawierają opracowania autorstwa wojskowych, geopolityków i funkcjonariuszy rosyjskich służb specjalnych. Szczególnie interesujące w tym kontekście są rozważania dotyczące mechanizmów tzw. wojen limitroficznych (ros. '*лимитрофная война*', '*война в лимитрофе*'), których autorką jest prof. Natalia Komlewa, wykładowca w Katedrze Teorii i Historii Nauk Politycznych Uralskiego Federalnego Uniwersytetu im. Borysa Jelcyna w Jekaterynburgu. Warto podkreślić, że N. Komlewa jest członkiem prezydium Akademii Problemów Geopolitycznych, której działalnością kieruje gen. płk Leonid Iwaszow[22]. Termin l i m i t r o f w rosyjskiej geopolityce oznacza niestabilne obszary peryferyjne, które tworzą przestrzeń oddzielającą od siebie wielkie imperia lub cywilizacje. Pojęcie to wprowadził do rosyjskiego dyskursu naukowego Wadim Cymburskij (1957–2009), twórca metafory „Rosji Wyspy". Według W. Cymburskiego na obszarze Eurazji istnieje pięć wielkich geocywilizacji: romano-germańska, arabsko-irańska, rosyjska, chińska oraz indyjska. W wyniku rozpadu Związku Radzieckiego powstał pas suwerennych państw ciągnący się od krajów Europy Środkowo-Wschodniej, przez Naddniestrze, Zakaukazie, Azję Środkową oraz tereny zasiedlone przez ludy ałtajskie i turecko-mongolskie aż do granicy rosyjsko-chińskiej. Tę peryferyjną dla wszystkich cywilizacji strefę W. Cymburskij określił mianem „Wielkiego Limitrofu". Według

[19] Por. А. Умланд, *В защиту конспирологии: ответ Сергею Кудели на его антиполитический анализ «гибридной войны» в Восточной Украине*, „Форум новейшей восточно европейской истории и культуры" 2014, nr 2, s. 34–40; С. Куделя, *Ответ Андреасу Умланду: война в Донбассе началась изнутри*, „Форум новейшей восточно европейской истории и культуры" 2014, nr 2, s. 40–45; A. Shekhovtsov, *The Spectre of Ukrainian "Fascism": Information Wars, Political Manipulation*, *and Reality*, w: *What does Ukraine Think?* A. Wilson (red.), London 2015, s. 80–89.

[20] P a r a d y g m a t g e o p o l i t y c z n y – metoda albo wzorzec prostego i wewnętrznie spójnego rozpatrywania procesów, zdarzeń, tendencji, trendów w stosunkach międzynarodowych w optyce kategorii geograficznych i przestrzennych, dokonywany poprzez syntezę interdyscyplinarnej wiedzy. J. Macała, *Czym jest geopolityka? Spory wokół jej definicji*, w: *Geopolityka. Elementy teorii, wybrane metody i badania*, Z. Lach, J. Wendt (red.), Częstochowa 2010, s. 16.

[21] W. Marciniak, *Przestrzeń jako kategoria dyskursu politycznego w Rosji współczesnej*, Warszawa 2004, s. 20–21.

[22] *Кафедра политических наук Уральского федерального университета имени первого Президента России Б.Н. Ельцина, Комлева Наталья Александровна* [online], http://polit.ispn.urfu.ru/home/kafedra/staff/ [dostęp: 1 IX 2015].

geopolityka, zachodnia część tego obszaru może się stać narzędziem wykorzystywanym do izolowania i destabilizowania Rosji przez zachodnie ośrodki siły, dlatego też konieczne jest utrzymanie wpływów rosyjskich na osi Kaliningrad–Półwysep Krymski[23]. Cymburskij pisał, że:

> (…) oprócz bliskiej zagranicy, geopolityczne interesy Rosji w tym czy innym stopniu uwzględniają sytuację na całym Wielkim Limitrofie, który tworzy łańcuch regionów, stykających się ze sobą przestrzennie, dysponującymi zbieżnymi funkcjami w cywilizacyjnej i geoekonomicznej strukturze kontynentu i będącymi w stanie w swej konfiguracji występować jako pewien „półprzewodnik" konfliktogennych impulsów i antyrosyjskich projektów[24].

Koncepcję „limitrofu" rozwinęła N. Komlewa, łącząc ją z problematyką wojen hybrydowych. Według niej pojęcie l i m i t r o f odnosi się do grupy niewielkich państw odgrywających rolę bufora, których geopolityczna przestrzeń jest pod pośrednią kontrolą jakiegoś regionalnego lub światowego mocarstwa. W strefie buforowej (limitrofie), oprócz przestrzeni geograficznej (ląd, morze, powietrze i kosmos) istnieje także przestrzeń ekonomiczna, informacyjno-cybernetyczna oraz informacyjno-ideologiczna. W tego rodzaju sferach prowadzą aktywną działalność aktorzy niepaństwowi i wszelkie ponadnarodowe organizacje, korporacje, kościoły, związki religijne itd. Zdaniem autorki *technologia tworzenia limitrofów* pozwala zachować danemu mocarstwu (ośrodkowi siły) niezależność, ich posiadanie zaś zwiększa stopień jego bezpieczeństwa przez możliwość wzmocnienia własnego potencjału gospodarczego, politycznego, militarnego itp. Warto dodać, że to właśnie w tej „troficznej" funkcji limitrofu jest zawarte semantyczne znaczenie tego pojęcia (od łac. '*limes*' – granica i gr. '*τροφή*' – aprowizacja, środki utrzymania). Państwa buforowe mogą zostać wykorzystane przez regionalny ośrodek siły jako narzędzie do prowadzenia walki z geopolitycznym przeciwnikiem, która toczy się w całej geopolitycznej przestrzeni limitrofu. Ponadto chroni on nadrzędny ośrodek siły przed analogicznymi działaniami strony przeciwnej. Uzyskanie kontroli nad limitrofem pozwala także na rozciągnięcie wpływów nad daleko położonymi, bezpośrednio niedostępnymi terytoriami[25].

Jak zauważa N. Komlewa, niestabilne i peryferyjne obszary stają się często strefami działań wojennych i przewlekłych konfliktów regionalnych. W jej opinii są to tzw. wojny limitroficzne. Ich postać jest uzależniona od rodzaju przestrzeni geopolitycznej, w której się toczą: przestrzeń geograficzna jest areną wojny konwencjonalnej, w przestrzeni informacyjno-ideologicznej toczy się walka informacyjno-psychologiczna, w przestrzeni ekonomicznej są prowadzone działania mające na celu osłabienie poten-

[23] В.Л. Цымбурский, *Борьба за евразийскую Атлантиду: геоэкономика и геостратегия*, „Pro et Contra" 1999, nr 4, s. 3, 16–32. Por. L. Sykulski, *Rosja Wyspa i Wielki Limitrof. Myśl geopolityczna Wadima Cymburskiego*, w: *Problemy współczesnej Europy – ujęcie interdyscyplinarne*, R. Fedan, B. Petrecka, S. Dyrda-Maciałek (red.), Jarosław 2014, s. 355–363; J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, s. 231–232.

[24] Cyt. za: J. Czachor, *Współczesna geopolityka rosyjska. Koncepcja Wadima Cymburskiego*, „Wrocławski Przegląd Międzynarodowy" 2010, nr 1, s. 44.

[25] Н.А. Комлева, *Лимитроф в современном геополитическом процессе*, „Пространство и Время" 2013, nr 3, s. 1–7; Н.А. Комлева, *Лимитроф как геополитическая технология*, „Известия Уральского федерального университета. Серия 1. Проблемы образования, науки и культуры" 2010, nr 3, s. 37–45; Н.А. Комлева, *Несколько замечаний относительно природы и типологии геополитических пространств*, „Пространство и Время" 2014, nr 1, s. 90–101.

cjału gospodarczego przeciwnika, a z kolei w przestrzeni informacyjno-cybernetycznej dochodzi do cyberataków i innych działań o charakterze informacyjno-technicznym. Według autorki wojna hybrydowa jest takim rodzajem konfliktu, który toczy się we wszystkich tych przestrzeniach równocześnie, obejmując z czasem swoim zasięgiem znacznie szerszy zakres – sferę geocywilizacji przeciwnika. Mamy więc tutaj do czynienia z koncepcją wojny hybrydowej ukazanej jako zjawisko przestrzenne. W tym kontekście autorka interpretuje przebieg kryzysu ukraińskiego, stanowiącego jej zdaniem „wojnę limitroficzną", czyli wojnę hybrydową, której celem jest osłabienie „geocywilizacji rosyjskej"[26].

Koncepcję wojny hybrydowej w Federacji Rosyjskiej interpretuje się także pod kątem fenomenologicznym (jako zjawisko) i technologicznym (jako technologię służącą do wywierania politycznego wpływu), co znajduje odzwierciedlenie w pracach Andrieja Manojły, byłego funkcjonariusza FSB, członka Komitetu Naukowego przy Radzie Bezpieczeństwa FR, który obecnie pełni funkcję profesora politologii na Państwowym Uniwersytecie Moskiewskim[27]. Podobne podejście metodologiczne prezentuje również Aleksandr Bartosz, docent doktor, członek korespondent Akademii Nauk Wojskowych Sztabu Generalnego Sił Zbrojnych FR w Moskwie oraz dyrektor Informacyjnego Centrum ds. Problemów Bezpieczeństwa Międzynarodowego przy Moskiewskim Państwowym Uniwersytecie Lingwistycznym. Według tych autorów „technologia wojen hybrydowych" jest przede wszystkim wytworem wojskowości Stanów Zjednoczonych, które przy jej pomocy realizują własne cele polityczne. USA, dążąc do światowej hegemonii, próbuje wykorzystać globalną niestabilność i osłabić pozycję swoich strategicznych oponentów, którymi są przede wszystkim Rosja i Chiny, a w mniejszym stopniu również Unia Europejska. Polityka ta jest realizowana za pomocą specjalnch środków w postaci technologii „kolorowych rewolucji", „kontrolowanego chaosu" (czyli stopniowego, niejawnego uzyskiwania możliwości sterowania procesami politycznymi, gospodarczymi i kulturalnymi w danym państwie) oraz wojen hybrydowych. Takie działanie przyczynia się do powstania globalnego środka ciężkości i podważa fundamenty porządku światowego[28].

W ujęciu autorów, stworzona w USA koncepcja wojny hybrydowej zakłada kombinacyjne, sekwencyjne zastosowanie różnych strategii współczesnych wojen (konwencjonalnej, informacyjnej, ekonomicznej i psychologicznej) w celu porażenia sił i środków nieprzyjaciela, osiągnięcia geopolitycznej przewagi nad nim i zmuszenia

[26] Н.А. Комлева, *Войны в лимитрофах: эволюция технологий*, „Пространство и Время" 2015, nr 12, s. 32–42. Por. Н.А. Комлева, *Войны сверхдержав: от «горячих» к гибридным*, „Вестник Московского государственного областного университета" 2015, nr 1, s. 1–26. Por. И.Н. Воробьев, В.А. Киселев, *Стратегические категории время и пространство в современных войнах*, „Военная мысль" 2008, nr 8, s. 62–70.

[27] А.В. Манойло, *Биография* [online], http://andreymanoylo.vov.ru/biografia.html [dostęp: 1 IX 2015].

[28] А.В. Манойло, *Гибридные войны и цветные революции в мировой политике*, „Право и политика" 2015, nr 7, s. 918–920; А. Бартош, *Гибридные войны как проявление глобальной критичности современного мира*, „Геополитика и безопасность" 2015, nr 1, s. 71–73. Por. В.В. Карякин, *Стратегии непрямых действий, «мягкой силы» и технологии «управляемого хаоса» как инструменты переформатирования политических пространств*, „Информационные войны" 2014, nr 3, s. 29–30. Por. В.Е. Лепский, *Рефлексивный анализ технологий управляемого хаоса как оружия разрушения субъектности развития*, „Рефлексивные процессы и управление. Международный научно-практический междисциплинарный журнал" 2010, nr 10, s. 5–23; А. Бартош, *Модель управляемого хаоса в сфере военной безопасности*, „Вестник Академии военных наук" 2014, nr 1, s. 69–78. Por. Г. Почепцов, *Революция.com. Основы протестной инженери и Европа*, Москва 2005, s. 69–74.

go do zawarcia pokoju na warunkach korzystnych dla agresora. W sformułowanej przez A. Manojłę i A. Bartosza definicji jest również zauważalne podejście geopolityczne, ponieważ rodzaje wymienionych przez nich wojen odpowiadają formom geopolitycznej przestrzeni (tj. przestrzeni geograficznej, informacyjno-cybernetycznej, informacyjno-ideologicznej i ekonomicznej). Szczególne zainteresowanie eksperci przejawiają jednak technologiami, których zastosowanie umożliwia stworzenie sprzyjających warunków do prowadzenia i eskalacji wojny hybrydowej. Jedną z takich technologii jest w opinii A. Manojły i A. Bartosza tzw. kolorowa rewolucja, która stanowi preludium wojny hybrydowej. Według autorów kolorowa rewolucja to organizowanie politycznych przewrotów w warunkach sztucznie inicjowanej destabilizacji państwa (tzw. teoria kontrolowanego chaosu), które polegają na wywieraniu nacisku na władzę przy pomocy politycznego szantażu. Działanie to odbywa się za pośrednictwem inspirowanych z zewnątrz ruchów i organizacji młodzieżowych o silnym potencjale protestu i przebiega z wykorzystaniem m.in. portali społecznościowych i mediów elektronicznych. Celem „kolorowych rewolucji" jest obalenie władzy danego państwa przez jego własnych obywateli i umożliwienie przejęcia możliwości sterowania nim przez obcy ośrodek siły, który zainicjował przewrót. Jako przykład praktycznego zastosowania technologii „kolorowych rewolucji" autorzy podają wydarzenia rozgrywające się podczas tzw. arabskiej wiosny w Tunezji, Libii i Egipcie oraz w Gruzji i na Ukrainie w latach 2006 i 2013. Technologie „kolorowych rewolucji" tworzą więc warunki sprzyjające transformacji konfliktu w fazę militarną. Zdaniem autorów, taki scenariusz został zrealizowany na Ukrainie: kolorowa rewolucja (incydent→protest→Majdan) przeistoczyła się w zbrojny bunt, którego eskalacja spowodowała wojnę domową, a ta z kolei przybrała postać wojny hybrydowej[29].

Według A. Bartosza szczególną rolę w tzw. predeterminowaniu, czyli kreowaniu sprzyjającej sytuacji umożliwiającej przejście do stanu wojny hybrydowej, odgrywa wywiad. Ma on mieć charakter hybrydowy, czyli powinien być prowadzony kompleksowo z wykorzystaniem różnorodnych sił i środków. Głównym celem wywiadu jest przede wszystkim penetrowanie struktur państwowych nieprzyjaciela, lokalizowanie i wykorzystywanie jego słabości. Najważniejszym zadaniem wywiadu jest natomiast zdobywanie informacji dotyczących ukrytych, niejawnych grup oraz organizacji terrorystycznych, paramilitarnych i ekstremistycznych o charakterze religijnym lub politycznym, a także innych elementów funkcjonujących w sieci w postaci odizolowanych komórek. W tym kontekście chodzi nie tylko o rozpoznanie wrogiej struktury, lecz także o stworzenie jej własnego odpowiednika w państwie nieprzyjaciela. Struktura ta powinna składać się ze specjalnych grup wywiadowczo-uderzeniowych, które funkcjonują, opierając się na strategii oporu niekierowanego. Równie istotna jest także praca analityczna. Aby prowadzić różnorodne, asymetryczne działania mające spowodować jak największy uszczerbek w zasobach przeciwnika, należy skorzystać z możliwości interdyscyplinarnego wywiadu. Jego celem jest wykorzystanie informacji, które na pierwszy rzut oka nie mają wojskowego lub politycznego znaczenia, w dalszej perspektywie jednak mogą być przydatne

[29] А.В. Манойло, *Гибридные войны*…, s. 920–928; А. Бартош, *Гибридные войны как проявление*…, s. 73–76. Por. А.В. Манойло, *Роль стратегий «управляемого хаоса» в политическом кризисе в Украине*, „Международная жизнь" 2014, nr 7, s. 118–135; tenże, *Armed Rebellion in Ukraine could be the Last Wake-up call to Russia*, „Sententia. European Journal of Humanities and Social Sciences" 2014, nr 1, s. 51–56; tenże, *Украинский кризис и «управляемый хаос»: след «цветных революций» Арабской Весны*, „Власть" 2014, nr 4, s. 24–28.

w przygotowaniu i prowadzeniu operacji o charakterze hybrydowym. Dlatego też w strukturach wywiadu powinni znaleźć się eksperci z różnych dziedzin wiedzy, szczególnie wojskowi, ekonomiści, kulturoznawcy, psychologowie, etnolodzy i lingwiści oraz specjaliści badający cechy psychologiczne ludności danego kraju lub regionu[30].

Geopolityczna interpretacja wojny hybrydowej jako strategii synergetycznego, kompleksowego oddziaływania we wszystkich przestrzeniach danego państwa znalazła również uznanie wśród rosyjskich wojskowych. Według nich zagrożenia hybrydowe stanowią największe niebezpieczeństwo dla państwa, ich kompleksowy charakter zaś uniemożliwia neutralizację środkami i działaniami tylko jednego segmentu władzy państwowej (np. resortu obrony). Wymaga to podjęcia skoordynowanych działań wielu organów i instytucji władzy państwowej, które należy prowadzić we wszystkich sferach bezpieczeństwa narodowego[31]. Interpretacja zachodnich wojen hybrydowych jako zagrożenia ze strony NATO i USA dla państwa rosyjskiego znalazła się także w nowej *Doktrynie Wojennej FR* zatwierdzonej przez Radę Bezpieczeństwa FR 20 grudnia 2014 r. Jest ona szczególnie widoczna w punkcie 12, dotyczącym zagrożeń zewnętrznych, który w porównaniu z tekstem poprzedniej doktryny z 2010 r. został uzupełniony o cztery nowe podpunkty stanowiące nawiązanie do działań przewidzianych w zachodnich koncepcjach wojny hybrydowej:

1) istnienie (powstawanie) ognisk napięć etnicznych i międzywyznaniowych, działalność międzynarodowych radykalnych ugrupowań zbrojnych, zagranicznych prywatnych kompanii najemnych w rejonach przylegających do granicy państwowej FR i granic jej sojuszników, a także istnienie sprzeczności terytorialnych, wzrost separatyzmu i ekstremizmu w poszczególnych rejonach świata,
2) wykorzystanie technologii informacyjnych i komunikacyjnych do celów polityczno-wojskowych, do realizacji działań sprzecznych z prawem międzynarodowym, wymierzonych przeciwko suwerenności, niezawisłości politycznej oraz integralności terytorialnej państw i stanowiących zagrożenie dla pokoju międzynarodowego, bezpieczeństwa, globalnej i regionalnej stabilności,
3) instalowanie, w tym w rezultacie obalenia legalnych organów władzy państwowej, w państwach graniczących z FR reżimów, których polityka zagraża interesom Rosji,
4) działalność dywersyjna służb specjalnych oraz organizacji obcych państw i ich koalicji przeciwko FR[32].

Należy zaznaczyć, że oficjalne akty normatywne FR, w tym doktryny polityki zagranicznej, bezpieczeństwa informacyjnego lub doktryny wojenne, nie powinny stanowić podstawowego źródła szczegółowych analiz zamierzeń politycznych pań-

[30] А. Бартош, *Гибридные войны как проявление глобальной критичности современного мира* [online], http://isc.mslu.ru/index.php?option=com_content&task=view&id=366&Itemid=36 [dostęp: 1 IX 2015]. Por. А.А. Зиновьев, *Эволюционный перелом XX века и новые функции учреждений разведки*, „Информационные войны" 2013, nr 2, s. 71–74. Odnośnie do strategii oporu niekierowanego zob. J. Tomasiewicz, *Strategia oporu niekierowanego w wojnie asymetrycznej*, „Przegląd Geopolityczny" 2009, nr 1, s. 161–191.

[31] Б.В. Андрианов, В.В. Лойко, *Вопросы применения ВС РФ*…, s. 67; В.А. Киселев, И.Н. Воробьев, *Гибридные операции как новый вид военного противоборства*, „Военная мысль" 2015, nr 5, s. 41–48.

[32] Cyt. za: *Военная доктрина Российской Федерации (утверждена Президентом РФ 25.12.2014., No Пр-2976)*, „Геополитика и безопасность" 2015, nr 1, s. 137. Por. В.К. Белозёров, *Геополитические смыслы Военной доктрины Российской Федерации*, „Геополитика и безопасность" 2015, nr 1, s. 9–15; J. Darczewska, *Diabeł tkwi w szczegółach*…, s. 17–18.

stwa rosyjskiego, lecz dawać ogólny obraz relacji Kremla ze światem zewnętrznym. Doświadczenie historyczne pokazuje, że tego rodzaju dokumenty są wykorzystywane jako narzędzie w kampaniach propagandowych i walce informacyjnej. Dotyczy to również wspomnianej doktryny wojennej, uwiarygadniającej tezę, według której wojny hybrydowe są postrzegane w Rosji jako fundamentalne zagrożenia jej bezpieczeństwa, samo ich pojęcie zaś służy do tłumaczenia agresywnych zamiarów NATO.

***

Wydarzenia na Ukrainie, w regionie Bliskiego i Środkowego Wschodu oraz w Afryce Północnej (ekspansja Państwa Islamskiego) wywołały ogólnoświatową debatę dotyczącą współczesnej sztuki wojennej, w której zaczyna dominować pogląd, jakoby doszło do fundamentalnych zmian w dziedzinie strategii i taktyki prowadzenia wojen. Pokłosiem tej dyskusji jest m.in. pojawienie się nowych pojęć i koncepcji, czego przykładem jest wszechobecna tendencja do określania współczesnych wojen i konfliktów „wojnami hybrydowymi". Podejmując się próby oceny tego zjawiska z perspektywy historycznej, należy podkreślić, że takie działania, jak presja polityczna, demonstracja siły militarnej w celu zastraszenia wroga, blokada ekonomiczna, oddziaływanie psychologiczne, dywersja i sabotaż były znane i stosowane od stuleci. Bezspornym pozostaje fakt, że w warunkach intensywnego postępu naukowo-technicznego oraz rozwoju środków masowego przekazu konieczne były modyfikacje dotyczące zarówno środków, jak i metod prowadzenia działań wojennych (m.in. stworzona w latach 90. XX w. koncepcja walki metodą sieciocentryczną, obecnie realizowana i wdrażana w czołowych armiach świata[33]), ale ogólne założenia pozostały niezmienne. Aby udowodnić tę tezę, warto posłużyć się choćby dwoma zaczerpniętymi z historii przykładami:

1. Konwergencja działań, które mają rzekomo stanowić o nowatorskim charakterze wojen hybrydowych mieści się w ramach tzw. wojen specjalnych (ang. '*special warfare*'). Ich założenia opracowano w Stanach Zjednoczonych w okresie prezydentury Johna F. Kennedy'ego (trwała od 20 stycznia 1960 r. do 22 listopada 1963 r.). Sformułowano wtedy pogląd, że zastosowanie odpowiednich form działań o charakterze politycznym i ekonomicznym połączonych z ograniczonymi działaniami militarnymi może przynieść zamierzone efekty bez ryzyka wywołania globalnego konfliktu. Podejście to stanowiło alternatywę dla powszechnie wówczas akceptowanej w ZSRR i USA strategii odstraszania opartej na masowym wykorzystaniu broni jądrowej. Aby skutecznie prowadzić takie operacje, konieczne było dokonanie odpowiednich reform w strukturze armii USA, co zaowocowało powstaniem tzw. Grup Sił Specjalnych (Special Forces Groups) formowanych pod kątem działania na ściśle określonym teatrze działań wojennych, z uwzględnieniem jego kulturowej, gospodarczej, językowej i religijnej

[33] Zob. na przykład: A.K. Cebrowski, J.J. Garstka, *Network-Centric Warfare: Its Origin and Future*, „US Naval Institute Proceedings Magazine" 1998, nr 124, z. 1, s. 28–35; D.S. Alberts, J.J. Garstka, F.P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, Washington 2002.

specyfiki. Ośrodek „wojny specjalnej" mieści się do dzisiaj w kombinacie Fort Bragg, który nosi imię prezydenta J.F. Kennedy'ego i jest największym tego rodzaju ośrodkiem na świecie[34].

2. Synergia działań przypisywana jedynie współczesnym wojnom hybrydowym była charakterystyczna również dla polityki III Rzeszy, co miało miejsce w sferze zarówno militarnej, jak i propagandowo-psychologicznej. Oddziaływano m.in. na mniejszość niemiecką znajdującą się w innych krajach przez umacnianie wśród niej postaw patriotycznych i propagowanie ideologii nazistowskiej. Wspierano zagraniczne partie i organizacje o charakterze nacjonalistycznym i nazistowskim, wykorzystywano antagonizmy narodowościowe, religijne i kulturowe w celu zdestabilizowania poszczególnych krajów. W ten sposób tworzono tzw. V Kolumnę, która wspierała działania regularnych formacji niemieckich w początkowej fazie wojny. Zastosowanie presji politycznej, szantażu militarnego oraz wykorzystanie zdecydowanej postawy mniejszości niemieckiej doprowadziły m.in. do bezkrwawego zajęcia Czechosłowacji, co odbyło się przy biernej postawie zachodnich mocarstw. Równie symptomatycznym przykładem tego rodzaju działań były przygotowania do inwazji na Francję, która nastąpiła 10 maja 1940 r. Niemcy, mając szczegółowe informacje dotyczące nastrojów żołnierzy i społeczeństwa francuskiego, wywołanych świadomością ogromnych start poniesionych w I wojnie światowej, doskonale je wykorzystali. Zainicjowali i rozwinęli bezprecedensową, prowadzoną na szeroką skalę kampanię pacyfistyczną w prasie, radiu i telewizji (słynne *Pourquoi mourir pour Dantzig?*), którą ułatwiał brak cenzury we Francji. Ponadto, jak podkreśla Walter von Schellenberg, przeprowadzono wiele akcji dywersyjno-sabotażowych, sztucznie wywołując migrację ludności cywilnej, która blokowała przemarsze francuskiego wojska. Bardzo skuteczny okazał się masowy kolportaż broszury zawierającej rzekome proroctwo Nostradamusa, według którego bezpieczne będą tylko tereny południowo-wschodniej Francji[35].

W świetle powyższych, pobieżnie przywołanych przykładów, koncepcję wojny hybrydowej trudno uznać za nową formę prowadzenia wojen. Pojęcie to staje się raczej narzędziem walki informacyjnej toczącej się między Zachodem a Rosją. Przez jego użycie wyjaśnia się własnym społeczeństwom działania geopolitycznego oponenta, potęgując atmosferę strachu przed rzekomo nową formą działań wojennych, którą dysponuje przeciwnik. Co więcej, koncepcja wojny hybrydowej pełni także funkcję

[34] E.G. Piasecki, *The History of Special Warfare*, „Special Warfare. The Professional Bulletin of the John F. Kennedy Special Warfare Center and Schools" 2015, nr 28, s. 8–13. Odnośnie do genezy „wojen specjalnych" zob. A.H. Paddock, *US Army Special Warfare. Its Origins. Psychological and Unconventional Warfare, 1941–1952*, Washington 1982, s. 39 i nast.; tenże, *Psychological Operations, Special Operations, and US Strategy*, w: *Special Operations in US Strategy*, F.R. Barnett, B.H. Tovar, R.H. Shultz (red.), Washington 1984, s. 229–252; J. Stec, *Wojny specjalne*, cz. 1: *Refleksje historyczne* [online], http://geopolityka.net/jan-stec-wojny-specjalne-cz-1-refleksje-historyczne/ [dostęp: 1 IX 2015].

[35] L. Farago, L.F. Gittler, *German Psychological Warfare. Survey and Bibliography*, New York 1941, s. 62–78; F.S. Hellman, *Nazi Fifth Column Activities: A List of References*, Washington 1943; *The Labyrinth: Memoirs of Walter Schellenberg, Hitler's Chief of Counterintelligence*, tłum. L. Hagen, Boston 2000, s. 105; N. Jordan, *Strategy and Scapegoatism: Reflections on the French National Catastrophe*, w: *The French Defeat of 1940: Reassessments*, J. Blatt (red.), London 1998, s. 13–39; J. Stec, *Wojny specjalne*...

nowego paradygmatu badania i rozpatrywania przyczyn, skutków i sposobów prowadzenia współczesnych konfliktów. Na Zachodzie paradygmat ten jest rozpatrywany jako konwergencja szerokiego spektrum zintegrowanych i zastosowanych środków wykorzystywanych do zdobycia przewagi nad przeciwnikiem.

W Rosji percepcja paradygmatu wojny hybrydowej jest inna niż na Zachodzie. W rosyjskim dyskursie naukowym i wojskowym wojna hybrydowa nie ma charakteru klasyfikacyjnego, odnoszącego się do stricte rosyjskich koncepcji i teorii konfliktów zbrojnych. Wojny hybrydowe są natomiast postrzegane jako wytwór cywilizacji zachodniej, który jest poważnym zagrożeniem dla wszystkich sfer bezpieczeństwa wewnętrznego Federacji Rosyjskiej. Niemniej jednak Rosjanie nadają paradygmatowi wojny hybrydowej własne, oryginalne znaczenie. Interpretacja koncepcji wojny hybrydowej w Rosji polega na jej przedstawianiu w znaczeniu propagandowym, technologicznym oraz geopolitycznym jako konwergencji nie środków, lecz form przestrzeni geopolitycznej (przestrzeń geograficzna, przestrzeń ekonomiczna, przestrzeń informacyjno-psychologiczna, przestrzeń informacyjno-cybernetyczna). Według rosyjskich ekspertów we wszystkich tych sferach są równocześnie prowadzone działania mające na celu zdobycie przewagi geopolitycznej nad przeciwnikiem, jego osłabienie i zmuszenie do podjęcia decyzji politycznych korzystnych dla agresora.

Środki militarne i niemilitarne w rosyjskiej myśli wojskowej XIX–XXI wieku w kontekście kryzysu ukraińskiego

Na skutek stworzonego na Zachodzie paradygmatu wojny hybrydowej nie można w pełni określić i wyjaśnić rosyjskich działań prowadzonych na południowym wschodzie państwa ukraińskiego. Aby określić rodzaj strategii i taktyki stosowanych przez stronę rosyjską, warto do tego celu wykorzystać paradygmat kulturowy, którego podstawą są takie czynniki, jak: mentalność, tradycja i archetypy historyczne. Taką metodę badawczą przyjmuje się wówczas, gdy argumentacja wynikająca z paradygmatu realistycznego i jego fundamentalnych założeń (czyli: równowagi sił, interesu narodowego, „dylematu bezpieczeństwa") jest niewystarczająca[36]. Nowa sytuacja geopolityczna pokazała bowiem, że bazujące na powyższych czynnikach metody badań polityki Rosji nie umożliwiły uzyskania pełnej wiedzy na temat środków, metod i rzeczywistych sposobów działania. Należy pamiętać, że sposób prowadzenia wojny należy do integralnych aspektów rozwoju każdego społeczeństwa i jest dla niego tak samo charakterystyczny, jak wszelkie inne cechy. W wojnie wyraża się kultura danego społeczeństwa, wojna bywa także determinantem kultury danej społeczności lub narodu[37].

Opinie tę można również odnieść do rosyjskiej sztuki wojennej, która od stuleci jest oparta na odmiennych od wojskowości zachodniej tradycjach historycznych. Jako jeden z pierwszych tematykę tę podjął Włodzimierz Bączkowski. Analizy geostrategiczne jego autorstwa, których podstawą są badania sowietologiczne, dotyczą refleksji nad istotą „siły rosyjskiej" rozumianej jako fenomen kulturowy[38]. W. Bączkowski

[36] T.W. Grabowski, *Rosyjska siła. Siły Zbrojne i główne problemy polityki obronnej Federacji Rosyjskiej w latach 1991–2010*, Częstochowa 2011, s. 11–12; M. Деш, *Столкновения вокруг культуры: к оценке роли идей в исследованиях проблем безопасности*, „Pro et Contra" 1998, nr 3, s. 115.

[37] J. Keegan, *Historia wojen*, Warszawa 1998, s. 153. Szerzej na ten temat zob. M. van Creveld, *The Culture of War*, New York 2008, s. 169–229.

[38] Zob. W. Bączkowski, *Uwagi o istocie siły rosyjskiej*, w: *O wschodnich problemach Polski. Wybór pism*, W. Kloczkowski, P. Kowal (red.), Kraków 2000, s. 112–133; tenże, *Russian Colonialism: the Tsarist and Soviet*

doszedł do wniosku, że rosyjską państwowość uwarunkowały wpływy bizantyńskie, przejawiające się w odmiennej od europejskiej koncepcji władzy świeckiej, związki Rosji z dziedzictwem Chin i Orientu, a przede wszystkim zależność od imperium mongolskiego, przy nikłym oddziaływaniu kulturowym Zachodu. Wpływy te ukształtowały także rosyjską sztukę wojenną, która kładła nacisk na wykorzystanie różnorodnych środków, niekoniecznie militarnych: dyplomacji, intryg, propagandy, wywiadu, dywersji, pobudzania i wzniecania konfliktów etnicznych, stosowania forteli i podstępów wojennych. Udany podstęp uprawniał do odczuwania intelektualnej satysfakcji, główną natomiast zaletą wodzów powinna była być mądrość polegająca na osiągnięciu zwycięstwa bez narażania się na niebezpieczeństwo. Zwycięstwo jest jedno, środki zaś, którymi posługują się wodzowie, są odmienne i w swej istocie różnorodne[39]. Problematyka ta została poruszona m.in. w dziele *Sztuka wojny* autorstwa Sun Tzu, które do dzisiaj cieszy się ogromną popularnością wśród rosyjskich wojskowych, szczególnie jako źródło inspiracji dla opracowywania metod decepcji przeciwnika[40].

W tym kontekście W. Bączkowski powołuje się na ustalenia carskich i radzieckich oficerów z XIX i pierwszej połowy XX wieku, wykorzystując m.in. opinię księcia Nikołaja Golicyna (1850–1925), członka Wojennego Komitetu Naukowego przy Sztabie Głównym Armii Imperium Rosyjskiego w Sankt Petersburgu. N. Golicyn we wstępie do książki autorstwa gen. Iwanina, wydanej w kwietniu 1875 r., pisał, że jego praca (…) *tłumaczy nam, w jaki sposób system wojenny Czingischana był po części opanowany przez nas, wchodząc w ciągu dwóch stuleci tatarskiej niewoli w nasze wojskowe obyczaje w okresie przed reformami Piotra I*[41]. W. Bączkowski cytuje również opinię współczesnego mu radzieckiego stratega i historyka wojskowości gen. majora carskiej armii Aleksandra Swieczina (1878–1938), który, opisując historię radzieckiej sztuki wojennej, podkreślał:

> (…) zapożyczyliśmy na Wschodzie głęboki respekt dla techniki strzelniczej, dla prowadzenia walki z głębi (…) wielką uwagę dla służby wywiadowczej i ubezpieczenia

Empires, New York 1958. Szerzej na temat rosyjskiej kultury strategicznej zob. D. Adamsky, *The Culture of Military Innovation. The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, Stanford 2010, s. 24–58; S.J. Blank, *Class War on a Global Scale: The Leninist Culture of Political Conflict*, w: *Conflict, Culture, and History: Regional Dimensions*, S.J. Blank, E.L. Grinter (red.), Alabama 1993, s. 1–51; T.W. Grabowski, *Rosyjska siła*…, s. 11–46.

[39] W. Bączkowski, *Uwagi o istocie siły rosyjskiej*…, s. 129–130. Por. D. Ostrovski, *Muscovy and the Mongols. Cross Cultural Influences on the Steppe Frontier, 1304–1589*, Cambridge 1998, s. 36–64; K.C. Gustafson, *Protecting the New Rome: Byzantine Influences on Russian Intelligence*, w: *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, P.H.J. Davies, K.C. Gustafson (red.), Georgetown 2013, s. 67–89; С.П. Карпов, *Роль византийского наследия на Руси в формировании российской государственности и русской культуры*, w: *Российская государственность: исторические традиции и вызовы XXI века. Материалы Всероссийской научно-общественной конференции (Великий Новгород, 19 сентября 2012 г.)*, Москва 2013, s. 58–66.

[40] Odnośnie do wykorzystania starożytnych podstępów wojennych i dzieła Sun Tzu we współczesnych rosyjskich teoriach wojskowych zob. М.Ф. Ваккаус, *О военно-политических основах методологии строительства и применения Вооруженных Сил России*, „Военная мысль" 2009, nr 6, s. 60–67; В.Н. Каранкевич, *Как научиться обманывать противника*, „Военная мысль" 2006, nr 9, s. 44–58; В.И. Орлянский, *К вопросу о сущности обмана противника*, „Военная мысль" 2007, nr 7, s. 72–80; В.Д. Рябчук, *Еще раз о сущности обмана противника*, „Военная мысль" 2008, nr 1, s. 48–52; Г.Л. Смолян, *Рефлексивное управление – технология принятия манипулятивных решений*, „Труды Института Системного Анализа РАН" 2013, nr 2, s. 54–61.

[41] W. Bączkowski, *Uwagi o istocie siły rosyjskiej*…, s. 119. Por. М.И. Иванин, *О военном искусстве и завоеваниях монголо-татар и средне-азиятских народов при Чингис-хане*, Санкт-Петербург 1875, s. 6.

> (…). Azjatycka strategia wymagała przewidującej, przewrotnej polityki. Wszelki środek był uważany za dobry, o ile prowadził do sukcesu militarnego. Mongołowie nie skąpili pieniędzy na przekupienie, nie skąpili słów na obiecanki, wszelkie środki przeciwstawienia jednych interesów dynastycznych przeciwko drugim były wykorzystywane. Prawdopodobnie większa wyprawa wojskowa była przedsiębrana tylko wówczas, gdy zjawiła się pewność, że w organizmie państwowym sąsiada powstały głębokie szpary[42].

Echo tych spostrzeżeń pobrzmiewa także w zaleceniach Borysa Szaposznikowa (1882–1945), szefa Sztabu Generalnego RKKA, które zawarł w monografii pt. *Mózg armii*. Na jej kartach argumentował, że gwarantem zwycięstwa jest całkowity rozkład wewnętrzny nieprzyjaciela przez wykorzystanie wszystkich jego słabości. Przeciwnik musi zostać pokonany przed uderzeniem na niego siłami zbrojnymi, które powinny dokonać jedynie pacyfikacji wroga. Głównym sposobem przygotowania klęski nieprzyjaciela jest przeniknięcie do jego struktur państwowych, komórek decyzyjnych i dokonanie ich rozkładu od wewnątrz przez działania o charakterze dyplomatycznym, wywiadowczym, dywersyjnym i propagandowym oraz za pomocą wszelkich innych dostępnych środków[43].

Badając przebieg rosyjskich kampanii wojennych z wieków XVIII–XX, W. Bączkowski wskazuje, że terytoria, które stały się obiektem rosyjskiej ekspansji, były zamieszkiwane z reguły przez *narody znajdujące się w stanie upadku* lub *niestawiające większego oporu*. Według niego o powodzeniu rosyjskich podbojów przesądzały zwykle warunki niezależne od siły militarnej.

Rola siły zbrojnej Rosji we wszystkich tych wydarzeniach występuje w świetle bladym, jako coś marginalnego, co będąc zawsze słabym, jednocześnie umie zwyciężać, dzięki wspaniale układającym się okolicznościom ubocznym, przy których na pierwszy plan wysuwa się czynnik uchwycenia odpowiedniego momentu oraz świadomego tworzenia dogodnego dla siebie układu stosunków. Stajemy w ten sposób przed zjawiskiem siły rosyjskiej, leżącej gdzieś poza formalną siłą militarną[44].

W kontekście kulturowym jest także osadzona rosyjska koncepcja tzw. małej wojny (ros. ‘*малая война*’), której zasady po raz pierwszy skodyfikowano w Niemczech na przełomie XVIII i XIX stulecia[45]. Teoria i praktyka „małej wojny” zyskała szczególną popularność w Rosji, gdzie począwszy od pierwszej połowy XIX w. sposoby jej prowadzenia były systematycznie rozwijane i doskonalone. Dlatego też punktem wyjścia dla niniejszych rozważań jest wiek XIX. W okresie do I wojny światowej pod pojęciem „mała wojna” rozumiano tylko i wyłącznie walkę zbrojną prowadzoną przez działania o charakterze partyzanckim, realizowane przez niewielkie, lotne pododdziały wydzielone z większej części regularnej armii. Polegały one m.in. na niszczeniu linii zaopatrzenia i komunikacji nieprzyjacielskich wojsk, przechwytywaniu kurierów, likwidowaniu małych placówek i oddziałów wroga, niespodziewanych uderzeniach na tyły i flanki nieprzyjacielskich wojsk, sianiu paniki i ciągłym nękaniu wroga, przy unikaniu jak największych strat własnych[46].

---

[42] W. Bączkowski, *Uwagi o istocie siły rosyjskiej*…, s. 118–119. Por. A.A. Свечин, *Эволюция военного искусства с древнейших времен до наших дней*, t. 1, Москва 1927, s. 143–152.

[43] Б.М. Шапошников, *Мозг армии*, t. 3, Москва 1929, s. 226–334, w której autor szczegółowo omawia przedmiotową problematykę.

[44] W. Bączkowski, *Uwagi o istocie siły rosyjskiej*…, s. 114.

[45] A. von Bogusławski, *Der kleine Krieg und seine Bedeutung für die Gegenwart*, Berlin 1881, s. 10–17.

[46] *Военный энциклопедический лексикон: Том VIII*, Санкт-Петербург 1855, s. 427–428; Г.А. Леер,

Mimo że tradycja tego rodzaju działań sięga w Rosji czasów Piotra I, to szczegółowe zasady „małej wojny" po raz pierwszy opisał kpt. hrabia Denis Dawydow (1784–1839) w traktacie pt. *Zarys teorii działań partyzanckich*, który ukazał się w 1821 r.[47] W drugiej połowie XIX stulecia koncepcję „małej wojny" wzbogacono o problematykę działań policyjnych (tłumienie zamieszek, buntów, organizacja karnych ekspedycji i działań pacyfikacyjnych). W tym celu studiowano sposoby psychologicznego oddziaływania na przeciwnika (nie tylko na jego siły zbrojne, lecz także na ludność cywilną) oraz zagadnienia dotyczące psychologii tłumu i manipulowania nim[48].

Całkowita zmiana znaczenia terminu „mała wojna" oraz jej koncepcji nastąpiła w pierwszych latach istnienia bolszewickiej Rosji (tzw. *новая большая стадия малой войны*). W broszurze z 1921 r. pt. *Jedna doktryna wojenna i Armia Czerwona* były carski wojskowy Michaił Frunze podjął się próby teoretycznego opracowania koncepcji „małej wojny". Według niego miała ona zakładać systematyczne i planowe działanie w celu stworzenia dla armii nieprzyjacielskiej takich warunków, żeby jego przewaga techniczna okazała się bezsilna wobec słabo uzbrojonego, ale pełnego inicjatywy, śmiałego i zdecydowanego przeciwnika[49].

Koncepcję M. Frunzego sprecyzował M. Drobow w swojej książce pt. *Mała wojna. Partyzantka i dywersja*, która ukazała się w 1931 r. Według M. Drobowa „mała wojna" – określana także jako „wojna partyzancka", „operacja półwojenna" lub „ruch narodowo-wyzwoleńczy" – stanowi (…) *przejściową formę klasowej walki zbrojnej, której celem jest przejęcie władzy i ustanowienie dyktatury proletariatu*. Poprzestając na tym ogólnym odwołaniu się do ideologii marksizmu-leninizmu, M. Drobow, wykorzystując koncepcje carskich wojskowych i doświadczenia bolszewików, scharakteryzował amorficzną naturę „małej wojny". Według radzieckiego teoretyka jest to kompleks różnorodnych, aktywnych działań o charakterze wspomagającym lub improwizacyjnym, prowadzonych w celu spowodowania za pomocą wszelkich dostępnych środków maksymalnego uszczerbku w potencjale wroga wszędzie tam, gdzie jest to tylko możliwe. Działania te mają ułatwić walkę na głównych frontach wojny i spowodować jak największe osłabienie potencjału nieprzyjaciela. M. Drobow uważa też, że „małą wojnę" należy prowadzić zarówno w okresie pokoju, jak i wojny (tutaj rozumianych w klasycznym znaczeniu tych słów). Jej forma ulega ciągłej transformacji: w procesie swojego rozwoju może przybrać postać wojny lokalnej, regionalnej lub wielkiego powstania. „Mała wojna" może także być stopniowo wygaszana, przechodząc w dywersję lub inne skryte formy działalności wywrotowej prowadzonej *słowem i czynem*. Radziecki teoretyk podkreśla, że „mała wojna" jest samodzielnym bytem, który charakteryzuje się dynamiką widoczną w sposobach i metodach

Энциклопедия военных и морских наук: Том V, Санкт-Петербург 1891, s. 38; *Военная енциклопедия*, К.И. Величко (red.), Москва 1914, s. 136–137. Szerzej zob. И.В. Вуич, *Малая война*, Санкт-Петербург 1850, s. 139–254. Literatura dotycząca koncepcji „małej wojny" jest bogata. Tutaj ograniczono się jedynie do wymienienia najważniejszych publikacji. Antologię tekstów na temat koncepcji „małej wojny" w rosyjskiej teorii i praktyce wojskowej w okresie XIX–XXI stulecia oraz obszerną bibliografię zawiera m.in. opracowanie *Грозное оружие: Малая война, партизанство и другие виды асимметричного воевания в свете наследия русских военных мыслителей*, И.В. Домнин (red.), Москва 2007.

[47] Д.В. Давыдов, *Опыт теории партизанского действия*, Москва 1821, s. 31–109; В.И. Боярский, *Партизанство вчера, сегодня, завтра. Историко-документальный очерк*, Москва 2003, s. 14–18.

[48] М.А. Дробов, *Малая война. Партизанство и диверсия. Репринтное воспроизведение издания 1931 г.*, Москва 1998, s. 37; А. Зыков, *Как и чем управляются люди. Опыт военной психологии*, Санкт-Петербург 1898, s. 62–169.

[49] М.В. Фрунзе, *Единая военная доктрина и Красная армия*, „Красная Новь" 1921, nr 1, s. 94–106. Zob. В.В. Квачков, *Спецназ России*, Москва 2007, s. 42.

jej prowadzenia. Nie jest możliwe jej sklasyfikowanie i zamknięcie jej zasad w schemacie: formy „małej wojny" są zależne od twórczego potencjału podmiotów zaangażowanych w jej prowadzenie. W opinii M. Drobowa w „małej wojnie" należy wykorzystać wszystkie dostępne środki, którymi dysponuje dana klasa społeczna. Czym bardziej są one różnorodne, pomysłowe i rozwinięte, tym bardziej wzrasta skuteczność działań prowadzonych w ramach „małej wojny"[50].

Podstawowymi formami prowadzenia „małej wojny" są: partyzantka i dywersja. M. Drobow rozróżniał dwa rodzaje partyzantki: wojskową i typu powstańczego. Z kolei dywersja w ujęciu autora to działania prowadzone w czasie pokoju i wojny w sposób niejawny przez niewielkie, specjalnie do tego celu przeszkolone grupy. Głównym celem dywersji, która powinna mieć wszechstronny charakter, jest przede wszystkim oddziaływanie na psychikę przeciwnika, osłabienie jego woli walki i rozkład morale. Radziecki teoretyk rozróżniał następujące formy dywersji:

1) dywersja o charakterze ekonomicznym – uderzenia w transport, przedsiębiorstwa, osłabienie systemu finansów publicznych,
2) dywersja o charakterze politycznym – zakładała prowadzenie działań propagandowych (w tym propagandy specjalnej), inicjowanie wszelkiego rodzaju intryg, których celem powinny być struktury rządowe oraz organizacje wywierające jakikolwiek wpływ na społeczeństwo,
3) dywersja o charakterze militarnym – sabotaż sprzętu bojowego, wysadzanie składów, arsenałów i umocnień, niszczenie węzłów łączności itp.,
4) dywersja o charakterze terrorystycznym – polegała na likwidacji przez zabicie lub otrucie cywilnych lub wojskowych przywódców danego państwa[51].

Według M. Drobowa działania partyzanckie i dywersyjne należy prowadzić w sposób skoordynowany i kompleksowy nie tyle na całej przestrzeni frontu, ile wewnątrz nieprzyjacielskiego kraju z uwzględnieniem miejsca i czasu[52]. Cennym uzupełnieniem jego rozważań była publikacja autorstwa Konstantina K. Zwonariewa, wydana przez IV Zarząd Sztabu Generalnego RKKA w 1929 r., którą autor poświęcił wywiadowi agenturalnemu. W pierwszym tomie dzieła K. Zwonariew uznawał tzw. wywiad aktywny (dywersję) za część wywiadu agenturalnego. Publikacja ta stanowiła podstawy teoretyczne radzieckiej szkoły dywersji, która znalazła praktyczne zastosowanie w okresie Wielkiej Wojny Ojczyźnianej[53].

Okres powojenny w historii sowieckiej myśli wojskowej był czasem stagnacji. Czynnikiem, który ją spowodował, był rozwój technologii rakietowo-nuklearnej oraz konieczność liczenia się z ideologiczną, marksistowsko-leninowską teorią wojen.

[50] М.А. Дробов, *Малая война*…, s. 11, 198–200; В.В. Квачков, *Спецназ России*…, s. 42–43.

[51] М.А. Дробов, *Малая война*…, s. 158–159. Odnośnie do propagandy specjalnej (tzw. specpropagandy) w Armii Czerwonej zob. И.Б. Мощанский, *Информационная война. Органы спецпропаганды Красной армии*, Москва 2010, s. 8 i nast.

[52] М.А. Дробов, *Малая война*…, s. 199.

[53] К.К. Звонарев, *Агентурная разведка. Русская агентурная разведка всех видов до и во время войны 1914–1918 гг. Германская агентурная разведка до и во время войны 1914–1918 гг. Репринтное воспроизведение издания 1931 г.*, Киев 2005, s. 324–333; В.А. Иванов, *Разведывательная работа германского Генштаба против армий Северного фронта и борьба со шпионажем в 1915–1917 годах (из документов Архива УФСБ РФ по Санкт-Петербургу и Ленобласти)*, „Новейшая история России" 2014, nr 3, s. 292–311; В.В. Квачков, *Спецназ России*…, s. 46–47.

Koncentracja na wojnie rakietowo-jądrowej była tak duża, że nastąpiła atrofia myśli strategicznej poświęconej wojnie prowadzonej innymi siłami. Przewidywano zastosowanie broni atomowej zarówno na szczeblu strategicznym, jak i operacyjnym, a nawet taktycznym. Scenariusz wojny jądrowej zakładał, że kolejne uderzenia jądrowe miały być skierowane w siły zbrojne nieprzyjaciela, ośrodki miejskie i przemysłowe, co w konsekwencji miało zniszczyć potencjał ekonomiczny i morale wroga. Siłom konwencjonalnym pozostawiono jedynie spełnienie roli pacyfikacyjnej. W takich warunkach następowało stopniowe dezaktualizowanie się sowieckiej strategii militarnej[54].

Koncepcja „małej wojny", która zyskała wówczas miano „wojny rewolucyjnej", była jednak stosowana do prowadzenia walki za pośrednictwem tzw. ruchów narodowo-wyzwoleńczych w licznych wojnach lokalnych, toczonych głównie w krajach Trzeciego Świata[55]. Były one narzędziem geopolitycznej konfrontacji z USA w dwubiegunowym modelu świata, który ukształtował się po 1945 r. W „wojnach rewolucyjnych" wykorzystywano charakterystyczne dla „małej wojny" partyzanckie metody walki zbrojnej w połączeniu z działaniami propagandowymi, agitacyjnymi i terrorystycznymi. Przedsięwzięcia te zyskały także miano „aktywnych działań" (ros. *'активные мероприятия'*). Kluczowym elementem „aktywnych działań" była dywersja ideologiczna (ros. *'идеологическая диверсия'*), której pojęcie, w odróżnieniu od USA i pozostałych krajów członkowskich NATO, w Związku Radzieckim rozumiano bardzo szeroko. Dywersja ideologiczna w ujęciu radzieckich strategów i funkcjonariuszy KGB, utożsamiana także z pojęciem wojny psychologicznej, to jedna z podstawowych form działalności służb specjalnych polegająca na agitacyjno-propagandowych i wywiadowczo-organizacyjnych działaniach, przedsięwzięciach i operacjach prowadzonych w celu zdestabilizowania władz politycznych, moralno-politycznego stanu społeczeństwa i sił zbrojnych. Miało to doprowadzić do zmiany wewnętrznej i zagranicznej polityki danego państwa. Dywersja ideologiczna przejawiała się zarówno w bezpośrednich formach działalności wywrotowej (akty terrorystyczne i dywersyjne, likwidowanie działaczy społecznych i politycznych, walka zbrojna), jak i metodach pośrednich (inspirowanie, tworzenie i kierowanie działalnością tajnych i jawnych organizacji w danym kraju, działania dyplomatyczne, propagandowe, szantaż i korupcja). Tego rodzaju oddziaływaniu poddawano wszystkie sfery aktywności państwowej i społecznej, takie jak: religię, dominującą ideologię, politykę, ekonomię, moralność i system etyczny, prawo, kulturę i naukę. Działaniami podmiotów dywersji ideologicznej kierował 1. Zarząd Główny KGB, który umożliwiał także wywiadowczo-informacyjne zabezpieczenie poszczególnych operacji. Głównym celem dywersji ideologicznej była destrukcja kluczowych dziedzin aktywności społecznej, co miało doprowadzić do osłabienia państwa i pozbawienia go zdolności obronnych w przypadku wrogiej napaści[56].

---

[54] T.W. Grabowski, *Rosyjska siła*…, s. 48–49; *Военная стратегия*, В.Д. Соколовский (red.), Москва 1963, s. 19–23; 258–261; А.И. Калистратов, *Революция в военном деле и советское военное искусство*, „Военная мысль" 2009, nr 11, s. 17–29.

[55] В.А. Пронько, *Военная стратегия после Второй Мировой Войны*, w: *История военной стратегии России*, В.А. Золотарев (red.), Москва 2000, s. 479–486; *Военная стратегия*…, s. 227; Zob. przykłady tego rodzaju działań w: *SNIE 11/2–81, May 1981, Soviet Support for International Terrorism and Revolutionary Violence*, w: *CIA's Analysis of the Soviet Union 1947–1991. A Documentary Collection*, G.K. Haines, R.E. Legget (red.), Washington 2001, s. 105–108.

[56] *Высшая школа КГБ им. Ф.Э. Дзержинского. Научно-издательский отдел ВШКГБ им. Ф.Э.*

Problematyką wojny asymetrycznej zajmowali się również rosyjscy wojskowi przebywający na emigracji. Głównym osiągnięciem rosyjskiej emigracyjnej myśli wojskowej jest kontynuacja badań nad „małą wojną", które prowadził gen. Borys Holmston-Smysłowskij (1897–1988) oraz koncepcja „wojny buntowniczej" (ros. *'мятежевойна'*) Jewgienija Messnera (1891–1974)[57]. Podobnie jak „mała wojna" radzieckich wojskowych, tak i koncepcje wojen asymetrycznych w ujęciu emigracyjnych strategów charakteryzują się elastycznością, przybierając wiele form. Do najważniejszych desygnatów tych koncepcji należą:

- brak formalnego wypowiedzenia wojny, zatarcie różnic między okresem pokoju i wojny rozumianych w klasycznym znaczeniu tych słów,
- działania prowadzące do uniknięcia oficjalnego zaangażowania się państwa w konflikt zbrojny, brak monopolu państwa na prowadzenie działań militarnych,
- brak linii frontu, działania mogą rozpocząć się wewnątrz państwa z dala od jego granic,
- brak formalnej przynależności państwowej grup i formacji zbrojnych biorących udział w walkach,
- zrównanie roli uzbrojonych, zrewoltowanych grup społecznych z regularną armią, wzrost znaczenia sił specjalnych i tajnych służb. W ten paradygmat wpisują się m.in. rozważania gen. Holmstona-Smysłowskiego, które dotyczą możliwości koordynacji działań między operacjami desantowymi regularnych wojsk a podmiotami stosującymi taktykę „małej wojny"[58],
- kluczowe znaczenie mają długofalowe działania o charakterze psychologicznym, których głównym celem jest uzyskanie wpływu na społeczną świadomość. Ciężar prowadzenia takich działań spoczywa na dyplomatach, dywersantach, terrorystach i agitatorach,
- inspirowanie, organizowanie i finansowanie rozwoju ugrupowań radykalnych i ekstremistycznych (m.in. politycznych, religijnych) w państwie nieprzyjaciela,
- wzrastające znaczenie w stosunkach międzynarodowych roli państw nieuznawanych i państw dysfunkcyjnych (tzn. „upadłych"), przeniesienie głównego ciężaru walk na tereny zurbanizowane[59].

Дзержинского, Контрразведывательный словарь, Л.В. Каленская, Ю.И. Смирнов (red.), Москва 1972, s. 90–91, 161–162, 239–240; R. Shultz, *The Soviet Union and Revolutionary Warfare: Principles, Practices, and Regional Comparisons*, Stanford 1988, s. 115–187; D.S. Papp, *Soviet Unconventional Conflict Policies and Strategies in the Third World*, „The Journal of Conflict Studies" 1988, nr 8, s. 26–59; L. Pawlikowicz, *Organizacja, zadania oraz wybrane problemy funkcjonowania legalnych rezydentur zagranicznych wywiadu KGB w latach 1954–1991*, w: *Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne*, Z. Nawrocki (red.), Warszawa 2013, s. 137.

[57] И.В. Домнин, *Краткий очерк военной мысли Русского Зарубежья*, w: *Военная мысль в изгнании. Творчество русской военной эмиграции*, И.В. Домнин (red.), Москва 1999, s. 448–527.

[58] Б. Хольмстон-Смысловский, *О возможностях координации действий оперативно-воздушных десантов с элементами малой войны*, w: *Первая Русская национальная армия против СССР. Война и политика*, И.В. Домнин (red.), Москва 2011, s. 356–268.

[59] Б. Хольмстон-Смысловский, *О психологии «малой войны»*, w: *Первая Русская национальная армия*…, s. 280–297; Е.Э. Месснер, *Всемирная мятежевойна*, Москва 2004, s. 15–23, 210–214, 216–228, 332–340. Koncepcja „wojny buntowniczej" Jewgienija Messnera została szczegółowo omówiona przez autora niniejszego artykułu w odrębnym opracowaniu. Tutaj ograniczono się jedynie do przedstawienia jej głównych założeń. Szerzej zob. M. Wojnowski, *Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji „wojny buntowniczej" Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 58–91. Por. L. Sykulski, *Rosyjska koncepcja wojen*

Rewolucja naukowo-techniczna dokonana z inicjatywy marszałka Nikołaja Ogarkowa w siłach zbrojnych ZSRR w latach 80. XX w., która przejawiała się w zastosowaniu nowoczesnych technologii w dziedzinie uzbrojenia, komunikacji i środków masowego przekazu, znacznie zwiększyła możliwości i efektywność operacji prowadzonych w ramach wojen asymetrycznych[60]. Nowe rozwiązania technologiczne znalazły zastosowanie w koncepcji tzw. asymetrycznej odpowiedzi ZSRR na ogłoszoną 23 marca 1983 r. przez prezydenta Ronalda Regana Inicjatywę Obrony Strategicznej (Strategic Defense Initiative – SDI). Ze względu na użycie nowoczesnej techniki w budowie systemu antyrakietowego przeznaczonego do likwidacji rakiet balistycznych skierowanych na terytorium USA program ten nazywano potocznie „Gwiezdnymi wojnami". Prace nad programem sowieckiej „asymetrycznej odpowiedzi" prowadził zespół wojskowych i naukowców pod kierownictwem fizyka Jewgienija Wielichowa. W opracowywaniu formuły „asymetrycznej strategii" brał udział m.in. radziecki uczony i ekspert ds. bezpieczeństwa Andriej Kokoszin. Sięgnął on do koncepcji wspomnianego stratega Andrieja Swieczina, który zajmował się analizą działań asymetrycznych w różnych okresach historii wojskowości. Szczególne znaczenie dla koncepcji „asymetrycznej odpowiedzi" A. Kokoszina, zarówno w znaczeniu wojskowo-technicznym, jak i polityczno-psychologicznym, miało wspomniane już dzieło *Sztuka wojny* Sun Tzu. Jak podkreślał A. Kokoszin, traktat ten, *przesiąknięty duchem asymetryczności*, był dla niego inspiracją. Koncepcja „asymetrycznej odpowiedzi" w sferze technologicznej zakładała zastosowanie zintegrowanych podzespołów w postaci systemu rakietowego i nowych rodzajów broni tzw. perspektywicznej generacji (broń wiązkowa, laserowa i plazmowa, broń geofizyczna i klimatyczna, która oddziałuje na litosferę, jonosferę i atmosferę). Równie istotną rolę w formule radzieckiej „asymetrycznej odpowiedzi" odgrywał czynnik polityczno-psychologiczny. Zakładano przeprowadzenie szerokiej operacji informacyjno-psychologicznej w celu przekonania „amerykańskiej klasy politycznej", że Inicjatywa Obrony Strategicznej nie umożliwi Stanom Zjednoczonym uzyskania przewagi strategicznej na świecie. Ponadto, przez szerokie spektrum akcji w ramach dywersji ideologicznej, oddziaływania informacyjnego i propagandowego, starano się nakłonić amerykańskie elity, aby te nie dopuściły do wyjścia USA z układu o ograniczeniu systemów antyrakietowych (Anti-Ballistic Missle, ABM) podpisanego 26 maja 1972 r., który, zdaniem radzieckich wojskowych, zapewniał „równowagę strategiczną" pomiędzy ZSRR a USA[61].

Mając na uwadze założenia „odpowiedzi asymetrycznej", należy podkreślić, że pomimo faktu zastosowania nowoczesnych technologii, w dalszym ciągu jej koncepcja opierała się na wypracowanych w przeszłości wzorcach osiągania celów politycznych metodami niewojskowymi w formie dywersji, propagandy, tworzenia podziałów w obozie przeciwnika itp. To za ich pomocą starano się zniwelować prze-

buntowniczych Jewgienija Messnera, „Przegląd Geopolityczny" 2014, nr 11, s. 103–113; K. Kraj, *Ukraina i мятежевойна*, „E-Terroryzm" 2014, nr 7, s. 11–22.

[60] M.C. FitzGerald, *Marshal Ogarkov and the New Revolution in Soviet Military Affairs*, Alexandria 2003, s. 6–12; tenże, *Soviet Views on Future War: The Impact of New Technologies*, „Defense Analysis" 1991, nr 7, s. 171–208, tenże, *Advanced Conventional Munitions and Moscow's Defensive Force Posture*, „Defense Analysis" 1990, nr 6, s. 167–191.

[61] С.К. Ознобищев, В.Я. Потапов, В.В. Скоков, *Как готовился "асимметричный ответ" на "стратегическую оборонную инициативу" Р. Рейгана, Велихов, Кокошин и другие*, Москва 2008, s. 11, 20; А.А. Кокошин, *«Асимметричный ответ» на «Стратегическую оборонную инициативу» как пример стратегического планирования в сфере национальной безопасности*, „Международная жизнь" 2007, nr 7, s. 29–42.

wagę techniczną USA. Wydaje się, że na identycznym założeniu opierają się także współczesne rosyjskie koncepcje prowadzenia działań asymetrycznych. Jak podkreśla gen. Mahmut Gariejew, prezes Akademii Nauk Wojskowych, nowoczesne technologie i rozwój nowych rodzajów broni spowodują zwiększenie skuteczności dotychczasowych sposobów prowadzenia wojny, szczególnie w sferze informacyjnej. Pisał on m.in., że:

> (…) systematyczna emisja psychologicznie i ideologicznie nasyconego materiału o prowokacyjnej naturze, zawierającego zmieszane fałszywe i prawdziwe elementy informacji, może skutkować masową psychozą, powodować uczucie rozpaczy i przygnębienia oraz podważać zaufanie do własnego rządu i sił zbrojnych, co w konsekwencji może doprowadzić do zdestabilizowania sytuacji w kraju będącym obiektem takiego oddziaływania[62].

W historyczne i kulturowe tradycje rosyjskiej wojskowości wpisuje się treść wystąpienia szefa Sztabu Generalnego Sił Zbrojnych FR, gen. armii Walerija Gierasimowa. Wystąpienie to posłużyło zachodnim analitykom jako podstawa do uznania rosyjskiej strategii i taktyki za nową metodę prowadzenia „wojny hybrydowej". Referat wygłoszony przez generała uznano nawet za ogłoszenie nowej doktryny wojennej Rosji, którą nazwano „Dokryną Gierasimowa"[63]. Wystąpienie szefa Sztabu Generalnego Sił Zbrojnych FR odbyło się 25 stycznia 2013 r. podczas konferencji w Akademii Nauk Wojskowych w Moskwie. Generał podkreślił, że przebieg wydarzeń w Afryce i na Bliskim Wschodzie uwidocznił zmiany, które dokonały się w sposobach prowadzenia wojen. Działania wojenne (nazwał je „wojną nowej generacji"), nie sprowadzają się już do pokonania sił zbrojnych nieprzyjaciela i zajęcia jego terytorium. Dodał, że precyzyjne określenie granicy między wojną a pokojem stało się niemożliwe. Głównym celem we współczesnych konfliktach staje się systematyczny i planowy rozkład wszystkich struktur wrogiego państwa, co ma na celu jego maksymalne osłabienie[64]. Jest to realizowane za pomocą wielu środków, które Gierasimow określa terminami zapożyczonymi z zachodnich teorii wojskowości: strategia działań pośrednich (ros. *'стратегия непрямых действий'*) oraz środki niewojskowe (ros. *'невоенные средства'*). W opinii szefa sztabu rosyjskiej armii są to działania o charakterze politycznym, ekonomicznym, informacyjnym, a nawet humanitarnym, które prowadzi się wraz z wykorzystaniem „potencjału protestu" tkwiącego w społeczeństwach państw stanowiących cel agresji. Działania te mogą polegać także na politycznym izolowaniu danego państwa, wprowadzeniu sankcji

[62] M.A. Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, London 1998, s. 53.

[63] M. Galeotti, *The 'Gerasimov-doctrine' and Russian Non-Linear War*, Moscow's Shadows Wordpress.com z 6 VII 2014 [online], https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ [dostęp: 1 IX 2015]; R. McDermott, *Myth and Reality – A Net Assessment of Russia's 'Hybrid Warfare' Strategy Since the Start of 2014 (Part One)*, „Eurasia Daily Monitor" 2014, nr 11 [online], http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42966&no_cache=1#.VfLKCRHtlBc [dostęp: 1 IX 2015].

[64] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер" 2013, nr 8, s. 2. Por. tenże, *Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утверждённым Президентом Российской Федерации*, „Вестник Академии военных наук" 2014, nr 1, s. 14–23; tenże, *Генеральный штаб и оборона страны*, „Геополитика и безопасность" 2014, nr 1, s. 16–20.

ekonomicznych, blokowaniu szlaków komunikacji, szantażu militarnym, a nawet na zorganizowaniu kontyngentu międzynarodowych sił pokojowych rzekomo pod pretekstem obrony praw człowieka.

Pierwszorzędne znaczenie w tak pojętej koncepcji prowadzenia działań wojennych zajmują operacje sił specjalnych oraz środki walki informacyjnej. Według Gierasimowa działania zbrojne następują dopiero po osłabieniu nieprzyjaciela i pozbawieniu go zdolności obronnych. Rozpoczynają się one w okresie pokojowym, przez wprowadzenie na terytorium nieprzyjaciela niewielkich mobilnych pododdziałów wojskowych lub formacji nieregularnych, co odbywa się bez uprzedniego wypowiedzenia wojny. Walka przybiera formę działań charakteryzujących się dużą manewrowością i mobilnością różnych formacji zbrojnych, w tym sił specjalnych. Głównym celem walki zbrojnej jest zniszczenie potencjału militarno-ekonomicznego zaatakowanego państwa za pomocą krótkotrwałych precyzyjnych uderzeń w infrastrukturę krytyczną (problematyki tej dotyczy osobna koncepcja „wojny niekontaktowej/bezkontaktowej" autorstwa gen. Władimira Slipczenki)[65]. Atak następuje przez uderzenia na siły zbrojne i obiekty wrogiego państwa znajdujące się na całym jego terytorium, z uwzględnieniem miejsca i czasu. Walkę zbrojną charakteryzuje użycie na szeroką skalę broni precyzyjnego rażenia (ros. *'высокоточное оружие'*, BTO), robotyki oraz innych nowoczesnych rodzajów uzbrojenia. Gierasimow podkreśla przestrzenny wymiar konfrontacji: dochodzi do niej we wszystkich rodzajach przestrzeni geopolitycznej, tj. na lądzie, morzu i w powietrzu. Kierowanie siłami zbrojnymi i ich działaniami odbywa się w jednej przestrzeni informacyjnej. Według słów Gierasimowa w walce uczestniczy także tzw. komponent wojskowo-cywilny, czyli formacje paramilitarne i różnego rodzaju grupy o charakterze zbrojnym. Cały czas są prowadzone również działania o charakterze dywersyjnym i propagandowym, co pozwala zneutralizować przewagę nieprzyjaciela w określonych sferach[66].

W swoim wystąpieniu Gierasimow odwołał się do radzieckiego stratega Andrieja Swieczina, podkreślając ponadczasowy charakter jego opinii, według której (…) *każda wojna jest szczególnym przypadkiem, który wymaga stworzenia własnej, unikalnej logiki, a nie zastosowania jakiegokolwiek wzorca*[67]. W ten sposób generał dał do zrozumienia, że jest to jedynie zarys ogólnej koncepcji prowadzenia walki zbrojnej, jej przebieg i formy działań zaś zależą od wielu czynników i typu przeciwnika. Każda operacja o charakterze militarnym powinna być rozpatrywana indywidualnie, z uwzględnieniem m.in. takich czynników, jak cechy kulturowe, potencjał gospodarczy, profil psychologiczny elit rządzących oraz wszelkie słabości państwa stanowiącego obiekt potencjalnej agresji. Według rosyjskich wojskowych określenie i ocenę wszystkich tych czynników umożliwia tzw. analiza refleksyjna[68].

---

[65] В. Герасимов, *Ценность науки в предвидении*…, s. 3. Por. В.И. Слипченко, *Войны нового поколения: дистанционные бесконтактные*, Москва 2004, s. 44–58; В.А. Киселев, *Дистанционное противоборство*, „Военная мысль" 2008, nr 5, s. 77−84.

[66] В. Герасимов, *Ценность науки в предвидении*…, s. 3. Por. J. Beskid, *Vojna novej generácie realizovaná na Kryme*, w: *5. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnost. Zborník vedeckých a odborných prác*, B. Ďurkech (red.), Liptovský Mikuláš 2014, s. 24−33. Szczegółowym aspektom rosyjskiego modelu tzw. wojny nowej generacji autor niniejszego artykułu poświęcił odrębne opracowanie pt. *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskie*j, które znajduje się w druku.

[67] В. Герасимов, *Ценность науки в предвидении*…, s. 3.

[68] А.В. Первов, *Ситуационный анализ в сетевых войнах на основе рефлексивного подхода*, „Вестник академии военных наук" 2009, nr 2, s. 85–88. Por. М.В. Александров, *К вопросу о возможности создания*

Zastosowanie zachodniego paradygmatu „wojny hybrydowej" do określania specyfiki działań rosyjskich (przypomnijmy, że stanowi on jednolitą formułę środków wojskowych i niewojskowych) wydaje się nieskuteczne. Dzieje się tak dlatego, że koncepcja współczesnego konfliktu zbrojnego autorstwa gen. Gierasimowa nawiązuje do amorficznego charakteru koncepcji „małych wojen", „wojen buntowniczych" i „odpowiedzi asymetrycznych". Próżno szukać w nich ściśle określonego wzorca i paradygmatu prowadzonych działań. Zasady rzekomej nowej wojny, którą dostrzegają w koncepcji Gierasimowa zachodni eksperci, od stuleci pozostają niezmienne w rosyjskiej myśli wojskowej, z wyjątkiem zastosowania nowoczesnych rozwiązań technologicznych, które zwiększają możliwości prowadzonych operacji. Wystąpienie szefa Sztabu Generalnego nagłośnione w rosyjskich mediach, a następnie w zachodniej prasie, należy uznać za operację informacyjno-psychologiczną. Jej celem jest przekonanie zachodnich rządów i ich społeczeństw, że Rosja ma nową, nieznaną na Zachodzie, strategię działań wojennych. Słowa generała o rzekomych zmianach, które nastąpiły w sposobach prowadzenia wojen, co miały uwidocznić „kolorowe rewolucje" w Afryce Północnej i na Bliskim Wschodzie, są na Zachodzie interpretowane zbyt dosłownie[69]. Nie chodzi tutaj o nowatorskość sztucznego generowania rewolucji i przewrotów (praktykowanych od wieków), lecz o nowoczesne środki, które zostały wykorzystane do tego celu. W przypadku „arabskiej wiosny" było to m.in. zastosowanie na szeroką skalę mediów i portali społecznościowych (Facebook, Twitter), co stanowi rozwiązanie nowatorskie. Nowa nie jest więc sama idea inicjowania sztucznego przewrotu, lecz narzędzia, których użyto do realizacji tego celu[70].

Potwierdzeniem opinii o ścisłej zależności współczesnych rosyjskich koncepcji działań wojennych od znanych z przeszłości praw sztuki wojennej Imperium Rosyjskiego i ZSRR jest analiza autorstwa Siergieja Czekinowa i Siergieja Bogdanowa – wysokiej rangi oficerów związanych z Centrum Studiów Wojenno-Strategicznych Sztabu Generalnego Sił Zbrojnych FR. Ich rozważania są tożsame z treścią wystąpienia Gierasimowa. Według nich tzw. wojna nowej generacji charakteryzuje się:

- prowadzeniem długotrwałych działań asymetrycznych przez zastosowanie środków informacyjnych, psychologicznych, dyplomatycznych i ekonomicznych w celu osłabienia przeciwnika i stworzenia sprzyjających warunków ułatwiających agresję zbrojną,

---

математической модели прогнозирования военно-политической и стратегической ситуации вокруг РФ, w: *Некоторые аспекты анализа военно-политической обстановки: монография*, А.И. Подберезкина, К.П. Боришполец (red.), Москва 2014, s. 25−50; С.Н. Бухарин, В.В. Цыганов, *Ситуационный анализ в информационных войнах*, „Информационные войны" 2008, nr 2, s. 47−59; Н.М. Ракитянский, С.Н. Бухарин, *Ментальная матрица политической элиты в контексте теории информационного поля*, „Информационные войны" 2011, nr 1, s. 52−59.

[69] Zob. dla przykładu: A. Rácz, *Hybrid War in Ukraine*…, s. 36−37.

[70] P. Thorpe, *Information and Revolution in Egypt. Assessing the Role of New Media in Contemporary and Future Operating Environments*, „Special Warfare. The Professional Bulletin of the John F. Kennedy. Special Warfare Center and Schools" 2013, nr 26, s. 10–13; S. Lucente, G. Wilson, *Crossing the Red Line. Social Media and Social Network Analysis for Unconventional Campaign Planning*, „Special Warfare. The Professional Bulletin of the John F. Kennedy Special Warfare Center and Schools" 2013, nr 26, s. 20–26; M. Ben Moussa, *From Arab Street to Social Movements: Re-theorizing Collective Action and the Role of Social Media in the Arab Spring*, „Westminster Papers" 2013, nr 9, s. 47–71. Szerzej na temat roli mediów elektronicznych w kreowaniu potencjału protestu zob. M. Castells, *Networks of Outrage and Hope. Social Movements in the Internet Age*, Cambridge 2012, s. 218–244.

- zdezorientowaniem dowództwa sił zbrojnych oraz cywilnego przywództwa państwa wrogiego za pomocą kombinacji jawnych i tajnych działań prowadzonych za pośrednictwem mediów, dyplomacji, agencji i organizacji pozarządowych. Operacje te polegają przede wszystkim na wykorzystywaniu wszelkiego rodzaju sprzeczności etnicznych, politycznych, ekonomicznych i kulturowych w kraju stanowiącym obiekt agresji i wprowadzaniu fałszywych informacji, danych, instrukcji oraz rozkazów do przestrzeni informacyjnej nieprzyjaciela,
- zastraszaniem, oszukiwaniem, szantażowaniem i korumpowaniem przedstawicieli elit politycznych i wojska,
- stosowaniem na szeroką skalę różnego rodzaju środków propagandy i agitacji, których celem jest spowodowanie wzrostu niepewności, strachu i poczucia zagrożenia w społeczeństwie. Efekt ten jest potęgowany także przez działania dywersyjne i wywrotowe prowadzone przez różne grupy zbrojne, organizacje paramilitarne, związki zawodowe i inne organizacje,
- ustanowieniem strefy zakazu lotów nad terytorium zaatakowanego państwa, zablokowaniem jego dróg, mostów i węzłów komunikacyjnych, wykorzystaniem prywatnych organizacji o charakterze zbrojnym oraz grup złożonych z przeciwników ustroju społecznego i porządku politycznego kraju stanowiącego obiekt agresji,
- rozpoczęciem działań zbrojnych poprzedzonych akcją rozpoznawczą i wywiadowczą prowadzoną przy wykorzystaniu różnego rodzaju technologii i środków (operacje sił specjalnych, wywiad radioelektroniczny, użycie wywiadowczych i nawigacyjnych środków kosmicznych oraz środków rozpoznania osobowego),
- prowadzeniem działań zbrojnych we wspólnej przestrzeni informacyjnej, co gwarantuje jedną świadomość sytuacyjną,
- kierowaniem dużą ilością różnorodnych sił i środków w walce, m.in. dzięki wsparciu z kosmosu,
- przejęciem kontroli nad punktami oporu nieprzyjaciela i zniszczeniem ocalałych jednostek wroga przez użycie sił specjalnych, których zadanie polega na rozpoznaniu potencjału i zdolności bojowych przeciwnika, a następnie przekazaniu precyzyjnych danych dotyczących pozycji i położenia oddziałów nieprzyjaciela i znajdujących się w jego rękach obiektów infrastruktury krytycznej. Dzięki temu jest możliwe dokonanie uderzeń za pomocą broni precyzyjnego rażenia, co powoduje zniszczenie wszelkich miejsc oporu. Na ostatnim etapie następuje metodyczne pacyfikowanie wrogiego terytorium przez wojska lądowe i zajmowanie go[71].

Tak więc, analogicznie jak przed wiekami, głównym celem wojny prowadzonej środkami niemilitarnymi jest przygotowanie warunków do inwazji

[71] С.Г. Чекинов, С.А. Богданов, *О характере и содержании войны нового поколения*, „Военная мысль" 2013, nr 10, s. 13−25. Por. С.А. Богданов, *Асимметричные действия по обеспечению военной безопасности России*, „Военная мысль" 2010, nr 3, s. 13−22; С.Г. Чекинов, С.А. Богданов, *Влияние непрямых действий на характер современной войны*, „Военная мысль" 2011, nr 6, s. 3−13. Odnośnie do problematyki wzrostu znaczenia czynników technicznych we współczesnych wojnach z rosyjskiego punktu widzenia zob. И.М. Попов, *О долгосрочных характеристиках войн и вооружённых конфликтов*, w: *Некоторые аспекты анализа*…, s. 659−836.

zbrojnej. Potwierdza to przede wszystkim przebieg operacji mającej na celu opanowanie Półwyspu Krymskiego. Jej przeprowadzenie poprzedziły gruntowne działania o charakterze dywersyjno-wywiadowczym i dezinformacyjnym, co stanowi główny element powodzenia akcji prowadzonych w ramach „małej wojny" lub „wojny buntowniczej". Znajduje to odzwierciedlenie m.in. w opinii emerytowanego admirała Igora Kasatonowa, który przyznał, że (…) *Flota Czarnomorska przygotowała grunt, oficerowie wiedzieli, co się wokół dzieje, gdzie rozmieszczone są ukraińskie jednostki, a scenariusze wydarzeń były przerabiane na mapach*[72]. Igrzyska olimpijskie w Soczi skutecznie zaabsorbowały uwagę światowej opinii publicznej i dały Rosjanom możliwość umieszczenia jednostek wojskowych w pobliżu południowo-wschodniej granicy państwa ukraińskiego. Działanie to tłumaczono koniecznością zapewnienia bezpieczeństwa uczestnikom igrzysk, co nie wzbudziło żadnych podejrzeń. Wojska te wykorzystano do ochrony działań rosyjskich sił specjalnych na Krymie podczas inwazji. Rosjanie mieli dokładną wiedzę dotyczącą stanu osobowego jednostek wojsk ukraińskich, delegatur i placówek Służby Bezpieczeństwa Ukrainy (SBU) oraz ukraińskiej infrastruktury krytycznej. Wydaje się, że oprócz rozpoznania osobowego i elektronicznego prowadzili także tzw. wywiad psychologiczny, który polega na gromadzeniu, przetwarzaniu i analizowaniu informacji dotyczących stanu moralno-psychologicznego poszczególnych grup społecznych, wojska i personelu administracji. Działalności wywiadowczej prowadzonej przez Rosjan na Krymie niewątpliwie sprzyjało to, że siły zbrojne państwa ukraińskiego stanowiły relikt armii radzieckiej, z której wywodziły się ich kadry oraz z której czasów pochodziły sprzęt i systemy dowodzenia. Ponadto znaczną część korpusu oficerskiego ukraińskiej armii tworzyli absolwenci radzieckich uczelni wojskowych. Wielu żołnierzy sił specjalnych służących na Ukrainie po rozpadzie ZSRR wyjechało do Rosji. Infiltrację prowadzono także za pośrednictwem niewielkich grup wywiadowczo-dywersyjnych. Jedną z takich grup kierował Igor Striełkow vel Girkin (były żołnierz specnazu GRU lub też funkcjonariusz FSB, a nawet SBU)[73].

Nieprzypadkowo wybrano również czas przeprowadzenia operacji, w czym przejawia się akcentowana przez W. Bączkowskiego zdolność Rosjan (…) *do uchwycenia odpowiedniego momentu oraz świadomego tworzenia dogodnego dla siebie układu stosunków*[74]. Operację zrealizowano w okresie całkowitej destabilizacji i dezorganizacji państwa ukraińskiego, które spowodował przewrót w Kijowie. Nowe władze tworzono w pośpiechu i chaosie, społeczeństwo ukraińskie ulegało coraz intensywniejszej polaryzacji na tle politycznym i narodowościowym, do czego skutecznie przyczyniała się rosyjska wojna informacyjna[75]. W okresie od października 2013 r. do

[72] М. Перевозкина, *Адмирал Игорь Касатонов: «Конечно, это была наша армия»* [online], http://www.mk.ru/politics/2015/03/15/admiral-igor-kasatonov-konechno-eto-byla-nasha-armiya.html [dostęp: 1 IX 2015].

[73] M. Wrzosek, *Konflikt rosyjsko-ukraiński*…, s. 11−15; M. Wojnowski, *Aneksja Półwyspu Krymskiego w świetle teorii operacji specjalnych GRU*, „Secretum. Służby specjalne, bezpieczeństwo, informacja" 2014, nr 2, s. 106. Odnośnie do stanu armii ukraińskiej i jej uzależnienia od radzieckich wpływów zob. S. Denisentsev, *The Soviet Inheritance of Ukrainian Armed Forces*, w: *Brothers Armed: Military Aspects of the Crisis in Ukraine*, C. Howard, R. Pukhov (red.), London 2014, s. 25–57; A. Lavrov, A. Nikolsky, *Neglect and Rot: Degradation of Ukraine's Military in the Interim Period*, w: *Brothers Armed*…, s. 57−74; W. Parachomenko, *The State of Ukraine's Armed Forces and Military Reform*, „Journal of Slavic Military Studies" 2000, nr 13, s. 63−86.

[74] W. Bączkowski, *Uwagi o istocie siły rosyjskiej*…, s. 114.

[75] M. Wrzosek, *Konflikt rosyjsko-ukraiński*…, s. 14; M. Wojnowski, *Aneksja Półwyspu Krymskiego*…, s. 107.

lutego 2014 r. za pośrednictwem rosyjskich mediów prowadzono zakrojoną na szeroką skalę operację, która miała na celu zdyskredytowanie Euromajdanu, ukazując go jako bunt przeciwko legalnej władzy, inspirowany przez „trzecią siłę" z zewnątrz. Z kolei od lutego do marca 2014 r. prowadzono kampanię zmierzającą do zdemoralizowania władz cywilnych i wojskowych na Krymie oraz do rozpowszechnienia wśród światowej opinii publicznej historycznej, ale także prawnej, argumentacji uzasadniającej włączenie Krymu do Rosji[76].

Przygotowanie i zabezpieczenie informacyjne okazały się niezbędne nie tylko w kontekście operacji krymskiej, lecz także na dalszych etapach ekspansji rosyjskiej na terytorium Ukrainy. Obejmowały one następujące działania:

- skonfliktowanie grup narodowościowych i etnicznych wewnątrz państwa na podstawie tożsamości historycznej przez rozbudzanie i umacnianie sentymentów sowieckich przy jednoczesnym eksponowaniu znaczenia i roli radykalnych ugrupowań nacjonalistycznych („Prawy Sektor", „Swoboda"). Monopol rosyjskich środków masowego przekazu w krajach poradzieckich, w tym na Ukrainie, umożliwił stworzenie zamkniętego pola informacyjnego, dzięki czemu do świadomości społecznej docierała tylko i wyłącznie jednolita, stronnicza narracja rosyjska, w której ukazywano Ukrainę jako państwo słabe, upadłe i pozbawione sensu geopolitycznej egzystencji,
- wykorzystanie osoby obalonego prezydenta Wiktora Janukowycza do podważania legalności nowych władz ukraińskich i stworzenia alternatywnego, prorosyjskiego ośrodka władzy. W tym kontekście formułowano także narrację przekazu medialnego zawartą w stopniowaniu semantycznego znaczenia pojęć, od władz kijowskich poczynając, a na juncie kończąc,
- stosowanie wielu działań dezinformujących opinię publiczną, które prowadzono w prasie, radiu, telewizji i w internecie. Do najbardziej charakterystycznych należy zaliczyć przypadek tzw. doktora z Odessy[77] oraz historię mówiącą o tym, jakoby flagowy okręt ukraińskiej marynarki wojennej „Hetman Sahajdaczny" przeszedł na stronę rosyjską, wywieszając banderę z krzyżem św. Andrzeja,

[76] Е. Магда, *Гибридная война*…, s. 304–305; Б. Немцов, *Путин. Война. Независимый экспертный доклад*, И. Яшин, О. Шорина (red.), Москва 2015, s. 8–16; R. Allison, *Russian 'Deniable' Intervention in Ukraine: How and why Russia Broke the Rules*, „International Affairs" 2014, nr 90, s. 1258–1281; P. Pomerantsev, M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. A Special Report presented by The Interpreter, a project of the Institute of Modern Russia*, New York 2015, s. 14–24.

[77] Chodzi tu o posłużenie się przez rosyjską propagandę sfabrykowanym profilem lekarza Igora Rozowskiego, umieszczonym na portalu Facebook. Na profilu I. Rozowskiego pojawiła się informacja, jakoby „proukraińscy ekstremiści" mieli uniemożliwić mu udzielenie pomocy ludziom uwięzionym w płonących budynkach w Odessie. Rozowskij opisał także bestialstwa, których mieli się dopuścić ukraińscy bojownicy. Jego relacja zyskała ogromną popularność w rosyjskich mediach społecznościowych, została także przetłumaczona na języki angielski i niemiecki. Wkrótce jednak okazało się, że zdjęcie I. Rozowskiego umieszczone na profilu to w rzeczywistości zdjęcie innego lekarza – dentysty pochodzącego z Północnego Kaukazu. Profil ten okazał się zatem narzędziem trollingu, za którego pomocą rosyjska propaganda wywierała wpływ na emocje i poglądy zewnętrznego i wewnętrznego audytorium. Oprac. na podst.: *Analysis of Russia's Information Campaign against Ukraine. NATO Report*, Riga 2014, s. 27–28.

- masowe rozpowszechnianie w mediach zdjęć poległych żołnierzy ukraińskich, zniszczonego sprzętu wojskowego oraz śmierci cywilów, w celu zastraszenia i zniechęcenia obywateli Ukrainy do podejmowania służby wojskowej,
- eksponowanie w przekazie medialnym wszelkich napięć politycznych w Kijowie, sporów i konfliktów wewnątrz koalicji rządzącej, co miało spowodować podważenie zaufania do nowych władz,
- wykorzystanie kwestii dotyczącej dystrybucji gazu do uświadomienia państwom europejskim, że za wszelkie przyszłe problemy związane z przesyłem tego surowca będzie odpowiedzialna Ukraina. W tym kontekście było widoczne tworzenie na Zachodzie prorosyjskiego lobby znajdującego oparcie w partiach eurosceptycznych[78].

Opozycja, która przejęła władzę na Ukrainie, przez długie tygodnie nie wykazywała zainteresowania sytuacją ukraińskich jednostek stacjonujących na Krymie, które były niedofinansowane i niedozbrojone. Podważyło to zaufanie żołnierzy do cywilnego kierownictwa kraju. Ponadto dowództwo ukraińskich oddziałów stacjonujących na półwyspie nie otrzymało żadnych wytycznych, instrukcji ani rozkazów. Do działań mających na celu opanowanie Krymu przystąpiono w nocy z 27 na 28 lutego 2014 r. Grupa uzbrojonych mężczyzn wtargnęła do obiektów mieszczących miejscowy parlament oraz rząd Autonomicznej Republiki Krymu w Symferopolu i wywiesiła rosyjskie flagi państwowe. Incydent ten całkowicie zaskoczył siły ukraińskie, które w zaistniałej sytuacji nie zdobyły się na żadne przeciwdziałanie[79]. Nie można wykluczyć, że tę pierwszą grupę uderzeniową podającą się za tzw. Samoobronę Krymu tworzyli żołnierze i funkcjonariusze rosyjskich sił specjalnych. W tym kontekście nasuwa się bowiem analogia do przebiegu wstępnej fazy interwencji wojsk radzieckich w Afganistanie, gdzie 27 grudnia 1979 r. o godzinie 7.20 funkcjonariusze oddziału „Alfa", który podlegał 1. Zarządowi Głównemu KGB, ubrani w mundury afgańskiej armii wylądowali na lotnisku w Kabulu i dokonali zajęcia pałacu prezydenckiego[80]. W momencie rozpoczęcia operacji na Krymie siły ukraińskie i rosyjskie były mniej więcej wyrównane (ponad 14,5 tys. żołnierzy i marynarzy ukraińskich przeciwstawiono 15 tys. żołnierzy rosyjskich). W ostatnich dniach lutego przewaga strony rosyjskiej zaczęła się gwałtownie zwiększać. Przyczyniło się do tego tworzenie kolejnych oddziałów tzw. Samoobrony Krymu oraz przerzucanie rosyjskich jednostek wojskowych z terytorium FR, w czym decydującą rolę odgrywała Flota Czarnomorska. Rygorystyczne przestrzeganie ciszy radiowej uniemożliwiło zlokalizowanie ośrodków kierowniczych i węzłów informacyjnych Rosjan. Z pojazdów

[78] E. Магда, *Гибридная война*…, s. 295−304. Por. J. Szostek, J. Hutchings, *Dominant Narratives in Russian Political and Media Discourse during the Ukraine Crisis*, w: *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, R. Sakwa, A. Pikulicka-Wilczewska (red.), Bristol 2015, s. 183–197; E. Gaufman, *Memory, Media, and Securitization: Russian Media Framing of the Ukrainian Crisis*, „Journal of Soviet and Post-Soviet Politics and Society" 2015, nr 1, s. 141–175; J. Biersack, Sh. O'Lear, *The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy*, „Eurasian Geography and Economics" 2014, nr 55, s. 247–269.

[79] S.J. Cimbala, *Sun Tzu and Salami Tactics? Vladimir Putin and Military Persuasion in Ukraine, 21 February–18 March 2014*, „Journal of Slavic Military Studies" 2014, nr 27, s. 363–373; M. Wojnowski, *Aneksja Półwyspu Krymskiego*…, s. 107.

[80] M. Hassan Kakar, *Afghanistan. The Soviet Invasion and the Afghan Response, 1979–1982*, Berkeley 1995, s. 21–22.

rebeliantów poruszających się po terenie półwyspu zdjęto tablice rejestracyjne, z mundurów regularnych wojsk rosyjskich zaś usunięto wszelkie oznaki przynależności państwowej i organizacyjnej. Ponadto bojownicy tworzący formacje nieregularne dysponowali różnorodnym uzbrojeniem i umundurowaniem, co uniemożliwiło ich identyfikację[81].

Jak wykazano w niniejszym opracowaniu, autorzy koncepcji „małej wojny" i „wojny buntowniczej", a także współcześni rosyjscy wojskowi, szczególną wagę przywiązywali do wykorzystania „potencjału protestu" w kraju przeciwnika. Dlatego też nie może dziwić fakt, że wykorzystanie lokalnych partii i organizacji politycznych, inspirowanych, finansowanych i rozwijanych przez Kreml, było jednym z podstawowych elementów operacji krymskiej. W działaniach wzięła udział znaczna liczba tego rodzaju organizacji. Były to: „Wybór Ukrainy" pod przewodnictwem Wiktora Miedwiedczuka, Rosyjska Jedność Siergieja Aksionowa, ps. „Goblin", szefa lokalnej mafii (mimo iż jego partia cieszyła się niespełna czteroprocentowym poparciem, Aksionow został premierem samozwańczego rządu utworzonego w Symferopolu). W poczet tego typu organizacji należy zaliczyć działaczy Związku Kozaków Krymskich, Krymski Front, aktywistów Bloku Rosyjskiego, Narodowego Ruchu Wyzwolenia i Sojuszu Taurydy oraz Eurazjańskiego Związku Młodzieży pod przywództwem Pawła Kaniszczewa i Artura Dugina[82].

Głównym orężem stosowanym przez stronę rosyjską podczas operacji krymskiej były zarówno działania noszące znamiona dywersji ideologicznej, jak i środki tzw. zarządzania refleksyjnego (ros. *'рефлексивное управление', 'рефлексивный контроль'*). Pojęcie zarządzanie refleksyjne oznacza całokształt technik manipulacji i sterowania społecznego składający się z metod energetycznych (siła, przymus, presja, strach) i informacyjno-psychologicznych (propaganda, dezinformacja), których przygotowanie opiera się na stworzeniu specjalnego modelu przeciwnika imitującego jego zachowania[83]. Jako przykład tego rodzaju działań może posłużyć dezinformacja dotycząca przekazania 3 marca 2014 r. przez agencję Interfax-Ukraina, powołującej się na nieoficjalne źródło w ukraińskim ministerstwie obrony, wiadomości dotyczącej ultimatum wystosowanego przez dowództwo Floty Czarnomorskiej do oddziałów ukraińskich blokowanych na Krymie. Zgodnie z treścią tego ultimatum, gdyby do 4 marca 2014 r., do godz. 5.00, oddziały te nie skapitulowały, to wojska rosyjskie oraz rosyjscy i prorosyjscy bojownicy mieli przeprowadzić atak na wszystkie obiekty znajdujące

[81] M. Galeotti, *'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't*, w: *Ukraine and Russia*…, s. 156–165; Ch.K. Bartles, R. McDermott, *Russia's Military Operation in Crimea. Road – Testing Rapid Reaction Capabilities*, „Problems of Post-Communism" 2014, nr 61, s. 54–59; A. Lavrov, *Russian Again: The Military Operation for Crimea*, w: *Brothers Armed*…, s. 157–187. Por. А.М. Гольц, *Четвёртое взятие Крыма*, „Pro et Contra" 2014, nr 18, s. 45–56.

[82] Л. Слесарева, *Война нового типа* [online], http://psyfactor.org/news/crymwar2.htm [dostęp: 1 IX 2015]. Szczegółowy wykaz zidentyfikowanych organizacji, oddziałów najemnych i innych formacji zbrojnych biorących udział w walkach na Ukrainie po stronie rosyjskiej zawiera opracowanie: N. Mitrokhin, *Infiltration, Instruction, Invasion: Russia's War in the Donbass*, „Journal of Soviet and Post-Soviet Politics and Society" 2015, nr 1, s. 219–249. Por. K. Rękawek, *Neither "NATO's Foreign Legion" Nor the "Donbass International Brigades": (Where Are All the) Foreign Fighters in Ukraine?*, „PISM Policy Paper" 2015, nr 6, s. 1–12.

[83] С.А. Комов, *О способах и формах ведения информационной борьбы*, „Военная мысль" 1997, nr 4, s. 18−22; В.А. Лефевр, *Рефлексивное управление, моделирование и мораль. Доклад на международном симпозиуме «Рефлексивные процессы и управление»*, Москва 2000, w: *Рефлексия*, В.Е. Лепский (red.), Москва 2003, s. 454–455; T.L. Thomas, *Russia's Military Strategy in Ukraine: Indirect, Asymmetric and Putin – Led*, „Journal of Slavic Military Studies" 2015, nr 28, s. 456–458.

się w rękach Ukraińców. Informacja ta została przez stronę rosyjską zdementowana. Celem jej przekazania miało być prawdopodobnie wpłynięcie na stanowisko strony ukraińskiej na Radzie Bezpieczeństwa ONZ[84]. Podejmowano także próby dezintegracji i osłabienia morale ukraińskiej armii. Jednym z takich działań było mianowanie 24 marca 2014 r. na zastępcę dowódcy Floty Czarnomorskiej adm. Denisa Bierezowskiego, który opowiedział się po stronie Rosjan (doszło do tego 2 marca). W ten sposób dano czytelny sygnał wszystkim żołnierzom ukraińskim, że Federacja Rosyjska doceni zasługi każdego, kto przyczyni się do wsparcia jej działań na Krymie[85]. Ponadto wykorzystano to, że większość ukraińskich żołnierzy wraz z rodzinami mieszkała na Krymie. Dzięki temu znaczna ich część przeszła na stronę rosyjską lub zdezerterowała. Tylko 20 proc. ukraińskich żołnierzy zdecydowało się pozostać w siłach zbrojnych Ukrainy. W czasie operacji doszło do natychmiastowego tworzenia alternatywnego ośrodka władzy. Dnia 11 marca 2014 r. kontrolowany przez Moskwę krymski parlament ogłosił niepodległość Autonomicznej Republiki Krymskiej, a pięć dni później odbyło się „referendum". W jego wyniku nastąpiło przyłączenie półwyspu do Rosji. Dzień 16 marca 2014 r., w którym przeprowadzono referendum, można uznać za cezurę wyznaczającą koniec operacji[86].

Zakończenie

Scenariusz przebiegu operacji krymskiej został następnie powtórzony we wschodnich obwodach państwa ukraińskiego. Aneksja Półwyspu Krymskiego oraz kolejne etapy konfliktu stanowią potwierdzenie wykorzystania przez Rosję udoskonalonych i dopracowanych koncepcji „małej wojny" i „wojny buntowniczej". Rosjanie nie zaprezentowali tu żadnych nowatorskich rozwiązań. W ogromnej mierze stanowią one przykład prowadzenia działań na podstawie wspomnianych tu koncepcji. Istotnym novum jest natomiast zastosowanie nowoczesnej techniki zarówno w sferze walki informacyjnej, jak i w konwencjonalnych działaniach zbrojnych. Mimo to, główne założenia, mechanizmy i cele walki pozostały niezmienne. W związku z tym teorie o istnieniu nowej, charakterystycznej dla Rosji, koncepcji wojny hybrydowej należy uznać za niezgodne z rzeczywistością. Trzeba podkreślić, że teorie operacji hybrydowych oparte na jednolitym wzorcu trudno odnieść do rosyjskiej, elastycznej specyfiki prowadzenia działań wojennych. Na przykład interpretacja przebiegu operacji krymskiej i dalszych działań rosyjskich nie może być dokonywana bez pominięcia szczególnych uwarunkowań, w których dochodziło do realizacji tych przedsięzwzięć. Działania Rosjan na poziomie strategicznym, operacyjnym i taktycznym były uzależnione, i nadal są, od specyficznej sytuacji, w której znalazło się państwo ukraińskie, oraz od jego specyfiki kulturowej, etnicznej, politycznej i geograficznej. W związku z tym działania rosyjskie miały i mają charakter unikatowy – nie mogłyby być one zrealizowane w innych warunkach niż te, które Rosja stworzyła na Ukrainie. Były one pochodną gruntownej analizy

[84] M. Wrzosek, *Krym – polityczno-militarne aspekty konfliktu*, „Kwartalnik Bellona" 2014, s. 24; A. Wilk, *Rosyjska interwencja wojskowa na Krymie* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [dostęp: 1 IX 2015].

[85] M. Wojnowski, *Aneksja Półwyspu Krymskiego*…, s. 111.

[86] Р. Пухов, *Миф о «гибридной войне»*…, s. 1; J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, s. 23–24.

wywiadowczej wszelkich czynników, cech i uwarunkowań ukraińskiej państwowości. Inwazja zbrojna na Krym stanowiła natomiast podsumowanie poprzedzających ją przedsięwzięć.

Uwzględniając specyfikę rosyjskiej kultury strategicznej i myśli wojskowej wyrażonych w omówionych w niniejszym opracowaniu teorii i praktyce „małej wojny" i „wojny buntowniczej", należy podkreślić, że główną uwagę przywiązuje się w Rosji do działań prowadzonych w czasie poprzedzającym interwencję zbrojną. Przybierają one charakter niemilitarny i są uzależnione od wielu indywidualnych czynników decydujących o stanie danego państwa lub regionu. Próbując przewidzieć rosyjską logikę działania, należy przede wszystkim zwrócić uwagę na niedoskonałości i słabości własnej organizacji państwowej, specyfikę kulturową i etniczną kraju, stan elit przywódczych zarówno w wymiarze zbiorowym, jak i indywidualnym oraz na kwestie dotyczące mniejszości narodowych, tak wewnątrz państwa, jak i poza jego granicami. Pogłębionej analizy wymagają wszelkiego rodzaju negatywne tendencje i procesy zachodzące w państwie oraz ich źródła. Analiza tego rodzaju zagrożeń wymyka się jednolitym, schematycznym szablonom charakteryzującym koncepcje zagrożeń hybrydowych i wojen hybrydowych, stawiając przed kontrwywiadem ogromne wyzwania w postaci pozyskiwania, wyszkolenia i rozbudowywania kadry wysoko wykwalifikowanych ekspertów z różnych dziedzin wiedzy.

Warto także podkreślić, że rosyjskie rozumienie przyczyn, przebiegu oraz skutków konfliktów ma charakter geopolityczny, czyli przestrzenny. Oznacza to, że według Rosjan działania są prowadzone w przestrzeni geograficznej, ekonomicznej, informacyjno-cybernetycznej oraz informacyjno-psychologicznej danego państwa. Z punktu widzenia bezpieczeństwa Polski konieczne jest zatem stworzenie doktryny bezpieczeństwa informacyjnego RP, uwzględniającej rosyjską specyfikę działań. Stanowiłaby ona punkt odniesienia dla działalności legislacyjnej, precyzyjnie definiując zagrożenia i ich skutki. Państwo polskie nie dysponuje potencjałem materialnym, technologicznym i finansowym, aby przygotować symetryczną odpowiedź na rosyjskie formy oddziaływania informacyjnego. Pewną próbą udzielenia takiej odpowiedzi może być jednak prowadzenie szerokiej akcji informacyjnej i edukacyjnej w społeczeństwie oraz pogłębianie specjalistycznych studiów nad rosyjską myślą wojskową, strategią i historią rosyjskiej wojskowości, bez zamykania się tylko i wyłącznie w kręgu zachodniej sztuki wojennej.

Strategiczne scenariusze na najbliższe lata powinny zakładać zagrożenie nie tylko rosyjską agresją rozumianą tutaj wielowątkowo jako rozegranie polskiego „obszaru sworzniowego"[87] bez własnego zaangażowania bezpośredniego. Należy także

[87] Mianem sworznia geopolitycznego lub obszaru sworzniowego określa się państwa, których znaczenie nie wynika z ich potęgi czy ambicji, tylko raczej z ważnego położenia geograficznego i skutków ich potencjalnej niestabilności dla zachowań graczy geostrategicznych. To, które państwo pełni rolę sworznia geopolitycznego, wynika najczęściej z jego położenia geograficznego; niekiedy państwa te zyskują dzięki temu szczególną rolę, gdyż mogą umożliwiać ważnemu graczowi dostęp do istotnych obszarów lub też go blokować. W pewnych przypadkach sworzeń geopolityczny może stanowić tarczę obronną dla kluczowego państwa czy nawet regionu. Niekiedy samo istnienie sworznia geopolitycznego ma bardzo istotne konsekwencje polityczne i kulturalne dla jednego z sąsiadów, będącego bardziej aktywnym graczem geostrategicznym. Z tego względu głównym aspektem globalnej geostrategii Ameryki jest identyfikacja i ochrona państw, które w epoce po zakończeniu zimnej wojny pełnią rolę sworzni geopolitycznych. Oprac. na podst.: Z. Brzeziński, *Wielka Szachownica: główne cele polityki amerykańskiej*, tłum. T. Wyżyński, Warszawa 1998, s. 40–41 i 46–47; L. Moczulski, *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2010, s. 13–14; L. Sykulski, *Wojna hybrydowa z Ukrainą (zachodnią)?* [online], http://geopolityka.net/wojna-hybrydowa-z-

uwzględnić możliwą federalizację (rozpad) Ukrainy i związane z tym scenariusze rozwoju sytuacji. W dalszej perspektywie konieczne jest uwzględnienie ewentualności wystąpienia konfliktów na terytorium krajów bałtyckich i Mołdawii, przy pośrednim lub bezpośrednim zaangażowaniu Rosji, oraz konflikt polsko-białoruski.

ukraina-zachodnia/ [dostęp: 13 X 2015].

Łukasz Skoneczny

Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia

Nie ulega wątpliwości, że zjawisko wojny uległo w ciągu ostatnich kilkudziesięciu lat istotnym przeobrażeniom. Po pierwsze znacznie wzrosła liczba konfliktów wewnątrzpaństwowych. Po drugie coraz częściej w miejsce państwa pojawiają się różnego rodzaju podmioty o statusie pozapaństwowym. Po trzecie wreszcie nowo zaobserwowanym elementem współczesnych konfliktów zbrojnych jest rozmycie granicy pomiędzy żołnierzami a cywilami oraz stanem wojny a stanem pokoju[1].

Wśród głównych powodów wymienionych zmian analitycy wskazują na[2]:

- **zakończenie zimnej wojny** – w wyniku upadku ZSRR oraz rozwiązania Układu Warszawskiego oddaliło się ryzyko wybuchu globalnego konfliktu pomiędzy dwoma wrogimi blokami państwowymi, którego rezultatem mogła być wojna konwencjonalna lub nuklearna. Ponadto wraz ze zniknięciem rywalizacji między Wschodem i Zachodem zmniejszyła się liczba konfliktów zastępczych oraz wojen peryferyjnych inspirowanych przez oba te obozy. Negatywną stroną tego zjawiska jest natomiast brak „stabilizatora", który relatywnie przyczyniał się do umocnienia całego systemu międzynarodowego i zamrażał istniejące animozje na tle m.in. narodowościowym czy religijnym,
- **zakończenie procesu dekolonizacji i wojen postkolonialnych** – wiele konfliktów zbrojnych, do których dochodziło w drugiej połowie XX w., wybuchało na tle dążeń do uzyskania niezależności od dotychczasowych metropolii, a także toczyło się pomiędzy nowo powstałymi państwami np. o ustalenie granic,
- **militaryzację ludności cywilnej** – zjawisko to jest związane z utratą przez państwo monopolu na stosowanie przemocy. Skutkiem tego jest pojawienie się podmiotów pozapaństwowych będących stronami konfliktu. Często są to lokalne społeczności, które walczą o swoją tożsamość religijną, etniczną lub narodową. Przykładem tego zjawiska są np. konflikty w Somalii, Libii, konflikt izraelsko-palestyński i walki w Kosowie w 1999 r.

W tym kontekście pewne zaskoczenie musi wzbudzać fakt, że dopiero trwające walki na Ukrainie oraz wojna z tzw. Państwem Islamskim (dalej: IS – Islamic State[3]) wywołały – na niespotykaną dotychczas skalę – dyskusję, zwłaszcza wśród polityków oraz dziennikarzy, na temat natury obecnych konfliktów zbrojnych i zachodzącej w nich ewolucji. Szczególną popularność zyskał termin „wojna hybrydowa", który od momentu anektowania Półwyspu Krymskiego przez Rosję zaczął pojawiać się w wielu artykułach,

[1] Por. np. H. Welzer, *Wojny klimatyczne*, Warszawa 2010, s. 72–174; H. Münkler, *Wojny naszych czasów*, Kraków 2004, s. 97–153; K. Karolczak, *Terroryzm. Nowy paradygmat wojny w XXI wieku*, Warszawa 2010, s. 71–121.

[2] Szerzej zob. R. Łoś, J. Regina-Zacharski, *Współczesne konflikty zbrojne*, Warszawa 2010, s. 86–100.

[3] Ilekroć w artykule został użyty termin „Państwo Islamskie", autor odnosi się również do wcześniejszych postaci tej organizacji terrorystycznej: Islamskiego Państwa w Iraku (2006–2013) oraz Islamskiego Państwa w Iraku i Lewancie (2013–2014).

raportach oraz analizach związanych z problematyką bezpieczeństwa. Można odnieść wrażenie, że obecnie stanowi on słowo klucz, często nadużywane do opisu zjawisk znanych już od dawna. Mając na uwadze zamieszanie, jakie wywołuje nadmierne używanie tego terminu, należy spróbować udzielić odpowiedzi na następujące pytania: co rozumie się pod nazwą wojny hybrydowej, jakie są jej elementy charakterystyczne, czy jest to zjawisko jakościowo nowe oraz jakie warunki muszą zostać spełnione, aby można było zrealizować scenariusz wojny hybrydowej?

Wojna hybrydowa – ujęcie teoretyczne

Zgodnie z definicją h y b r y d a jest to *coś,* (...) *co składa się z różnych elementów, często do siebie niepasujących*[4]. W przypadku wojny hybrydowej chodziłoby więc – w dużym uproszczeniu – o taką aktywność jednej z walczących stron, która łączyłaby w sobie metody, formy oraz środki charakterystyczne dla różnorodnych działań militarnych i niemilitarnych.

Wbrew obiegowym opiniom, które pojawiły się w mass mediach, twórcami koncepcji „wojny hybrydowej" nie są Rosjanie, ale amerykańscy analitycy wojskowi. Miała być ona odpowiedzią na doświadczenia zdobyte przez armię Stanów Zjednoczonych w konfliktach w Afganistanie i Iraku oraz w tzw. wojnie z terroryzmem, a także próbą nowego podejścia teoretycznego, które będzie skuteczniej wyjaśniać otaczającą rzeczywistość[5].

Wojna hybrydowa według Williama J. Nemtha

Terminy „działania hybrydowe" oraz „wojna hybrydowa" pojawiły się już w 2002 r. w pracy mjr. Williama J. Nemetha *Future war and Chechnya: A case for hybrid warfare*[6]. Została ona poświęcona analizie konfliktu rosyjsko-czeczeńskiego. Autor zastosował w niej pojęcie h y b r y d o w o ś c i nie tylko w stosunku do działań prowadzonych przez czeczeńskich bojowników, lecz także do sposobu funkcjonowania tamtejszego społeczeństwa. Jedną z cech społeczeństwa hybrydowego jest połączenie nowoczesnych teorii politycznych z tradycyjną organizacją społeczną i obyczajowością[7]. Hybrydowy kształt danego społeczeństwa ma bezpośrednie przełożenie na sposób prowadzenia przez nie wojny. Według Nemetha wojna hybrydowa cechuje się m.in.[8]:

- **organizacją armii odzwierciedlającą poziom rozwoju społeczno-ekonomicznego danej wspólnoty oraz obowiązujące w niej normy** – społeczeństwo czeczeńskie jest zdecentralizowane, egalitarne i oparte na strukturze klanowej, dlatego w taki sam sposób byli zorganizowani bojownicy czeczeńscy w trakcie konfliktu z Rosją,
- **innym od zachodniego sposobem percepcji siły militarnej** – w przypadku „działań hybrydowych" ich siła ma polegać na masowym wykorzystaniu taktyk partyzanckich, które stwarzają poważne zagroże-

[4] *Wielki słownik wyrazów obcych PWN*, Warszawa 2008, s. 518.

[5] Por. np. A. Gruszczak, *Hybyrdowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, s. 11.

[6] W.J. Nemeth, *Future war and Chechnya: A case for hybrid warfare*, Monterey, CA 2002 [online], http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1 [dostęp: 2 IX 2015].

[7] Zob. tamże, s. 71.

[8] Zob. tamże, s. 73–76.

nie dla hierarchicznie zorganizowanych i wysoko zaawansowanych technologicznie oddziałów przeciwnika. Ponadto doświadczenia konfliktu rosyjsko-czeczeńskiego wskazują, że wojna hybrydowa jest prowadzona w sposób totalny, ponieważ jest traktowana jako narzędzie ochrony danej wspólnoty przed całkowitą zagładą. W związku z tym tego typu konflikt dopuszcza użycie wszelkich niezbędnych środków, w tym m.in. porwań oraz masowych mordów. Efektem działań hybrydowych jest także doprowadzenie do zatarcia się granicy między osobami zaangażowanymi w walki zbrojne a cywilami,

- **umiejętnością zastosowania nowoczesnych technologii w działaniach taktycznych oraz strategicznych** – w przypadku Czeczenów chodziło np. o wykorzystanie nowoczesnych technologii telekomunikacyjnych (m.in. telefonów komórkowych, telefonów satelitarnych) w celu zwiększenia efektywności dowodzenia, a także prowadzenia działań propagandowych (m.in. rozpuszczanie plotek o przejęciu broni masowego rażenia, która miałaby zostać użyta w jednym z rosyjskich miast, wykorzystanie znajomości języka rosyjskiego w celu dezinformowania oddziałów armii rosyjskiej). Posiadanie tych umiejętności oznacza również zdolność do innowacyjnego wykorzystania danej technologii w sposób, który nie był przewidziany przez jej twórców.

Od momentu opublikowania pracy Williama J. Nemetha pojęcie „wojny hybrydowej" było rozwijane przez innych teoretyków wojskowości. W dalszej części artykułu szczególną uwagę poświęcono koncepcjom amerykańskiego analityka Franka G. Hoffmana oraz aktualnego Szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej gen. Walerego Gierasimowa[9]. Wybór padł na koncepcje tych dwóch teoretyków wojskowości, ponieważ wydaje się, że są one najbardziej reprezentatywne dla omawianego zagadnienia oraz wywarły największy wpływ na środowisko analityczne.

Wojna hybrydowa według Franka G. Hoffmana

Rozważania Franka G. Hoffmana – byłego oficera armii amerykańskiej – na temat wojny hybrydowej zostały zaprezentowane w artykule *Conflict in the 21st century: Rise of the Hybrid Wars*[10]. Zespół Hoffmana z jednej strony przestudiował różne współczesne modele teoretyczne w celu zaproponowania nowego paradygmatu naukowego przyszłych wojen, z drugiej zaś postanowił zbadać przebieg historycznych konfliktów, po to, aby na ich przykładzie wyjaśnić potencjalne zagrożenia hybrydowe.

Analizie poddano teorię „wojen czwartej generacji", „wojen złożonych" (ang. '*compound wars*') oraz „wojny bez ograniczeń" (ang. '*unrestricted warfare*'). W przypadku „wojen czwartej generacji" zapożyczono twierdzenie o mieszanym charakterze przyszłych konfliktów zbrojnych (jednoczesne współistnienie stanu wojny i pokoju

[9] W celu zapoznania się z procesem ewolucji pojęcia „wojny hybrydowej" w amerykańskiej oraz rosyjskiej teorii wojskowej zob. np. A. Rácz, *Russia's Hybrid War in Ukraine – Breaking the Enemy's ability to resist*, Helsinki 2015 [online], http://www.fiia.fi/assets/publications/FIIAReport43.pdf, s. 27–47 [dostęp: 4 IX 2015].

[10] F.G. Hoffman, *Conflict in the 21st century: Rise of the Hybrid Wars*, Arlington 2007 [online], http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 28 VIII 2015]. Jest to wynik jego badań związanych z uczestnictwem w programie naukowym „Changing Character of Conflict", realizowanym przez Potomac Institute for Policy Studies.

oraz zanik granicy pomiędzy uczestnikami walk a cywilami) oraz utracie przez państwo monopolu na stosowanie przemocy – z czym jest związane pojawienie się podmiotów pozapaństwowych jako strony walczącej[11]. Z koncepcji „wojen złożonych" zaczerpnięto ideę synergicznego połączenia działań konwencjonalnych i nieregularnych na poziomie strategicznym, operacyjnym oraz taktycznym[12]. Ostatnią teorią przeanalizowaną przez Hoffmana i jego współpracowników była „wojna bez ograniczeń". W jej przypadku zwrócono uwagę m.in. na mieszczące się w jej ramach pojęcie wielokierunkowości (ang. *'omni-directionality'*) które zakłada, że w przyszłych konfliktach wszystkie sfery otaczającej nas rzeczywistości będą stanowiły jedno pole walki[13].

Na podstawie analizy wymienionych koncepcji, a także inspirując się lekturą Strategii Bezpieczeństwa Narodowego (*National Defence Strategy*) USA z 2005 r., zespół Hoffmana dokonał syntezy wskazanych elementów i zaproponował definicję wojny hybrydowej. Zgodnie z nią wojny hybrydowe zawierają w sobie zestaw różnych metod działań wojennych, wliczając w to działania konwencjonalne, nieregularne taktyki i ugrupowania zbrojne, akty terrorystyczne, w tym masową przemoc, oraz działania przestępcze[14].

Według Hoffmana konflikty hybrydowe mogą być prowadzone zarówno przez państwa, jak i podmioty pozapaństwowe. Ponadto operacje hybrydowe mogą być realizowane przez pojedyncze oddziały lub ich większe zgrupowania. Ich działania są koordynowane w ramach jednego, głównego pola walki, po to aby osiągnąć efekt synergii. Zwycięstwo w wojnie hybrydowej ma być osiągnięte przede wszystkim przez połączenie wykorzystania nowoczesnych technologii wojskowych z taktyką działań partyzanckich. Hoffman zwraca również uwagę na znaczenie aktywności przestępczej, która ma zwiększać chaos i proces rozkładu atakowanego państwa.

Kierując się opracowaną definicją, Hoffman i jego współpracownicy przestudiowali historyczne konflikty zbrojne, które mogłyby ilustrować wyzywania związane z wojną hybrydową. Badaniom zostały poddane: powstanie w Irlandii w latach 1919–1920, wojna w Afganistanie 1979–1989, a także konflikty na terenie byłej Jugosławii oraz na Bliskim Wschodzie. Ostatecznie uwagę skupiono na II wojnie w Libanie w 2006 r. pomiędzy armią izraelską a Hezbollahem. Konflikt ten został uznany za najlepszy przykład wojny hybrydowej. Przesądziły o tym jego następujące cechy[15]:

- zdolność podmiotu pozapaństwowego do rzucenia wyzwania militarnego zachodniemu modelowi prowadzenia działań zbrojnych,
- sposób koordynowania operacji zdecentralizowanych komórek bojowych przez kierownictwo Hezbollahu,
- wysoki poziom przeszkolenia wojskowego oddziałów Hezbollahu,
- wykorzystanie przez oddziały Hezbollahu obszarów miejskich do unikania ich wykrycia oraz organizowania zasadzek,
- zdolność obsługi przez bojowników Hezbollahu nowoczesnego sprzętu wojskowego, w tym rakietowych pocisków przeciwokrętowych oraz przeciwpancernych,
- umiejętność wtapiania się żołnierzy Hezbollahu w ludność cywilną,

[11] Tamże, s. 18–19.
[12] Tamże, s. 20–22.
[13] Tamże, s. 22–25.
[14] Tamże, s. 29.
[15] Tamże, s. 35–42.

- prowadzenie przez Hezbollah działań informacyjno-wywiadowczych realizowanych na poziomie strategicznym oraz operacyjnym (np. wykorzystanie nowoczesnego sprzętu do podsłuchiwania rozmów izraelskich żołnierzy prowadzonych przez telefony komórkowe).

Wojna hybrydowa według gen. Walerego Gierasimowa

Ewolucja współczesnych konfliktów zbrojnych jest przedmiotem zainteresowania również rosyjskich teoretyków wojskowości. W tym miejscu zostanie zaprezentowana koncepcja gen. Walerego Gierasimowa. Za wyborem tym przemawiają dwa powody. Po pierwsze Gierasimow jest aktualnym Szefem Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej i jego poglądy obrazują sposób myślenia o wojnie wśród najwyższych decydentów polityczno-wojskowych w Rosji. Po drugie przebieg konfliktu na Ukrainie jest najlepszym przykładem, jak doktryna Gierasimowa została zastosowana w praktyce.

Należy zauważyć, że Gierasimow w swoim artykule *Ценность науки в предвидении*[16] (*Znaczenie nauki w przewidywaniu*) ani razu nie używa pojęcia „wojna hybrydowa". Analizując jednak wskazane przez niego kierunki ewolucji przyszłych wojen, nie można mieć żadnych wątpliwości, że mówi on o elementach charakterystycznych dla tego zjawiska.

Gierasimow stwierdza, że w XXI w. będzie można zaobserwować tendencję do zanikania granic między stanem wojny i pokoju. Wojny nie będą – tak jak dotychczas – poprzedzane formalnym aktem ich wypowiedzenia. Będą przebiegały według nieznanego wcześniej schematu. Jako przykład nowego rodzaju konfliktów Gierasimow wskazuje na wydarzenia w Afryce Północnej oraz na Bliskim Wschodzie określane mianem „arabskiej wiosny". Gierasimow stawia dwa zasadnicze pytania: co oznacza „nowoczesna wojna" i jak armia powinna się do niej przygotowywać?

W jego ocenie zmieniły się „zasady prowadzenia wojny". Najważniejszego znaczenia nabrały niemilitarne środki działań wojennych. Coraz istotniejsze jest wykorzystanie różnorodnych instrumentów politycznych, ekonomicznych i humanitarnych w połączeniu z manipulowaniem nastrojami ludności zamieszkującej teren konfliktu. Działania te są wspierane przez środki militarne, szczególnie o charakterze wojny informacyjnej oraz operacji jednostek specjalnych. Otwarte wykorzystanie oddziałów zbrojnych – najczęściej pod postacią misji pokojowych oraz humanitarnych – jest dopuszczalne dopiero w późniejszej fazie konfliktu, po to aby przypieczętować ostateczny sukces.

Według Gierasimowa rozwój technologii informacyjnych pozwolił na znaczne usprawnienie procesu komunikacji pomiędzy operującymi siłami zbrojnymi a ich dowództwem. Nowoczesna przestrzeń informacyjna może być wykorzystana także do niwelowania potencjału bojowego przeciwnika. Gierasimow podaje tutaj przykład państw Afryki Północnej, w których internetowe sieci społecznościowe posłużyły do mobilizowania miejscowej ludności oraz wpływania na organy władzy.

W doktrynie Gierasimowa duży nacisk kładzie się także na działania asymetryczne, w tym szczególnie na wykorzystanie jednostek specjalnych oraz wewnętrznej

[16] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер" z 27 II 2013 r., [online], http://www.vpk-news.ru/articles/14632, tłumaczenie na język angielski, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ [dostęp: 31 VIII 2015].

opozycji politycznej w celu objęcia konfliktem całego wrogiego obszaru. Szczególną rolę mają do odegrania mobilne, mieszane oddziały bojowe, które nie będą się angażowały we frontalne walki z przeciwnikiem. Gierasimow ponadto uważa, że obecnie zacierają się różnice między strategicznym, operacyjnym oraz taktycznym poziomem działania, a także między operacjami ofensywnymi i defensywnymi.

Koncepcja Hoffmana i Gierasimowa – wnioski

Już na pierwszy rzut oka widać, że opisane koncepcje mają zarówno wiele elementów wspólnych, jak i różnych. Tak Hoffman, jak i Gierasimow podkreślają zmiany, jakie zachodzą w sposobie kierowania współczesnymi konfliktami zbrojnymi: decentralizację struktur dowodzenia, połączenie strategicznej, operacyjnej i taktycznej sfery działań oraz istotnego wzrostu znaczenia niemilitarnych środków prowadzenia wojny.

Obydwaj autorzy wskazują także na coraz większą rolę, jaką odgrywają nieregularne formy prowadzenia operacji wojennych. Chodzi tu zwłaszcza o wykorzystanie metod wojny partyzanckiej i małych oddziałów bojowych. Zgadzają się również co do tego, że w przyszłych konfliktach zbrojnych nie będzie jasnego podziału na stan wojny i pokoju oraz żołnierzy i cywilów.

Jeżeli chodzi o różnice, to można odnieść wrażenie, że Hoffman, stosując pojęcie „wojny hybrydowej". Skupia się przede wszystkim na taktyce działania jednostek bojowych. Mniej uwagi poświęca natomiast niemilitarnym środkom prowadzenia konfliktu hybrydowego, w przeciwieństwie do Gierasimowa, który przykłada do nich dużą wagę. Ponadto rosyjski wojskowy w swojej analizie podkreśla znaczenie wymiaru strategicznego przyszłych konfliktów. Dostrzega np. konieczność wykorzystania działań propagandowych – w tym nowoczesnych technologii informacyjnych – nie tylko w celu dezinformowania oddziałów wroga lub prowadzenia operacji wywiadowczych, lecz także zdobycia przychylności ludności zamieszkującej obszar konfliktu czy manipulowania jej nastrojami. Przebieg konfliktu na Ukrainie oraz wojna z IS pokazują, że może to być jeden z głównych czynników odróżniających wojny hybrydowe od wcześniejszych konfliktów zbrojnych.

Wojna hybrydowa – konflikt na Ukrainie oraz wojna z Państwem Islamskim

Historycy wojskowości są zgodni co do tego, że już w przeszłości istniały konflikty, które zawierały w sobie wiele elementów hybrydowych[17]. Obecnie pojęcie to pojawia się najczęściej w związku z trwającymi walkami na Ukrainie. Nie można jednak zapominać o działaniach prowadzonych przez IS, które także wykazują tego rodzaju cechy. W związku z tym zostanie podjęta próba opisu modelu współczesnej wojny hybrydowej na podstawie porównania konfliktów na Ukrainie i Bliskim Wschodzie, ich różnic i podobieństw. W dalszej części natomiast zostaną przeanalizowane czynniki, które umożliwiają jej skuteczne zastosowanie przez jedną z walczących stron.

[17] Zob. np. *Hybrid warfare: Fighting Complex Opponents from the Ancient World to the Present*, W. Murray, P.R. Mansoor (red.), Cambridge 2012.

Konflikt ukraiński oraz wojna z Państwem Islamskim – dwa modele wojny hybrydowej

Sytuacja na Ukrainie oraz na Bliskim Wschodzie jest interesująca z analitycznego punktu widzenia, ponieważ można tam zaobserwować tak naprawdę dwa modele wojny hybrydowej. W przypadku konfliktu ukraińskiego są to działania realizowane przez państwo (Rosja). Na terenie Syrii oraz Iraku jest natomiast odnotowywana aktywność organizacji terrorystycznej, jaką jest IS. Wydaje się, że porównanie poszczególnych elementów tych dwóch modeli ma zasadnicze znaczenie dla zrozumienia, jakie cechy charakterystyczne mają współczesne wojny hybrydowe.

Cele wojny hybrydowej

W obydwu konfliktach działania hybrydowe są realizowane z różnych pobudek. W przypadku Rosji chodziło o zdestabilizowanie państwa ukraińskiego bez wszczynania otwartej wojny, po to aby w perspektywie długofalowej zablokować integrację tego kraju z UE i NATO. Zamiarem IS jest natomiast zniszczenie Syrii oraz Iraku w celu stworzenia podwalin pod budowę globalnego kalifatu. Państwo Islamskie zdecydowało się na zastosowanie strategii hybrydowej, ponieważ nie miało – przynajmniej do zajęcia Mosulu w czerwcu 2014 r. – wystarczającej siły militarnej, ekonomicznej i politycznej, aby móc prowadzić konwencjonalne działania zbrojne na dużą skalę.

Z punktu widzenia bezpieczeństwa RP szczególnie istotny jest „model ukraiński" ze względu na problem tzw. agresji poniżej progu wojny. Wydarzenia na Ukrainie uświadomiły bowiem, że wojna hybrydowa może zostać wykorzystana przez jedną ze stron konfliktu do celowego ograniczania skali prowadzonych operacji zbrojnych, po to aby uniemożliwić określenie w sposób jednoznaczny stanu wojny oraz agresora, a tym samym zapobiec reakcji społeczności międzynarodowej.

Kwestia ta jest ważna, ponieważ może mieć w przyszłości wpływ na udzielenie pomocy sojuszniczej jednemu z państw członkowskich NATO. Zgodnie bowiem z art. 5 Traktatu Północnoatlantyckiego państwa NATO są zobowiązane do udzielenia sobie wzajemnej pomocy tylko w przypadku zbrojnej napaści na jedno z nich. Charakter działań w ramach wojny hybrydowej, ich niejednoznaczność, wzajemne przenikanie się stanu wojny i pokoju powodują, że w tej sprawie mogą wystąpić poważne wątpliwości prawne związane z tym, co należy rozumieć pod pojęciem „zbrojna napaść", czy są to wyłącznie otwarte działania zbrojne? Czy może ze zbrojną napaścią mamy do czynienia już w momencie aktywności tzw. zielonych ludzików?

Militarne metody prowadzenia wojny hybrydowej

Analiza militarnych metod prowadzenia działań hybrydowych przez oddziały prorosyjskich separatystów oraz przez IS wskazuje, że w obydwu przypadkach są one do siebie podobne. Wśród nich można wyróżnić:

- konwencjonalne działania zbrojne,
- działania nieregularne,
- akty terroryzmu.

Działania te są wykorzystywane na różnych etapach omawianych konfliktów i z różną intensywnością. W przypadku wydarzeń na Ukrainie można wyróżnić dotychczas dwie fazy: aneksję Półwyspu Krymskiego przez Rosję oraz walki na południowo-wschodniej Ukrainie. W pierwszym przypadku obserwowano działania nieregularne polegające na wykorzystaniu na dużą skalę funkcjonariuszy rosyjskich służb specjalnych oraz żołnierzy jednostek specjalnych SPECNAZ, pod postacią „lokalnych oddziałów samoobrony", których zadanie polegało na inspirowaniu niezadowolenia miejscowej ludności, manipulowaniu nią, a na końcowych etapach całej operacji – na przejmowaniu kontroli i zabezpieczaniu budynków administracji rządowej, infrastruktury krytycznej oraz jednostek wojskowych. W drugiej fazie – destabilizacji południowo-wschodniej Ukrainy – przeważały konwencjonalne działania zbrojne, podczas których wykorzystywano nowoczesny sprzęt wojskowy (czołgi, ciężką artylerię, broń przeciwlotniczą). Były one prowadzone przez oddziały prorosyjskich separatystów, „ochotników" rosyjskich oraz najemników z innych państw. W tej fazie konfliktu dochodziło również do działań terrorystycznych, m.in. porwań członków misji OBWE w kwietniu i maju 2014 r., porwań ukraińskich działaczy politycznych i społecznych lojalnych wobec Kijowa[18], używania ludności cywilnej jako żywych tarcz[19], zestrzelenia 17 lipca 2014 r. samolotu pasażerskiego malezyjskich linii lotniczych.

Z kolei w działaniach prowadzonych przez IS na terytorium Syrii oraz Iraku można obecnie wyróżnić trzy takie fazy. Pierwsza – obejmująca okres, gdy organizacja ta została niemal rozbita, czyli od grudnia 2008 r. do grudnia 2011 r. – polegała na prowadzeniu operacji nieregularnych wobec wojsk amerykańskich oraz irackich, głównie z zastosowaniem działań asymetrycznych, zwłaszcza zamachów bombowych. Następnie – po wycofaniu oddziałów Stanów Zjednoczonych z Iraku w grudniu 2011 r. – IS zorganizowało w latach 2012–2013 kampanię terroru wymierzoną w ludność cywilną, przede wszystkim wyznania szyickiego, aby wykazać bezradność irackich władz oraz wzniecić walki na tle religijnym. Ostatnia faza – od 2014 r. do dziś – to stosowanie przede wszystkim działań konwencjonalnych. Są one prowadzone za pomocą sprzętu oraz broni zdobytej w irackich i syryjskich bazach wojskowych.

W ramach militarnych metod prowadzenia wojny hybrydowej należy wspomnieć również o dużej roli, jaką odgrywa w nich „taktyka zastraszania" przeciwnika. Jako przykład takich działań można podać zachowanie Rosjan. Chodzi tu m.in. o rozlokowanie jednostek armii rosyjskiej blisko granicy z Ukrainą, organizowanie na wielką skalę ćwiczeń i manewrów wojskowych, niezapowiedziane alarmy bojowe, prowokacje w postaci lotów patrolowych rosyjskich myśliwców oraz bombowców naruszających przestrzeń powietrzną państw NATO. Wymienione działania mają służyć wywieraniu ciągłej presji militarnej na Ukrainę oraz UE w celu osłabienia ich woli walki i złagodzenia stanowiska przed podjęciem ewentualnych negocjacji.

[18] Zob. np. http://www.tvp.info/15992964/bicie-porwania-tortury-raport-amnesty-international-o-wschodzie-ukrainy [dostęp: 8 IX 2015].

[19] Zob. np. http://niezalezna.pl/54820-zywe-tarcze-na-ukrainskiej-wojnie-taktyka-putina-realizuje-sie-w-slowiansku [dostęp: 8 IX 2015].

Niemilitarne metody prowadzenia wojny hybrydowej

Działania niemilitarne wykorzystywane w ramach konfliktów hybrydowych mają na celu głównie oddziaływanie na ludność cywilną oraz społeczność międzynarodową. Ich zadaniem jest osłabianie woli oporu, zwiększanie poziomu zniechęcenia oraz niezadowolenia społecznego, co w rezultacie ma doprowadzić do zakończenia konfliktu zgodnie z interesem agresora.

Przykładem skutecznie zastosowanych działań niemilitarnych w wojnie hybrydowej jest przebieg konfliktu na Ukrainie. Jest to związane z dużym potencjałem politycznym i ekonomicznym Rosji, która może stosować wieletakich działań. Natomiast IS próbuje dopiero budować quasi-państwowe struktury na zdobytych terytoriach, w związku z czym na obecnym etapie ma minimalne możliwości wykorzystania tych środków.

Analiza wydarzeń na Ukrainie wskazuje, że wśród niemilitarnych metod prowadzenia wojny hybrydowej można wymienić:

- **presję ekonomiczną** – może ona polegać na wprowadzeniu embarga lub wysokich ceł na produkty importowane z państwa, wobec którego są prowadzone działania hybrydowe, lub z krajów udzielających mu wsparcia. Mogą to być również groźby odcięcia dostaw surowców strategicznych,
- **dużą aktywność służb specjalnych** – ich zadaniem jest gromadzenie informacji oraz budowa siatek wywiadowczo-sabotażowych realizujących działania na terytorium atakowanego państwa,
- **działania ofensywne w cyberprzestrzeni** – prowadzone przez służby specjalne agresora lub powiązane z nimi grupy hakerów oraz haktywistów, których celem jest paraliżowanie funkcjonowania państwa atakowanego (jego administracji, infrastruktury krytycznej itd.),
- **wielokierunkowe działania dyplomatyczne** – polegające na dyskredytowaniu wizerunku państwa atakowanego oraz budowaniu politycznego lobby w organizacjach międzynarodowych w celu uniemożliwienia reakcji z ich strony lub łagodzenia wprowadzanych przez nie sankcji ekonomicznych i politycznych.

Działania propagandowo-informacyjne w wojnie hybrydowej

Trwające na Ukrainie oraz Bliskim Wschodzie konflikty hybrydowe pokazały również, jak ważną rolę odgrywa w nich umiejętnie zorganizowana propaganda. Możliwości tkwiące we właściwym wykorzystaniu informacji potwierdził w pełni przypadek Ukrainy – zwłaszcza sposób, w jaki Rosjanie dokonali aneksji Półwyspu Krymskiego. Zastosowane przez nich działania informacyjno-propagandowe miały na celu (...) *podporządkowanie elit i społeczeństw innych państw w sposób niezauważalny, przy wykorzystaniu różnych tajnych i jawnych kanałów (służb specjalnych, dyplomatycznych, medialnych)*, *oddziaływania psychologicznego, dywersji ideologicznej i politycznej*[20]. Chociaż tego rodzaju przedsięwzięcia były podejmowane także we wcześniejszych konfliktach zbrojnych, to skala zrealizowania ich na Ukrainie świadczy o tym, że będą one odgrywały coraz większą rolę w przyszłości.

[20] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, s. 5.

Za pionierów nowoczesnych działań propagandowo-informacyjnych należy uznać Rosjan. Stworzyli oni bowiem hierarchicznie zorganizowany system organów państwowych, instytucji naukowych oraz powiązanych z nimi mediów, który jest odpowiedzialny za wypracowywanie strategii, prowadzenie działań w zakresie walki informacyjnej i ich koordynowanie. Jego zadaniem jest zarówno kształtowanie oraz manipulowanie poglądami rosyjskiego społeczeństwa, jak i oddziaływanie na społeczność międzynarodową zgodnie z interesem Moskwy.

Celem rosyjskich działań propagandowo-informacyjnych w związku z konfliktem ukraińskim jest: budowa pozytywnego wizerunku Rosji, podkreślanie znaczenia tego państwa dla stabilności systemu międzynarodowego i jego bezpieczeństwa, osłabianie solidarności państw członkowskich NATO oraz UE, wytworzenie w społeczeństwie rosyjskim poczucia „oblężonej twierdzy" i zagrożenia ze strony państw zachodnich. Do realizacji wymienionych zadań są wykorzystywane oficjalne media, m.in. RIA Novosti, Russia Today, Voice of Russia, Agencja REX czy Agencja Informacyjna Regnum. Często korzystają one z agentury wpływu, w tym posługują się opracowaniami oraz wypowiedziami zagranicznych dziennikarzy, polityków i naukowców, które zawierają oceny wydarzeń na Ukrainie zbieżne z polityką Moskwy. Do działań propagandowo-informacyjnych są angażowani także przedstawiciele rosyjskich placówek dyplomatycznych oraz współpracujące z nimi podmioty, których zadaniem jest promowanie interesów Rosji poza granicami kraju.

W przypadku IS mamy do czynienia z dużo mniejszym poziomem instytucjonalizacji walki informacyjnej, chociaż jej skala jest podobna. Wykorzystywane są do tego najnowocześniejsze zdobycze technologiczne. Państwo Islamskie ma na celu z jednej strony dotarcie do radykalnych wyznawców islamu w innych państwach, zwłaszcza europejskich, oraz ich aktywizację, a z drugiej mobilizację oraz konsolidację bojowników biorących udział w walkach na terenie Syrii i Iraku. Głównym polem działań propagandowo-informacyjnych islamskiej organizacji jest sieć internetowa, w tym szczególnie portale społecznościowe oraz platformy hostingowe. Państwo Islamskie umieszcza na nich m.in.:

- filmy instruktażowe dotyczące konstruowania bomb, rakiet, obsługi broni itd.,
- materiały propagandowe zawierające groźby ataków terrorystycznych, zachęcające do uczestnictwa w walkach na Bliskim Wschodzie po stronie IS, wzywające do przeprowadzenia indywidualnych zamachów terrorystycznych, pokazujące egzekucje na „niewiernych" itp.,
- e-magazyny – czasopisma skierowane do odbiorców w państwach zachodnich, Rosji oraz Turcji. Zawierają one treści ekstremistyczne, religijne, opisują warunki życia na terenach zajętych przez IS, co ma stanowić zachętę do przyjazdu dla innych radykalnych wyznawców islamu.

Czynniki warunkujące skuteczne zastosowanie wojny hybrydowej

Kolejne pytanie, które pojawia się w związku z wojną hybrydową, dotyczy warunków, jakie muszą zostać spełnione, aby można ją było efektywnie prowadzić. Do odpowiedzi na nie zostanie wykorzystana analiza wydarzeń na Ukrainie, w Syrii oraz

Iraku oraz wyniki rozważań Andrása Rácza[21], który zajmował się tą problematyką w kontekście rosyjskiej wojny hybrydowej.

Pierwszym warunkiem, który musi zostać spełniony, jest **poważny kryzys w państwie** będącym celem ataku. Przykład Ukrainy, Syrii i Iraku pokazuje, że skuteczne zastosowanie działań hybrydowych jest możliwe tylko wtedy, gdy państwo atakowane nie jest zdolne do pełnienia swoich podstawowych funkcji lub ma poważne trudności z ich pełnieniem, gdy jego władzom brakuje legitymizacji, a społeczeństwo jest skonfliktowane i podzielone. Wśród cech szczegółowych można wskazań na:

- złe funkcjonowanie administracji państwowej, wojska oraz służb bezpieczeństwa (Ukraina, Syria, Irak) oraz wysoki poziom korupcji w tych instytucjach,
- istnienie silnych grup interesów, które realizują swoje partykularne cele, osłabiając tym samym politykę prowadzoną przez władze centralne i integralność całego państwa (Ukraina, Irak),
- duży poziom niezadowolenia z władz państwowych. U jego podstaw może leżeć konflikt na tle politycznym (Ukraina, Syria), etnicznym (Ukraina, Irak) lub religijnym (Irak).

Kolejnym warunkiem koniecznym do skutecznego prowadzenia wojny hybrydowej jest **istnienie na terenie państwa atakowanego mniejszości narodowych lub religijnych, które stanowią znaczną część społeczeństwa i utożsamiają się z agresorem**. Wykorzystując resentymenty, agresor zyskuje możliwość manipulowania ich działaniami, angażowania ich w prowadzone operacje wojskowe i wywiadowcze, a w skrajnych przypadkach inspirowania ruchów separatystycznych, radykalnych oraz ekstremistycznych. Tezę tę potwierdzają zarówno wydarzenia na Ukrainie (referendum w sprawie przyłączenia Krymu do Rosji, utworzenie tzw. Donieckiej Republiki Ludowej oraz tzw. Ługańskiej Republiki Ludowej), jak i w Syrii oraz Iraku (wykorzystywanie przez IS odwołań do religii w celu zdobycia poparcia ludności sunnickiej zamieszkującej te państwa).

Jednym z najważniejszych czynników jest również **możliwość dotarcia z przekazem propagandowym do społeczeństwa państwa atakowanego**. Nie można bowiem zapominać, że jednym z najważniejszych celów współczesnych wojen hybrydowych jest wygranie bitwy w umyśle przeciwnika. Aby to osiągnąć, konieczne jest istnienie wolnego rynku mediów, na którym silną pozycję ma agresor (Ukraina) lub taki poziom dostępności do nowoczesnych technologii telekomunikacyjnych wśród ludności państwa atakowanego, który umożliwi powszechne zapoznawanie się z materiałami propagandowo-informacyjnymi zamieszczanymi na portalach społecznościowych, stronach internetowych czy platformach hostingowych (Irak, Syria).

Reasumując doświadczenia zdobyte podczas konfliktu na Ukrainie, w Syrii i Iraku, można założyć**,** że prowadzenie wojny hybrydowej jest dopuszczalne tylko wtedy, kiedy opisane warunki występują jednocześnie. W przeciwnym razie okazałaby się ona prawdopodobnie nieskuteczna.

[21] Por. A. Rácz, *Russia's Hybrid War*…, s. 73–83. Stworzył on katalog warunków, jakie muszą zostać spełnione, aby Rosja mogła skutecznie zastosować działania hybrydowe w prowadzonym przez siebie konflikcie zbrojnym.

Podsumowanie

Wojny hybrydowe nie są zjawiskiem nowym. Z wieloma ich elementami świat miał już do czynienia w przeszłości. Wydarzania na Ukrainie oraz na Bliskim Wschodzie pokazują jednak ewolucję zachodzącą w dotychczasowym sposobie prowadzenia konfliktów. W przyszłości strategia wojny hybrydowej będzie prawdopodobnie wykorzystywana przez podmioty, które nie chcą stosować konwencjonalnych działań zbrojnych ze względu na brak odpowiednich środków i potencjału bądź grożące im skutki poniesienia odpowiedzialności za otwarte wywołanie konfliktu. Wojna hybrydowa może być przez nie postrzegana jako równie skuteczna metoda osiągania zamierzonych celów, przy jednocześnie zdecydowanie mniejszych kosztach politycznych, ekonomicznych, militarnych i wizerunkowych, które musiałaby te podmioty ponieść.

Analiza warunków, które pozwalają na efektywne prowadzenie wojny hybrydowej, pokazała, że są na nią narażone przede wszystkim państwa pogrążone w głębokim kryzysie, których społeczeństwo jest podzielone i skonfliktowane na tle politycznym, etnicznym lub religijnym. W tym świetle należy uznać za przesadzone obawy państw UE, które wyrażają zaniepokojenie powtórzeniem scenariusza ukraińskiego na swoim terytorium. Oczywiście nie można wykluczyć zastosowania przez Rosję wobec nich któregoś z elementów wojny hybrydowej. Należy jednak pamiętać, że wtedy ma się do czynienia nie z konfliktem hybrydowym, ale – w zależności od użytych środków – z wojną informacyjną, działalnością dywersyjno-sabotażową czy wojną handlową. Aby mówić o wojnie hybrydowej, musi zostać spełniony jeden ważny warunek, na który zwracał uwagę zarówno Hoffman, jak i Gierasimow. Chodzi tu o jednoczesne użycie środków militarnych, niemilitarnych oraz propagandowych na poziomie strategicznym, operacyjnym i taktycznym prowadzonego konfliktu.

Kwestie poruszone w artykule nie wyczerpują tematu wojny hybrydowej. Mogą jednak posłużyć za wprowadzenie do tej problematyki i stanowić punkt wyjścia do dalszych analiz w tym zakresie. Warto też zwrócić uwagę na następujące pytania: jak w warunkach państwa demokratycznego reagować na zagrożenia wojny hybrydowej? Czy państwo demokratyczne jest zdolne do skutecznego przeciwdziałania wojnie informacyjnej, np. w wydaniu rosyjskim? Jaki – w perspektywie długofalowej – wpływ na możliwość prowadzenia działań hybrydowych przez IS będzie miał napływ ludności muzułmańskiej do państw europejskich?

Krzysztof Liedel

Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?

Dynamika zmian w polskim środowisku bezpieczeństwa znacznie wzrasta w ostatnich latach. Wśród najważniejszych przyczyn takiego stanu rzeczy należy wymienić między innymi wyczerpującą się „premię bezpieczeństwa" wynikającą z zakończenia przed ćwierćwieczem zimnej wojny. W ciągu ostatnich 25 lat panowało bowiem przekonanie, że po zakończeniu napięć międzyblokowych ostatecznie odsunięto zagrożenie konfliktem militarnym na wielką skalę. Miało to przynieść ustabilizowanie się środowiska międzynarodowego w stopniu, który pozwoli na realną międzynarodową współpracę dla rozwoju, zamiast powtarzającego się w historii cyklu rywalizacji i konfliktów. Jako istotny czynnik wpływający na zmiany w polskim środowisku bezpieczeństwa trzeba ponadto wskazać pojawienie się nowych strategii i taktyk działania w przestrzeni międzynarodowej stosowanych przez aktorów działających w tym regionie.

Od 15 lat jesteśmy świadkami zmiany percepcji międzynarodowych zagrożeń bezpieczeństwa. W latach 90. XX w. panowało przekonanie, że doświadczenia II wojny światowej i zimnej wojny w dużym stopniu wyeliminowały zagrożenie klasycznym konfliktem o charakterze militarnym. Według niektórych badaczy miał nawet nastąpić „koniec historii"[1]. Był to okres zmian w środowisku międzynarodowym. Podjęto wówczas dyskusję na temat konieczności reformy Sojuszu Północnoatlantyckiego, który należało dostosować do nowego środowiska bezpieczeństwa. Środowiska, jak zakładano, pozbawionego wyzwań towarzyszących powstawaniu i ugruntowywaniu się pozycji NATO jako jednego z filarów globalnego ładu. Mogą o tym świadczyć choćby zapisy *Nowej doktryny strategicznej NATO* przyjętej podczas szczytu Sojuszu w Lizbonie w 2010 r., które opis środowiska bezpieczeństwa zaczynały od następującego stwierdzenia:

> Dzisiaj obszar euroatlantycki jest spokojny i zagrożenie terytorium NATO atakiem konwencjonalnym jest niewielkie. Jest to historyczny sukces polityki silnej obrony, euroatlantyckiej integracji i aktywnego partnerstwa, które wytyczały drogę NATO przez ponad pół wieku[2].

Z drugiej strony, przeciwwagą dla przekonania o „końcu historii" i koncepcji rosnącego bezpieczeństwa był rozwój zagrożeń o charakterze asymetrycznym, za którymi stali przede wszystkim aktorzy niepaństwowi, tacy jak międzynarodowe zorganizowane struktury przestępcze czy organizacje terrorystyczne. Bez wątpienia najważniejszym momentem zmiany w postrzeganiu tego, co stanowi największe zagrożenie dla współczesnych demokratycznych państw prawa, były wydarzenia z 11 września 2001 r. Atak na bliźniacze wieże World Trade Center dowiódł tego, że aktor niebędący państwem

[1] Pojęcie sformułowane przez Francisa Fukuyamę; był to również tytuł jego eseju napisanego w 1989 r., który został rozwinięty w książce *The End of History and the Last Man* wydanej w Stanach Zjednoczonych w 1992 r. W Polsce ukazały się dwie publikacje tego autora: *Koniec historii*, Poznań 1996 i *Ostatni człowiek*, Poznań 1997, które są tłumaczeniami fragmentów *The End of History*…

[2] *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, tłumaczenie robocze BBN [online], https://www.bbn.gov.pl/pl/wydarzenia/2694,KoncepcjaStrategicznaNATOtlumaczenie.html [dostęp: 22 IX 2015].

może wstrząsnąć globalnym ładem. Pokazał także, że nawet bez formalnej zmiany prawnomiędzynarodowych podstaw funkcjonowania (a zatem zmian w *Traktacie Północnoatlantyckim*) Sojusz Północnoatlantycki będzie nadal stanowił o kształtowaniu środowiska bezpieczeństwa. Po raz pierwszy bowiem w odpowiedzi na zagrożenie dla jednego z członków Sojuszu powołano się na *casus belli* zapisane w artykule 5 *Traktatu Północnoatlantyckiego*:

> Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez Artykuł 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. O każdej takiej zbrojnej napaści i o wszystkich środkach zastosowanych w jej wyniku zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa[3].

Zapisy te są tym istotniejsze, że – podobnie jak w przypadku *Karty Narodów Zjednoczonych* – trudno spodziewać się takiego rozwoju wydarzeń na arenie międzynarodowej, który pozwoliłby na realną zmianę traktatu, dostosowującą go do współczesnych wyzwań. Oznacza to, że w zbliżających się dziesięcioleciach będziemy opierać swoje bezpieczeństwo na zapisach aktu prawnomiędzynarodowego, który został powołany do życia w połowie ubiegłego wieku, a jego skuteczność będzie zależna od jego międzynarodowej interpretacji. Ta ostatnia zaś jest kwestią szczególnie istotną, biorąc pod uwagę przywołaną powyżej frazę (…) *podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami* ***taką akcję, jaką uzna za konieczną,*** *nie wyłączając użycia siły zbrojnej* (wyróżnienie własne autora).

Traktat Północnoatlantycki nie zobowiązuje zatem państw członkowskich do użycia siły wobec zagrożenia dla terytorium jednego lub więcej członków Sojuszu, lecz wymaga podjęcia kroków *uznanych za konieczne*. Jeśli więc dane państwo członkowskie uzna za konieczne udzielenie pomocy humanitarnej, i takiej udzieli, to wywiąże się ze swoich formalnych zobowiązań. Zasada *pacta sunt servanda* (w dobrej wierze!) chyba nigdzie nie jest tak istotna, jak w przypadku militarnego sojuszu obronnego opartego na tak sformułowanym *casus belli*.

Staje się to tym istotniejsze, im więcej nowych zagrożeń postrzegamy w swoim środowisku bezpieczeństwa. Konieczne wydaje się przypomnienie koncepcji sposobu kształtowania odpowiedniej percepcji zagrożenia i oceny stanu bezpieczeństwa sformułowanej przez Daniela Freia. Zdiagnozował on problem związany z postrzeganiem bezpieczeństwa, wskazując na cztery możliwe sposoby takiej percepcji:

1) stan braku bezpieczeństwa – występuje wtedy, gdy istnieje duże rzeczywiste zagrożenie zewnętrzne, a postrzeganie tego zagrożenia jest prawidłowe (adekwatne),

[3] *Traktat Północnoatlantycki*, Waszyngton, 4 IV 1949 r. [online], http://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pl [dostęp: 22 IX 2015].

2) stan obsesji – występuje w sytuacji, gdy nieznaczne zagrożenie jest postrzegane jako duże,
3) stan fałszywego bezpieczeństwa – występuje wówczas, gdy poważne zagrożenie zewnętrzne jest postrzegane jako niewielkie,
4) stan bezpieczeństwa – wstępuje wtedy, gdy zagrożenie zewnętrzne jest nieznaczne, a jego postrzeganie jest prawidłowe[4].

Koncepcja ta ma znaczenie w związku z problemami, jakie nastręcza nie tylko ocena, ale wręcz definiowanie zagrożeń w środowisku międzynarodowym oraz elastycznie sformułowane zobowiązanie wzajemnej pomocy, zapisane w przywołanym artykule 5 *Traktatu Północnoatlantyckiego*. Z tego właśnie względu rzadko kiedy dyskusja o kwestiach definicyjnych, toczona na poziomie akademickim, ma tak istotne znaczenie, jak dziś. *Realpolitik* już w połowie XIX w. została przez autora tego pojęcia określona jako (...) *prawo władzy rządzące państwami tak, jak prawo grawitacji rządzi światem fizycznym*[5]. I do tej „realności" polityki międzynarodowej, niezależnie od tego, jak bardzo jest zaskakująca, musimy się dziś odnosić. Jednym z elementów uprawiania tego typu polityki jest wykorzystywanie niebezpośrednich metod prowadzenia konfliktu, w tym konfliktu zbrojnego. Z całą pewnością można stwierdzić, że znakiem czasów jest konflikt hybrydowy.

Co jednak rozumiemy przez to pojęcie i do czego się ono odnosi? Oto pytania, z którymi warto się zmierzyć nie tylko ze względu na ciekawość naukową, lecz także z uwagi na dynamikę zdarzeń na arenie międzynarodowej, znacznie wyprzedzającą międzynarodowe porozumienia w dziedzinie bezpieczeństwa. Według analitycznego opracowania estońskiego Międzynarodowego Centrum Obrony i Bezpieczeństwa (International Centre for Defence and Security)[6], powołującego się na Franka Hoffmana, badacza zagadnień związanych z bezpieczeństwem międzynarodowym, w o j n a h y b r y d o w a (ang. *'hybrid warfare,*) to:

> (…) połączenie morderczości konfliktu międzypaństwowego i przedłużającej się żarliwości konfliktu nieregularnego. (…) Skomplikowane kampanie łączą operacje konwencjonalne o niskiej intensywności i operacje specjalne, działania ofensywne w cyberprzestrzeni oraz operacje psychologiczne wykorzystujące media społecznościowe i tradycyjne w celu wywierania wpływu na opinię publiczną, również na poziomie międzynarodowym[7].

Zdefiniowanie konfliktu (wojny hybrydowej) na potrzeby polskiego systemu bezpieczeństwa wzięło na siebie Biuro Bezpieczeństwa Narodowego. Na stronie BBN w opracowaniu *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa* czytamy:

---

[4] D. Frei, *Sicherheit. Grundfragen der Weltpolitik*, Stuttart 1977, s. 17−21, cyt. za: R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje − struktury − funkcjonowanie*, Warszawa 1999, s. 28−29.

[5] L. von Rochau, *Grundsätze der Realpolitik*, t. 1, Stuttgart 1853 [online], https://books.google.pl/books?id=c0hGAAAAcAAJ&pg=PP5 [dostęp: 22 IX 2015].

[6] Zob. http://www.icds.ee/.

[7] E. Hunter, P. Pernik, *The Challenges of Hybrid Warfare*, ICDS, kwiecień 2015 [online], http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf [dostęp: 22 IX 2015].

> Wojna hybrydowa [to] wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.[8]

Definicję wojny hybrydowej zaczerpniętą ze strony BBN warto uzupełnić innymi pojęciami z tegoż opracowania, które są niezbędne do pełnego zrozumienia zagrożeń wynikających z popularyzacji taktyk hybrydowych w działaniach państw. Szczególnie istotne w tym kontekście jest pojęcie a g r e s j i p o d p r o g o w e j. I tak, w *(Mini)Słowniku BBN* jest ona zdefiniowana następująco:

> Agresja podprogowa – działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa[9].

Warto w tym miejscu przywołać wspomnianą już wcześniej niedookreśloność artykułu 5 *Traktatu Północnoatlantyckiego*. W okolicznościach niesprzyjającego klimatu politycznego, przy umiejętnym stosowaniu przez potencjalnego agresora taktyk, które uniemożliwiają społeczności międzynarodowej jednoznaczne stwierdzenie, czy rzeczywiście ma już do czynienia z wojną, agresja podprogowa może stanowić jedno z najpoważniejszych zagrożeń współczesnego świata.

Kolejnym ważnym pojęciem, do którego zdefiniowania zmusza obecna sytuacja międzynarodowa, są z i e l o n e l u d z i k i. Choć zostało ono ukute w odniesieniu do rozwoju sytuacji na wschodniej Ukrainie i w związku z tym ma charakter bardzo potoczny, to odnosi się do zjawiska, które należy traktować jako niezwykle poważne zagrożenie. Zgodnie z przywoływanym już *(Mini)Słownikiem BBN*:

> „Zielone ludziki" – potocznie stosowane określenie uzbrojonych żołnierzy nieposiadających dystynkcji wojskowych, ani innych wyróżników, które pozwalałyby na określenie ich narodowości, prowadzących zbrojne działania regularne i nieregularne na terytorium wschodniej Ukrainy, wymierzone przeciwko jej integralności i niezawisłości[10].

Istotną cechą zagrożeń hybrydowych jest to, że przydatność omawianych taktyk jest różna w zależności od teatru działań, na jakim funkcjonuje państwo i jego potencjalny przeciwnik. Dowodem na to są chociażby wydarzenia na wschodniej Ukrainie.

Realizacja działań zaczepnych i ofensywnych jest możliwa w sytuacji spełnienia określonych warunków, np.: dużego zróżnicowania etnicznego, niedoskonałej kontroli terytorialnej i kontroli ruchu granicznego. Prawdopodobieństwo nieoczekiwanego pojawienia się na przykład w Polsce brygad „zielonych ludzików" jest znacznie mniejsze, niż

[8] *(Mini)Słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa* [online], http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 22 IX 2015].

[9] Tamże.

[10] Tamże.

w przypadku państw mniej stabilnych. System obrony i bezpieczeństwa wewnętrznego RP sprawia, że Polska powinna być wyczulona na bardziej zaawansowane sposoby ataku stosowane w przypadku konfliktu hybrydywego.

Szczególne obszary potencjalnej walki w konflikcie hybrydowym, w których występuje konieczność podejmowania działań i przeciwdziałania zagrożeniom, a które zostały dostrzeżone w Polsce, to cyberprzestrzeń i infosfera. Walka informacyjna toczona zarówno w cyberprzestrzeni, jak i w mediach oraz problemy definicyjne i polityczne dotyczące konfliktu hybrydowego są jednymi z priorytetów w kwestii aktywnego przeciwdziałania zagrożeniom. W związku z tym są potrzebne działania dostosowawcze na poziomie prawnym i strategicznym. W Polsce tego rodzaju inicjatywa została podjęta już w 2014 r., kiedy to powstawały zręby przyjętej przez Radę Bezpieczeństwa Narodowego *Doktryny cyberbezpieczeństwa RP*.

Dokument ten, którego źródłami były zarówno *Strategia Bezpieczeństwa Narodowego*, jak i wyniki poprzedzającego jej przyjęcie *Strategicznego Przeglądu Bezpieczeństwa Narodowego*, stanowi, że:

> **Strategicznym celem** w obszarze cyberbezpieczeństwa RP, sformułowanym w Strategii Bezpieczeństwa Narodowego RP, **jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni**, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia[11].

Jeśli chodzi o infosferę i zapewnienie bezpieczeństwa informacyjnego RP, to zapisy o podobnym charakterze znalazły się w projekcie *Doktryny bezpieczeństwa informacyjnego RP*. Dokument ten, będący w końcu lipca 2015 r. jeszcze w opracowaniu, zawiera stwierdzenie, że:

> Celem strategicznym w obszarze bezpieczeństwa informacyjnego jest zapewnienie bezpiecznego funkcjonowania RP w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych (zwłaszcza administracji publicznej, służb bezpieczeństwa i porządku publicznego, służb specjalnych i sił zbrojnych), sektora prywatnego i społeczeństwa obywatelskiego[12].

Łatwo zauważyć, że podejście metodologiczne w obu dokumentach jest bardzo zbliżone i wynika z przywoływanego już *Strategicznego Przeglądu Bezpieczeństwa Narodowego*. Istotną wartością obu doktryn jest urealnienie i precyzyjne zdefiniowanie nowych wyzwań i zagrożeń. Nowych nie w sensie powstania niespotykanego dotąd rodzaju zagrożenia (gdyż taka konstatacja w stosunku do wojny informacyjnej stałaby w sprzeczności ze *Sztuką wojny* Sun Tzu), ale raczej w kontekście priorytetyzowania zadań i określania najważniejszych obszarów aktywności w zmieniającym się środowisku bezpieczeństwa. Trzeba bowiem podkreślić, że transsektorowość jest nie-

[11] *Doktryna cyberbezpieczeństwa RP* [online], https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, s. 9 [dostęp: 22 IX 2015]. Wyróżnienie w tekście oryginalnym.

[12] Projekt *Doktryny bezpieczeństwa informacyjnego RP*, lipiec 2015 r. [online], https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, s. 5 [dostęp: 22 IX 2015].

odłączną cechą zagrożeń w cyberprzestrzeni i zagrożeń informacyjnych. Konieczność tworzenia i optymalizacji funkcjonowania stosownych fizycznych elementów systemu bezpieczeństwa narodowego i obrony (np. wyspecjalizowanych jednostek wojskowych oraz właściwych jednostek organizacyjnych służb specjalnych) staje się jednym z priorytetów organizacji systemu bezpieczeństwa narodowego, umożliwiającym jego efektywne funkcjonowanie.

Wykorzystywanie wielu środków, które mogą służyć realizacji celów operacyjnych i strategicznych w konflikcie hybrydowym, wymaga umiejętnego posługiwania się narzędziami, zwłaszcza tymi typowymi dla ochrony cyberprzestrzeni i infosfery. Nie tylko pozwalają one na ewentualne opanowanie systemu dowodzenia i kontroli przeciwnika, lecz także pomagają wywierać wpływ na szeroko pojętą opinię publiczną w kraju i za granicą. Przy założeniu, że jednym z najtrudniejszych aspektów zarządzania kryzysem wynikającym z zagrożeń hybrydowych jest aspekt komunikacji i wypracowania wspólnej świadomości sytuacyjnej, cyberprzestrzeń i infosfera stają się najbardziej prominentnymi polami prowadzenia walki i pierwszą linią starcia. Uważna obserwacja ruchów przeciwnika i system wczesnego ostrzegania prawidłowo funkcjonujący w tych właśnie dwóch obszarach będą stanowić o zdolności do prowadzenia działań prewencyjnych w innych wymiarach dotyczących bezpieczeństwa państwa i jego obywateli.

Wysiłki podejmowane przez jednostki administracji publicznej RP, których celem jest sformułowanie doktrynalnej odpowiedzi na nowe zagrożenia świadczą o tym, że zagrożenia związane z konfliktem hybrydowym są w Polsce dobrze rozpoznane.

Środowisko bezpieczeństwa RP, definiowane podczas Strategicznego Przeglądu Bezpieczeństwa Narodowego (SPBN), było postrzegane jako niezwykle złożone i dynamiczne już na etapie analiz prowadzonych w związku z tym przedsięwzięciem. Warto jednak podkreślić, że w *Białej Księdze Bezpieczeństwa Narodowego*[13], wydanej w 2013 r. jako podsumowanie SPBN, nie występują jeszcze takie terminy, jak „wojna hybrydowa" czy „agresja podprogowa".

Tym ważniejsze było sformułowanie odpowiednich definicji oraz wprowadzenie do debaty publicznej pojęć określających otaczającą nas rzeczywistość międzynarodową. Choć definicje te nie mają charakteru prawnomiędzynarodowego ani nawet prawnego w skali krajowego systemu prawa, to mogą stać się początkiem formułowania koncepcji odpowiedzi na takie zagrożenia. W przypadku Polski jest to o tyle istotne, że toczący się za naszą wschodnią granicą konflikt rosyjsko-ukraiński jest źródłem potencjalnych zagrożeń dla stabilności w regionie. Nie należy o tym zapominać nawet w sytuacji takich aktualnych wydarzeń, jak np. trwający od miesięcy kryzys imigracyjny, na który Europa nie znajduje dobrej recepty, gdyż zmiana geopolityczna wynikająca z ewolucji rosyjskiej polityki międzynarodowej pozostaje istotnym czynnikiem wpływającym na bezpieczeństwo RP i jej obywateli.

Konieczność dostosowania nie tylko uregulowań prawnych, lecz także przede wszystkim podstaw koncepcyjnych prowadzenia działań defensywnych oraz zaczepno-obronnych wymaga pełnej świadomości sytuacyjnej i realnej oceny środków, jakimi dysponuje przeciwnik, znajomości jego celów geostrategicznych oraz intencji w długiej perspektywie.

[13] *Biała Księga Bezpieczeństwa Narodowego RP*, Warszawa 2013.

W debacie publicznej pojawiają się głosy mówiące o tym, że wprowadzanie pojęcia „wojny hybrydowej" mija się z celem, ponieważ w historii ludzkości konflikty od zawsze były prowadzone wszelkimi dostępnymi środkami, które mogły zwiększyć prawdopodobieństwo osiągnięcia założonego celu. Część badaczy argumentuje więc, że zamiast koncentrować się na tworzeniu nowych pojęć, trzeba skupić się na wykrywaniu i definiowaniu złożonych kombinacji dostępnych środków walki tak, aby być gotowym na przeciwdziałanie im[14].

I choć z punktu widzenia taktyki wojskowej i operacji realizowanych na teatrze działań wojennych subtelne rozróżnienia pojęciowe mogą mieć nikłe znaczenie, to z punktu widzenia politycznego, w sytuacji potrzeby jasnego zdefiniowania międzynarodowych reakcji na zaistnienie aktu wojny, te definicje mogą stanowić o „być albo nie być" solidarności pomiędzy sojusznikami. Ta solidarność, a także wspólne, spójne obraz i ocena sytuacji mogą być niezmiernie ważne w przypadku potencjalnego konfliktu. Doktryna wojenna Federacji Rosyjskiej z 2014 r. daje szczególne powody do dbałości o tego rodzaju solidarność w kontekście zagrożeń hybrydowych. Jak bowiem warto przypomnieć, to właśnie w tym dokumencie pojawiają się następujące zapisy:

1. kompleksowe użycie sił zbrojnych, jak również politycznych, ekonomicznych, informacyjnych i innych środków niewojskowych, realizowanych przy szerokim wykorzystaniu potencjału protestu i sił operacji specjalnych,
2. wpływanie na przeciwnika na całej głębokości jego terytorium, w globalnej przestrzeni informacyjnej, w przestrzeni powietrzno-kosmicznej, na lądzie i morzu,
3. udział w działaniach wojennych nieregularnych formacji zbrojnych i prywatnych firm wojskowych,
4. stosowanie niebezpośrednich i asymetrycznych metod działań,
5. wykorzystanie sił politycznych i ruchów społecznych finansowanych i zarządzanych z zewnątrz[15].

Biorąc pod uwagę sformułowania tego dokumentu oraz jego usytuowanie prawno-polityczne nietrudno skonstatować, że (niezależnie od używania nomenklatury „hybrydowa") niestandardowa forma konfliktu wykorzystująca komponenty asymetryczne, informacyjne i niebezpośrednie stała się immanentną częścią rzeczywistości, w której funkcjonują współczesne państwa.

Analizując złożoność wykorzystywanych środków i sposobów walki, problemy z ich definiowaniem, małą intensywność potencjalnych wrogich działań (czyli działania poniżej progu agresji) oraz anonimowość sił biorących udział w ewentualnym konflikcie, sformułowanie sojuszniczej odpowiedzi zaczyna być kwestią decyzji politycznej, która zastępuje automatyzm wynikający z międzynarodowych porozumień obronnych. Stanowi to duże wyzwanie, zwłaszcza w związku z przywołanym zapisem *Traktatu* o tym, że państwa członkowskie Sojuszu mają reagować na potencjalną agresję przez podjęcie (…) *takiej akcji, jaką uzna*[ją] *za konieczną* – bez bezpośredniej wzmianki o bezwzględnym obowiązku udzielania pomocy zbrojnej.

[14] D. Van Puyvelde, *Hybrid war: does it even exist?* [online], http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [dostęp: 22 IX 2015].

[15] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle Doktryny Wojennej Rosji,* maj 2015 [online], http://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf [dostęp: 22 IX 2015].

Z tego powodu, niezależnie od puryzmu pojęciowego krytykującego wprowadzanie do obiegu sformułowań, takich jak „wojna hybrydowa", trzeba zgodzić z jednym: jakbyśmy tego stanu (nie)bezpieczeństwa nie nazwali, musimy być przygotowani do funkcjonowania w środowisku bezpieczeństwa, w którym konflikt mieszany, wykorzystujący wszystkie dostępne taktyki, strategie, metody i środki jest faktem. I nostalgia za czasami starcia klasycznego, jasno określonego granicami *ius in bello*, nie przywróci go prawdopodobnie już nigdy.

Jolanta Darczewska

Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?

Na naszych oczach Rosja przekształciła realny konflikt ukraińsko-rosyjski i interwencję zbrojną na Ukrainie w wirtualny konflikt Rosji z Zachodem. Powracając do starego modelu polityki zagranicznej opartego na rywalizacji ze Stanami Zjednoczonymi, Rosja manifestuje swoje ambicje geopolityczne i siłą wytycza granice „cywilizacji rosyjskiego świata", rzucając wyzwanie postzimnowojennemu porządkowi w Europie. W najnowszej historii były one przyczyną wielu trudności i zwrotów w relacjach Rosji z Zachodem. Jak dotąd Zachód nie znalazł dobrej odpowiedzi na rewizjonistyczną politykę Rosji ani pomysłu na zneutralizowanie towarzyszących jej akcji informacyjnych.

W ostatnich latach akcje te przybrały na intensywności, wywołując refleksję na temat samej natury wojny informacyjnej, jej głębszych przyczyn, mechanizmów oraz potencjału sił i środków. Potencjał ten jest budowany w Rosji od lat, od lat trwa także szeroko zakrojony publiczny dyskurs na temat walki informacyjnej, jej podstaw koncepcyjnych, metodologicznych i organizacyjnych. Niniejszy tekst przybliża aktualne trendy w tej debacie, które wyraźnie przekładają się na praktykę oddziaływania informacyjnego. Rosyjscy teoretycy i praktycy stale odwołują się przy tym do dorobku zachodniej myśli wojskowej, zacierając w ten sposób granice między jego wymiarem defensywnym i ofensywnym (*Takie działania są uzasadnione, bowiem Rosja musi się bronić*) oraz manipulacyjnie, podkreślając, że rosyjskie działania nie różnią się od zachodnich.

Rosyjska wizja świata – światopoglądowe podstawy wojny informacyjnej

Podczas dorocznego spotkania Klubu Wałdajskiego, które odbyło się pod koniec października 2014 r. w Soczi, zatytułowanego „Porządek światowy: nowe reguły czy gra bez reguł", prezydent Władimir Putin akcentował, że Rosja jest gotowa przeciwstawić się Stanom Zjednoczonym, kruszącym światowy porządek i stawiającym ludzkość na skraju wojny. (…) *Jednostronny dyktat skutkuje eskalacją konfliktów* (…). *Powoduje poszerzenie przestrzeni chaosu, zamiast wzmacniania suwerennych, stabilnych państw. Zamiast doskonalenia demokracji oznacza poparcie dla wielce podejrzanej publiki – od neonazistów do radykałów islamskich*[1]. Wyjaśniając genezę konfliktu rosyjsko-ukraińskiego, tłumaczył, że spowodował go pośpiech, z jakim Unia Europejska dążyła do stowarzyszenia z Ukrainą. *Było to dla Rosji nie do przyjęcia, gdyż godziło w jej interesy w sąsiednim państwie*.

Sekretarz Rady Bezpieczeństwa FR Nikołaj Patruszew zinterpretował wydarzenia na Ukrainie w kluczu teorii spiskowej jako (...) *kontynuację planu rozpadu ZSRR i Rosji*[2]. Ujmuje ten plan w dłuższej perspektywie, przytaczając długą listę (…) *amerykańskich operacji specjalnych zorientowanych w ciągu minionych 25 lat na totalne przeformatowanie przestrzeni poradzieckiej pod amerykańskie interesy* (Wiosna Ludów 1989 r., woj-

[1] Zob. *«Валдайская» речь Путина: критика Запада как путь к диалогу*, RIA Novosti z 24 X 2014 r. [online], http://ria.ru/politics/20141024/1029977993.html [dostęp: 28 IX 2015].

[2] Zob. И. Егоров, *Вторая «холодная». Николай Патрушев: «Отрезвление» украинцев будет жёстким и болезненным*, „Российская газета" z 15 X 2014 [online], http://www.rg.ru/2014/10/15/patrushev.html [dostęp: 28 IX 2015].

ny w Czeczenii, wojna na Bałkanach, poradzieckie kolorowe rewolucje – przyp. aut.). (…) *W efekcie wyrosło całe pokolenie zatrute nienawiścią do Rosji i mitycznymi europejskimi wartościami*. Generał zasugerował przy tym, że Ukraina nie ma innej opcji niż pozostanie częścią tzw. rosyjskiego świata: (…) *Ukraina nie jest w stanie rozwijać się bez Rosji – czy to się komuś podoba, czy nie*[3].

Zachodnie próby zdemontowania „kruchej" przestrzeni poradzieckiej dostrzega także patriarcha Moskwy i Wszechrusi Cyryl. W orędziu wygłoszonym 11 listopada 2014 r. z okazji otwarcia XVIII Wszechświatowego Ruskiego Soboru Narodowego patriarcha powiedział:

> (…) Rok 2014 otworzył nowy rozdział w historii świata, rozdział trudny, dramatyczny, znamionujący koniec tego, co można nazwać «światem poradzieckim». Ten świat był kruchy. Nie wyłonił się w nim trwały porządek, oparty na wzajemnym zrozumieniu i poszanowaniu się ludzi należących do różnych kultur i cywilizacji. Ci, którzy uważają się za zwycięzców zimnej wojny, wmawiają wszystkim, że wyznaczona przez nich droga rozwoju jest jedynie słuszna. Dominując w globalnej przestrzeni informacyjnej, narzucają światu swoje rozumienie gospodarki i ustroju państwowego, próbują zdławić gotowość do obrony wartości i ideałów odbiegających od idei społeczeństwa konsumpcyjnego[4].

Przytoczone wypowiedzi łączy wspólna matryca światopoglądowa. Najwyżsi przedstawiciele hierarchii politycznej, „siłowej" i cerkiewnej identycznie postrzegają świat i identycznie objaśniają problemy Rosji w relacjach międzynarodowych. Umieszczają je w paradygmacie geopolitycznym i nadają im ideologiczny sens. Takie zideologizowane idee z jednej strony maskują rzeczywiste przyczyny konfliktu rosyjsko-ukraińskiego, z drugiej zaś umożliwiają strategiczne zarządzanie informacją traktowaną jako broń oraz rozbudowę potencjału sił i środków walki informacyjnej. Jest ona prowadzona na wielu płaszczyznach (ekonomicznej, politycznej, dyplomatycznej, humanitarnej, wojskowej) i wielu frontach, w tym (a nawet – przede wszystkim) na froncie wewnętrznym.

W Rosji (czyli właśnie na froncie wewnętrznym) wyżej przedstawiona w uproszczeniu konspirologiczna wizja świata, dodatkowo wyraziście wskazująca wroga, trafia na podatny grunt. Propagandowo nośna, zapewnia skuteczność oddziaływania informacyjnego. Potwierdzają to badania opinii publicznej: 65–70 proc. Rosjan kategorycznie odrzuca udział Rosji w konflikcie na Ukrainie, traktując go jako ukraiński konflikt wewnątrzpolityczny. Niemal pełną jednomyślność (95–96 proc.) rosyjscy respondenci wykazują w odpowiedzi na pytanie o odpowiedzialność FR w przedłużającym się konflikcie, naruszaniu porozumień mińskich i zestrzeleniu samolotu MH17. Odpowiedzialność tę zdecydowanie przerzucają na (...) *Zachód, który wciąga Ukrainę w orbitę swoich wpływów*[5].

---

[3] Tamże.

[4] *Слово Святейшего Патриарха Кирилла на открытии XVIII Всемирного русского народного собора* [online], http://www.patriarchia.ru/db/text/3367103.html [dostęp: 28 IX 2015].

[5] *Российская социология украинского конфликта* [online], http://www.levada.ru/27-08-2015/rossiiskaya-sotsiologiya-ukrainskogo-konflikta [dostęp: 28 IX 2015].

Podstawy koncepcyjne: „Wielka Europa", „Wielka Eurazja", „Wielka Rosja"…

Obarczanie Zachodu odpowiedzialnością za niekonwencjonalną wojnę na Ukrainie to tylko jedna z wielu operacji wojny informacyjnej Rosji z Zachodem. Wojna ta nie rozpoczęła się wraz z Euromajdanem w grudniu 2013 r. (…) *Zmiana w rosyjskiej polityce nastąpiła w okresie, gdy za sprawą rewolucji róż i pomarańczowej rewolucji doszły do władzy w Tbilisi i Kijowie nowe polityczne elity, pragnące, by ich kraje rozwijały się dokładnie w przeciwnym niż Rosja kierunku* – pisał Ronald Asmus[6]. Zmiana ta rozpoczęła się w momencie, kiedy Rosja weszła na ścieżkę autorytaryzmu. Priorytetem dla polityków na Kremlu stało się odzyskanie geopolitycznej kontroli nad przyległymi do FR obszarami i odbudowanie stref wpływów z czasów ZSRR. Próbowali nie dopuścić do tego, aby sąsiedzi Rosji (kraje bałtyckie, Gruzja, Ukraina, a wcześniej Polska, Czechy i Słowacja) weszły na ścieżkę prozachodnią. Przez ostre kampanie informacyjne Kremla przeciwko tym krajom przebijało się stanowisko, że Europa Środkowa i Wschodnia są strefą wpływów FR, a wszelkie działania Zachodu podważające te wpywy są równoznaczne z podważaniem mocarstwowej pozycji Rosji. Świadomość własnych ograniczeń osłabiła wówczas rosyjski sprzeciw wobec rozszerzenia NATO i UE. Proponowaną alternatywą dla prozachodniej orientacji państw aspirujących do NATO i UE stały się „pozytywne" oferty krzyżowych gwarancji bezpieczeństwa dla tych państw, utworzenia strefy bezatomowej i przekształcenia NATO w blok polityczny będący częścią nowego regionalnego systemu bezpieczeństwa z udziałem Rosji (projekt „Wielkiej Europy" od Brestu do Władywostoka). Rozwijany równolegle projekt „Wielkiej Eurazji" nie przekreślił tej alternatywy, uzbroił jednak Rosję w nowe konstrukty ideowe: budowany Związek Eurazjatycki z centrum w Moskwie ma być odrębną „cywilizacją", której misją jest powstrzymywanie ekspansji cywilizacyjnej Zachodu.

Od początku oba projekty kształtowały się w opozycji do liberalnej wizji świata, o czym świadczy nieustannie propagandowo nagłaśniana wewnątrzrosyjska gra między dwoma nurtami: „prozachodnim" liberalnym i „eurazjatyckim" konserwatywnym. Ten ostatni przeszedł znamienną ewolucję: od wersji łagodnej (1993 r. – doktryna bliskiej zagranicy; jawne raporty Służby Wywiadu Zagranicznego (SWR), tzw. raporty Primakowa, w tym zwłaszcza pierwszy, pt. *Rola Rosji na obszarze WNP*) przez geopolitykę w działaniu (1999 r. – tzw. pętla Primakowa: premier, na wieść o rozpoczęciu operacji NATO w Kosowie, zawrócił samolot, którym leciał z wizytą do USA; a także słynne rewizjonistyczne wystąpienie W. Putina podczas konferencji bezpieczeństwa w Monachium w 2007 r.), aż do obecnego, ekspansywnego nurtu imperialno-nacjonalistycznego reprezentowanego przez rzeczników koncepcji „Wielka Rosja".

Po powrocie W. Putina na urząd prezydenta w 2012 r. projekty „Wielka Eurazja" i „Wielka Rosja" miały służyć kontynuowaniu odbudowy pozycji mocarstwowej Rosji w starym, imperialnym stylu. Te geopolityczne projekty mają walor praktyczny: za pomocą są formułowane zasady działania na rzecz politycznej reintegracji Azji i Europy Wschodniej. Głoszą istnienie na obszarze odpowiadającym terytorium byłego Imperium Rosyjskiego odrębnej wspólnoty cywilizacyjno-historycznej. Podkreślają sens kulturowy wspólnoty rosyjskojęzycznej (koncepcja tzw. rosyjskiego świata). Pojęcie „narodu" rozszerzają na obszary, na których dominuje język i kultura rosyjska. Projekty te stały

[6] R. Asmus, *Mała wojna, która wstrząsnęła światem. Gruzja, Rosja i przyszłość Zachodu*. Warszawa 2010, s. 376 i nast.

się narzędziem zarządzania konfliktami na obszarze poradzieckim (Abchazja, Osetia Północna, Krym itd.), konfrontacji ze światem zachodnim, który jest postrzegany jako źródło wartości alternatywnych i jako agresor na obszarze żywotnych interesów Rosji. Z jednej strony weszły do instrumentarium mobilizacji i konsolidacji społeczeństwa FR, a z drugiej stały się alternatywną rosyjską ofertą dla wszystkich państw, „które nie godzą się z amerykańską hegemonią na świecie". Imperialna mobilizacja i konsolidacja zaowocowała jednocześnie porównywalną z kultem jednostki pozycją prezydenta FR W. Putina budującego „nowoczesną wielką Rosję" na użytek wewnętrzny i przekształca się w (…) *globalnego lidera, organizatora globalnej symfonii* (…), *wyraziciela tych, którzy nie chcą świata jednobiegunowego*[7].

Oddziaływanie informacyjne zbudowane na takiej podstawie koncepcyjnej nie jest zjawiskiem nowym. Niektóre tezy (np. że świat nie może być jednobiegunowy) są powtarzane niezmiennie od początku lat 90. XX w. Niezmienne są bowiem cele strategiczne Rosji: zdobycie pozycji mocarstwa globalnego, poszerzenie imperium, osłabienie, sparaliżowanie NATO, „odamerykanizowanie" i „porwanie" Europy oraz poszerzenie grona sojuszników Rosji. Nowe cele są związane z rewolucją cyfrową – należą do nich: multimedialne kanały powielania informacji, szeroka skala oddziaływania (odpowiednio do globalnej mocarstwowej misji Rosji), a także wysoki poziom agresji informacyjnej. Niezmienny jest też obraz sytuacji geopolitycznej na świecie, a także Stanów Zjednoczonych narzucających państwom swój system wartości i model rozwoju. Z tego względu władze Ukrainy (*junta*) w rosyjskiej propagandzie nadal będą przedstawiane jako *pionki w geopolitycznej grze USA*, Polska i kraje bałtyckie – jako *przyczółki USA w walce z Rosją*, rosyjska gra w Syrii zaś jako przejęcie przez W. Putina od B. Obamy inicjatywy walki z Państwem Islamskim, gdyż amerykańska taktyka w tej kwestii jest nieskuteczna[8].

Rosja zbroi się nadal

Rosyjski teoretyk Siergiej Rastorgujew z Instytutu Problemów Bezpieczeństwa Informacyjnego Uniwersytetu im. M.W. Łomonosowa nie widzi różnicy między celami wojny informacyjnej a celami pozostałych rodzajów wojen: wszystkie toczą się o zasoby innych państw (w przypadku wojen informacyjnych – o zasoby społeczne):

> (…) *Kluczem do tych zasobów są elity i media przeciwnika. Ważnym czynnikiem jest posiadanie wśród tych elit i mediów niezbędnej masy agentów wpływu, których agresor rekrutuje spośród osób o egoistycznym bądź niewolniczym światopoglądzie*. (…) *strategia wojny informacyjnej zawsze łączy mnóstwo powiązanych wzajemnie taktycznych operacji informacyjnych. Globalny cel tych operacji nie zawsze jest widoczny. Ale taka jest natura rzeczy. Bo cóż to za operacja, która jest rozpoznawalna dla wszystkich, w tym dla ofiary?*[9]

[7] Wypowiedź popularnego obecnie lidera opinii Siergieja Kurginiana, zob. http:// www.regnum.ru/news/polit/1981097.html) [dostęp: 28 IX 2015].

[8] http://russila.su/2015/09/05/rossija-schitaet-neeffektivnoj-amerikanskuyu-koalitsiyu-ptotiv-ig [dostęp: 28 IX 2015].

[9] О. Назаров, *Информационные войны – угроза для цивилизации* [online], „*Литературная газета*" 2013, nr 42, http://www.lgz.ru/article/-42-6435-23-10-2013/informatsionnye-voyny-ugroza-dlya-tsivilizatsii-/ [dostęp: 28 IX 2015].

S. Rastorgujew od dawna powtarza, że taktyka defensywna w tej wojnie prowadzi do klęski: (…) *wojna informacyjna oznacza ofensywę, zaś o skuteczności działań decyduje realny potencjał sił i środków oddziaływania lub jej brak*[10].

Pod cele prowadzonych wojen informacyjnych przewartościowano zagrożenia dla Rosji. Od dawna są one postrzegane jako próba zawładnięcia zasobami FR, ich wyeksploatowania i degradacji. O ile wcześniej akcentowano eksploatowanie zasobów surowcowych, to obecnie na pierwszy plan są wysuwane zagrożenia ideologiczne i cywilizacyjne[11]. Wpisuje się to w obserwowaną w Rosji od lat militaryzację polityki. Służąca jej manipulacja własnej i zagranicznej opinii publicznej ma uzasadnić działania Kremla na arenie wewnętrznej i międzynarodowej.

Identyczną percepcję zagrożeń demonstrują przedstawiciele władz wojskowych i politycznych Rosji. W dniu 1 września 2015 r. podczas inauguracji nowego roku szkoleniowego w Wojskowej Akademii Sztabu Generalnego szef Sztabu Generalnego Sił Zbrojnych FR gen. Walerij Gierasimow za główne wojskowe zagrożenie dla Rosji uznał (…) *kolorowe rewolucje, które przyjmują formę walki zbrojnej i są prowadzone zgodnie z regułami sztuki wojennej*[12]. Zagrożenie to prezydent W. Putin utożsamia z próbami politycznej destabilizacji Rosji, którym Kreml da zdecydowany opór (*W Rosji kolorowej rewolucji nie będzie*). Za sojusznika władz uznaje w tym kontekście „społeczeństwo obywatelskie" FR, podkreślając konieczność jego ścisłego współdziałania z organami władzy państwowej[13].

Prezydent często spotyka się z przedstawicielami specyficznie rozumianego społeczeństwa obywatelskiego, instruując ich i wytyczając im zadania. Politologom powiedział: (…) *Rosja nie pozwoli sobie narzucić poczucia winy*, a historykom powierzył (…) *misję obrony rosyjskiego stanowiska w przestrzeni informacyjnej*[14]. Rosyjskie Towarzystwo Geograficzne, któremu przewodniczy minister obrony gen. Siergiej Szojgu, prezydent określił mianem „systemowego lidera" i zaangażował m.in. do stworzenia rosyjskiej alternatywy Wikipedii, gdyż ta (…) *nie jest w stanie wiarygodnie informować o rosyjskich regionach i życiu w kraju*. Spotyka się też z prezesem Imperatorskiego Prawosławnego Towarzystwa Palestyńskiego, gen. Siergiejem Stiepaszynem, który w swej karierze zawodowej pełnił wiele eksponowanych funkcji, m.in. szefa FSB, premiera FR, dyrektora Izby Obrachunkowej FR (odpowiednik polskiej NIK). Działające przy Towarzystwie Centrum ds. Rozwoju Chrześcijaństwa na Wschodzie organizuje pomoc humanitarną dla Syrii, odbudowuje cerkwie zniszczone przez Państwo Islamskie itp. Z racji swych obowiązków S. Stiepaszyn ma dobre relacje z prezydentem Baszarem al-Asadem[15].

Takie działania unaoczniają, że Rosja dąży do utrzymania kierunku wyznaczonego w dokumentach strategicznych, m.in. w *Doktrynie bezpieczeństwa informacyjnego FR* (2000 r.) czy *Doktrynie wojennej FR* (2014 r.). Z punktu widzenia Kremla wymaga to pod-

[10] Tamże.

[11] Szerzej na ten temat zob. http://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2015-05-19/diabel-tkwi-w-szczegolach-wojna-informacyjna-w-swietle-doktryn [dostęp: 28 IX 2015].

[12] *Глава Генштаба: в мире продолжается экспорт радикализма и хаоса*, РИА Новости z 5 X 2015 r., [online], http://ria.ru/defense_safety/20150901/1220907690.html [dostęp: 28 IX 2015].

[13] Zob. *Заседание Совета Безопасности Российской Федерации* [online], http://www.scrf.gov.ru/news/825.html [dostęp: 28 IX 2015].

[14] Е. Рыковцева, *Путин: инструктаж для историков*, Радио Свобода [online], http://www.svoboda.org/content/transcript/26675801.html [dostęp: 28 IX 2015].

[15] Zob. wypowiedź S. Stiepaszyna dla radia „Echo Moskwy" z 16 III 2015 r., http://www.msk.ru [dostęp: 28 IX 2015].

trzymania dyskursu imperialnego (który w rosyjskiej teorii jest traktowany jako *broń koncepcyjna, intelektualna*), doskonalenia metod i środków oddziaływania informacyjnego (*broń metodologiczna*) oraz zbudowania szerokiego zaplecza wykonawczego (*broń organizacyjna*). Ma to w zamierzeniu zapewnić Rosji przewagę informacyjną nad Zachodem.

Rozwój dyskursu imperialnego

Dominującym nurtem w tym dyskursie jest sięganie po stereotypy historyczne (*wojna historyczna*). W ten sposób wykazuje się ciągłość imperialną Rosji – od Rusi Kijowskiej przez Wielkie Księstwo Moskiewskie, Imperium Rosyjskie i ZSRR aż po Federację Rosyjską. Zmanipulowane fakty historyczne są sprowadzane do rosyjskiej propagandowej wizji świata, służą osłabianiu negatywnych dla Rosji konotacji (np. ukraińskich w genezie państwa rosyjskiego) i wzmacnianiu negatywnych skojarzeń dotyczących innych państw (pamięć o zwycięstwie nad faszyzmem warunkuje skuteczność stereotypu Ukraińca „faszysty"). Tym należy wyjaśniać gloryfikację Wielkiej Wojny Ojczyźnianej, której 70-lecie zakończenia obchodzono z wyjątkową oprawą medialną. Otoczoną kultem pamięć historyczną o zwycięstwie ZSRR nad faszyzmem Kreml wykorzystał do własnych celów politycznych: Zachód chce odebrać Rosji jej zwycięstwo, bezcześci pomniki ofiar wojny itp.

Propagandowe eksploatowanie historii nie jest zjawiskiem nowym, w minionym dziesięcioleciu było jednak uruchamiane głównie podczas kampanii informacyjnych w środkach masowego przekazu. W bieżącym roku trwa nieprzerwanie i znajduje wyraz na wszystkich „frontach" rosyjskiej walki informacyjnej, także dyplomatycznym i eksperckim. Świadczy o tym choćby głośna wypowiedź ambasadora FR Siergieja Andriejewa relatywizująca przyczyny II wojny światowej, do której doprowadziła także (…) *polityka Polski blokującej zbudowanie koalicji przeciwko Niemcom hitlerowskim*. W historycznym kluczu rosyjscy analitycy wyjaśniają bieżące problemy Rosji w stosunkach z innymi państwami. Ekspert Rosyjskiego Instytutu Studiów Strategicznych Oleg Niemienskij[16] w swym obszernym artykule *Relacje polsko-ukraińskie na obecnym etapie* przewartościował przy okazji obecny stan relacji polsko-rosyjskich. Przyczyną ich pogorszenia jest w jego ocenie (…) *odwieczna (co najmniej od XVI–XVII ww.) walka Polski z Rosją o przywództwo na Wschodzie*, przy czym (…) *celem Warszawy nie jest bynajmniej integralność terytorialna Ukrainy*. Polskiej polityce na Wschodzie O. Niemienskij przypisuje „syndrom imperialny": (…) *współczesna Polska to kraj z silnym syndromem postimperialnym: Polska rzuca wyzwanie w walce o swoje terytoria nie zwykłemu państwu, lecz drugiemu imperium*[17].

Przykładem gry imperialnym dziedzictwem jest też samo pojęcie r o s y j s k i ś w i a t, odwołujące się do historycznych pojęć P a x R o m a n a oraz P a x B r i t a n i c a i podkreślające w ten sposób miejsce Rosji w świecie. Podobne idee wyznaczają „linie" propagandy i interpretacji propagandowej służące jednocześnie kreowaniu nowych mitów i nowej rzeczywistości. Najbardziej nośny jest przy tym stereotyp wszechobecnego „wroga" Rosji.

[16] Na marginesie: Oleg Niemienskij jest analitykiem Centrum Badań Problemów Bliskiej Zagranicy RISI, specjalizuje się w badaniach problemów RP. Ta ciekawostka świadczyłaby albo o anachronizmie analityki resortowej, albo o roszczeniowym podejściu do RP – jako kraju „bliskiej zagranicy".

[17] О.Б. Неменский, *Польско-украинские отношения на современном этапе*, „Вопросы национальной стратегии" 2014, nr 6 (27), s. 68.

Etykietowanie i stygmatyzowanie przeciwnika

W praktyce propagandowej etykietowanie i stygmatyzowanie przeciwnika oznacza budowanie przejaskrawionego obrazu wroga, zarówno wewnętrznego („zdrajca narodu", „piąta kolumna"), jak i zewnętrznego („zgniły Zachód"). Wróg jest opisywany językiem nienawiści. Jest to praktyka rodem z KGB, oparta na czarno-białej optyce „swój–obcy". Zamknięcie społeczeństwa za żelazną kurtyną wymagało żelaznej argumentacji. Wróg był przeszkodą w realizacji „świetlanej" przyszłości, mnożył władzom trudności (amerykańscy militaryści zmuszali Rosjan do zbrojeń, a władze musiały podjąć wyzwanie, *aby tylko nie było wojny*). „Wróg" służy poprawie samooceny i jest stereotypem wyjątkowo dogodnym do manipulowania krajową i zagraniczną opinią publiczną. Jest to także sposób zastraszania własnego społeczeństwa (aby następnie zaakcentować, że państwo jest w stanie zneutralizować tego „wroga") oraz społeczeństw innych państw (aby podpowiedzieć, że mają alternatywę i gwaranta suwerenności w postaci Rosji). Wyolbrzymiane zagrożenie ze strony „wrogich sił" służy także maskowaniu swoich niepowodzeń.

Niejako „klasycznym" wrogiem w rosyjskiej propagandzie jest rusofob. Temat rusofobii jest stale podtrzymywany w dyskursie publicznym w Rosji i za granicą. (…) *Polska ma ugruntowaną w świecie opinię kraju rusofobicznego, w którym zarówno emocje zwykłych ludzi, jak i debata polityczna na temat Rosji koncentrują się nie wokół narodowych interesów, ale negatywnych emocji* – przypomniał 6 lipca 2015 r. Jakub Korejba, gość polskojęzycznego radia Sputnik. Wspomniany wyżej O. Niemienskij, tym razem jako uczestnik rozpropagowanego forum „Rusofobia i wojna informacyjna przeciwko Rosji", zorganizowanego w Moskwie w dniach 25–26 września 2015 r. przez Fundację Rozwoju Społeczeństwa Obywatelskiego „Dyplomacja Publiczna", postulował zrównanie rusofobii z antysemityzmem oraz sformułowanie międzynarodowej definicji prawnej tego pojęcia. W przyjętej rezolucji uczestnicy forum domagają się ponadto *międzynarodowego przedyskutowania i potępienia rusofobii*[18]. Postulat wprowadzenia tego tematu do debaty globalnej współbrzmi z sygnalizowanym przez nacjonalistów planem antyrusofobicznej ofensywy na arenie międzynarodowej[19]. Ta antyrusofobiczna ofensywa – jak należy sądzić – już się rozpoczęła. Powiązana z „Dyplomacją Publiczną" Międzynarodowa Organizacja Monitoringowa CIS-EMO zainicjowało np. publikację wygłoszonych na wspomnianej konferencji referatów, rozpoczynając od wystąpienia Polaka[20] potępiającego rusofobię i sugerując, że problem ten jest dostrzegany nie tylko w Rosji.

Jeśli dotąd rusofobię przypisywano głównie krajom bałtyckim i Polsce (co dla Zachodu miało być argumentem na to, że osiągnięcie porozumienia Rosji z tymi krajami jest nieosiągalne), to w ostatnich miesiącach występowanie tego zjawiska rozciągnięto na WNP, w tym także na Federację Rosyjską (rusofob jako wróg wewnętrzny) oraz, co zrozumiałe, Stany Zjednoczone – np. propagandowe wydawnictwo Eksmo wydało książkę Andrieja Cygankowa pt. *Rusofobia: antyrosyjskie lobby w USA*[21].

[18] А. Шур, *Ценности традиционно защитили*, Коммерсант.ru z 27 IX 2015 r. [online], http://www.kommersant.ru/doc/2819980 [dostęp: 28 IX 2015].

[19] А. Касмынин, *Русофобия: план наступления* [online], http://zavtra.ru/content/view/rusofobiya-plan-nastupleniya/) [dostęp: 28 IX 2015].

[20] M. Wiśniowski, *Русофобия made in Poland* [online], http://www.cis-emo.net/ru/news/vishnevskiy-rusofobiya-made-poland) [dostęp: 28 IX 2015].

[21] А. Цыганков, *Русофобия: антироссийское лобби в США*, Москва 2015.

Formatowanie mediów pod „globalną misję Rosji"

Pod koniec 2013 r. powołano międzynarodową agencję „Rosja dzisiaj" (RT), która połączyła telewizję Russia Today, radio „Gołos Rossii" i agencję RIA Novosti. Utworzony w ten sposób państwowy koncern wykorzystuje formaty multimedialne. Dynamizuje akcje informacyjne, tworząc strony na portalach społecznościowych i nowe międzynarodowe przyczółki oddziaływania sieciowego (np. Centrum Międzynarodowego Dziennikarstwa i Studiów[22] czy powstały w lipcu 2014 r. Klub Zinowjewowski[23]. W 2015 r. budżet RT zwiększono o 40 proc., co jest związane z uruchomieniem nowych kanałów: w języku niemieckim i francuskim. W listopadzie 2014 r. dyrektor generalny koncernu Jewgienij Kisielow zaprezentował dodatkowo kolejny multimedialny projekt pod nazwą „Sputnik", który scala i koordynuje z Moskwy pracę zagranicznych rozgłośni pracujących dotychczas pod marką „Gołos Rossii". Przekaz nadawany w 30 językach multiplikują wielojęzyczne portale internetowe, agencja informacyjna, radiofonia analogowa i cyfrowa oraz aplikacje mobilne. Na wzór RT radiowy przekaz propagandowy ma być dostosowany do lokalnej specyfiki – będzie szerzej korzystał z usług lokalnych dziennikarzy i liderów opinii. Prezentując ten projekt, Kisielow stwierdził: (…) *Ekskluzywna treść „Sputnika" jest przeznaczona dla miliardów odbiorców na całym świecie, którzy są zmęczeni agresywną propagandą promującą jednobiegunowy świat i którzy chcą innej perspektywy*[24]. Jak dotąd nowy portal w języku polskim (pl.sputniknews.com) nie różni się od portalu rozgłośni „Gołos Rossii" ani pod względem treści propagandowych, ani grona osób obsługujących rosyjską propagandę.

Rozwój „analityki informacyjnej"

Sądząc na podstawie informatora Rosyjskiej Rady Stosunków Międzynarodowych na temat ośrodków prowadzących badania międzynarodowe[25], Rosja jest „mocarstwem analitycznym". Wspomniane badania prowadzi tu 341 ośrodków, przy czym największym prestiżem cieszy się analityka akademicka. Warto zauważyć, że w informatorze są wymienione ośrodki analityczne i badawcze Rosyjskiej Akademii Nauk, uniwersytetów oraz tzw. niezależne centra (nie znajdziemy tu jednak służb analitycznych GRU, SWR, FSB, centrów sytuacyjnych, organów statystyki ani trudnej do oszacowania liczby komórek analitycznych działających przy prywatnych służbach bezpieczeństwa koncernów państwowych i prywatnych). Jest oczywiste, że utrzymanie monopolu informacyjnego Kremla wymaga ujednolicenia tych ośrodków. „Niepoprawne politycznie" ośrodki są w różny sposób dyscyplinowane, np. przez wstrzymanie bądź ograniczenie dotacji albo dyskredytację. Analizy „agentów zagranicznego wpływu" podjął się np. Rosyjski Instytut Studiów Zagranicznych, stygmatyzując w prawie 100-stronicowym raporcie ośrodki nieprawomyślne, np. Centrum Badania Opinii Lewady czy moskiewski oddział Carnegie[26].

Nowe zadania (monitoring, diagnozowanie i wartościowanie sytuacji z perspektywy interesów Rosji) zrodziły szczególny rodzaj analityki – analitykę informacyjną. Propaguje ją m.in. Rosyjska Szkoła Analityki, której pomysłodawcą jest płk FSB Jurij Kur-

[22] Zob. http://ria.ru/cj/.

[23] Zob. http://ria.ru/zinoviev_club/20141120/1034273877.html.

[24] *Дмитрий Киселёв представил международный проект «Спутник»* [online], http://www.ntv.ru/novosti/1261480 [dostęp: 28 IX 2015].

[25] Zob. http://ir.russiancouncil.ru/organisation/agf.

[26] Zob. http://riss.ru/analitycs/5043/.

nosow. Założenia projektu zaprezentował w swoich publikacjach książkowych[27]. Projekt ten jest oparty na jednolitej platformie metodologicznej, która (…) *umożliwi połączenie wysiłku analitycznego i skuteczne przeciwdziałanie obcej ekspansji cywilizacyjnej*. Autor stawia dwa cele: po pierwsze, stworzenie współczesnej rosyjskiej szkoły analitycznej, która (…) *ułatwi wychowanie zdrowo myślących obywateli, zdolnych do przeciwstawienia się ekspansji obcych struktur i kultur, prowadzącej do informacyjnego spustoszenia świadomości, tj. mentalnego ludobójstwa Rosjan*, po drugie zaś, ukształtowanie stałego zainteresowania tą dziedziną wiedzy oraz jej wykorzystanie w interesie publicznym. W ujawnionej na blogu www.7788.ru/rusanalytse *Koncepcji Rosyjskiej Szkoły Analityki* cele te doprecyzowano. (…) *Szkoła będzie wdrażać nowe technologie kolektywnej pracy analitycznej* (…), *co ma zabezpieczyć: przejęcie przez Rosję historycznej perspektywy przejścia do nowej sytuacji geopolitycznej, zarządzanie zhierarchizowanymi systemami społecznymi, w tym zarządzanie mechanizmami ich samoorganizacji, a także realizację projektów specjalnych*[28].

Praktyczną działalność analityczną rozwija Akademia Informacyjnej Samoobrony[29] działająca od 2008 r. pod auspicjami Rosyjskiej Akademii Nauk i Rosyjskiej Akademii Nauk Wojskowych. Wydaje ona kwartalnik „Informacyonnyje wojny", który jest zarazem projektem edukacyjnym i platformą jednoczącą specjalistów w zakresie bezpieczeństwa informacyjnego. Utytułowani analitycy wojskowi zgrupowani w działającej od 1999 r. Akademii Problemów Geopolitycznych gen. Leonida Iwaszowa[30] prowadzą badania w zakresie doktryny geopolitycznej, opracowują też projekty geopolityczne dla krajów WNP i Szanghajskiej Organizacji Współpracy. Część analityków GRU zainicjowała ponadto projekt „Akademia Zarządzania Rozwojem. Instytut Niebopolityki". Związani z nią autorzy forsują m.in. ideę „bezpieczeństwa analitycznego"[31]. Pojęcie to jest rozpatrywane na trzech poziomach (człowieka, kraju i relacji władza–społeczeństwo). Wśród funkcji analityki są wymienione m.in. mentalne odblokowanie obywateli (tj. ich zdolności do odróżniania prawdy od kłamstwa, pierwiastka narodowego od obcej naleciałości itp.) oraz analityczne odblokowanie zaufania do władz (doprowadzenie do sytuacji, w której obywatele nie odrzucają inicjatyw władz). Do parametrów określających stan bezpieczeństwa analitycznego Rosji zalicza się: samowystarczalność analityczną, wspieranie geopolitycznego projektu kraju (analityka projektowa i światopoglądowa), walkę analityczną (analityczna dezinformacja), obronę analityczną (rozpoznawanie i przeciwdziałanie dywersji analitycznej), odtwarzalność i rozwój zasobów (aktywów) analitycznych. Najbardziej aktywny przedstawiciel tej „akademii" płk Andriej Diewiatow postuluje m.in. tworzenie „analitycznych specnazów". Podkreśla także ezoteryczne korzenie rosyjskiej analityki oraz bogate tradycje, bliższe raczej analityce wschodniej niż zachodniej.

Próby rozwiązania problemu usieciowienia akcji informacyjnych

Pomysły dotyczące zarządzania krajem (i informacją) odnajdujemy także w publikacjach niezliczonej rzeszy analityków „cywilnych". Profesor W.E. Lepski proponuje

[27] J. Kurnosow, *Analityka jako broń intelektualna*, Moskwa 2012, tenże, *Algebra analityki*, Moskwa 2015 i inne.

[28] Zob. http://www.7788.ru/analytic/.

[29] Zob. www.iwars.su.

[30] Zob. akademiagp.ru.

[31] Zob. np. И. Козырев, *Сетецентрическа война* [online], www.peremeny.ru/books/osminog/8370 [dostęp: 28 IX 2015].

np. koncepcję „2. konturu strategicznego", tj. harmonijnego połączenia podejścia hierarchicznego (wertykal) i sieciowego (środowiskowego). Diagnozując bierność i apatię rosyjskiego społeczeństwa oraz brak zaufania do władz, profesor jako remedium na te bolączki zaleca *upodmiotowienie społeczeństwa*, czyli uruchomienie procesu „zbierania podmiotów"[32]. Jest oczywiste, że w rosyjskiej autorytarnej praktyce politycznej upodmiotowienie społeczeństwa nie wchodzi w grę – profesor Lepski i analitycy wojskowi szukają raczej technologii systemowego połączenia rozproszonych grup społecznościowych (niekiedy żywiołowych nacjonalistycznych, niekiedy nieprzekonanych do polityki Kremla), aby przekształcić je w silny front poparcia władz.

O ile zachodnie sieci społecznościowe są z natury rzeczy „demokratyczne" (umożliwiają swobodne wyrażanie opinii), o tyle sieci rosyjskie, powielające przekaz skonstruowany przez państwo, noszą piętno doświadczeń z czasów KGB i zimnej wojny. Technologie sieciowe dotyczą zarówno realnej, jak i wirtualnej przestrzeni informacyjnej. Struktury sieciowe są organizowane na bazie konkretnych instytucji, od góry instruowane, kontrolowane i korygowane. W praktyce ludzie podłączeni do sieci mogą mieć różne tożsamości, różne tożsamości mają także poszczególne środowiska. Nazwiska analityków stowarzyszonych w Klubie Przyjaciół Wojskowego Instytutu Języków Obcych Armii Czerwonej[33] można odnaleźć na portalach Akademii/Instytutu Niebopolityki[34], Szkoły Zdrowego Rozsądku[35], na portalu publicystów sieciowego czasopisma „Zmiany"[36], Centrum Kulturalno-Oświatowego Nowy Wiek[37]. Portale i szkoły analityczne mogą być też prowadzone przez garstkę osób, jak np. rozreklamowany w sieci www.netocracy.us, prowadzony przez małżeństwo Denisowów. Ich realizowany od 2008 r. projekt – jak czytamy – (…) *powstał na mocy decyzji i przy wsparciu najwyższych władz politycznych i wojskowych FR*. Ich działalność jest też klasycznym przejawem „maskirowki" w sieci: postronny obserwator bądź osoba zainteresowana konkretnym problemem odnosi wrażenie, że ma do czynienia ze znaczącą społecznością („potężnym podmiotem kolektywnym").

Tego rodzaju sieci, działające zgodnie z zasadą sieciowego kolektywizmu, w ramach wspólnej matrycy światopoglądowej, są ściśle scentralizowane. Innym przykładem takiej sieciówki jest istniejący od 2006 r. rusrand.ru, w nazwie pozycjonujący się jako odpowiednik amerykańskiego think tanku Rand Corporation. Internetowy adres kryje kilka ośrodków: Centrum Naukowej Myśli Politycznej i Ideologii, Centrum Analizy Problemowej i Projektowania Zarządzania Państwem, jest też adresem powstałego w 2008 r. Stowarzyszenia Eksperckiego „Rosyjski Intelekt Sieciowy". Najbardziej aktywnym uczestnikom projektu dyrektor Stowarzyszenia prof. S. Sułaszkin wręcza zaświadczenia o uczestnictwie[38]. W projektach związanych z Rusrandem uczestniczy Władimir Jakunin, były prezes Rosyjskiej Kolei. Jakunin jest także współzałożycielem Światowego Forum Społecznego „Dialog Cywilizacji" oraz Fundacji na Rzecz Wspierania Badań Historycznych i Kulturowych „Źródła". Udział W. Jakunina – byłego oficera KGB i bliskiego współpracownika prezydenta W. Putina z czasów petersburskich – w tych projektach potwierdzałby tezę o zakamuflowanych funduszach rządowych uru-

[32] W.E. Lepskij, *Analitika razwitija i razwitije analityki,* „Znanije – Włast'" 2013, nr 32 (632).
[33] Zob. www.clubvi.ru.
[34] Zob. www. nebopolitica.ru.
[35] Zob. www.shzs.info.
[36] Zob. www.peremeny.ru.
[37] Zob. www.noviyvek.org/.
[38] http://goslyudi.ru/blog/ayefremov/38333/.

chamianych za pośrednictwem koncernów państwowych. Podobne przykłady można mnożyć: powstałe w 2012 r. Centrum Badań Polityczno-Wojskowych Aleksieja Podbieriozkina[39] było np. wspólną inicjatywą Moskiewskiego Państwowego Instytutu Stosunków Międzynarodowych (MGIMO) i koncernu zbrojeniowego Ałmaz-Antiej. Konferencję „Analityka a rozwój strategiczny i bezpieczeństwo Rosji", która odbędzie się w Moskwie 22 października br. pod patronatem nowo powstałego Stowarzyszenia „Analityka"[40] współorganizują Izba Społeczna przy Prezydencie FR, Rosyjska Akademia Nauk, Akademia Nauk Wojskowych, a także Spółka Akcyjna „Wiertolioty Rossii", SA „Radioelektronika", SA „Sistiemy Uprawlenija" i inne.

Rozwój fasadowych instytucji tzw. społeczeństwa obywatelskiego

Zbudowanie przez rosyjskie państwo własnej sieci, przedstawianej przez cytowanych wyżej analityków jako *sieć sieci informacyjnych i analitycznych specnazów*, wymagało zniszczenia niezależnego od państwa sektora instytucji pozarządowych[41] i zastąpienia go instytucjami wspierającymi politykę Kremla. Wsparcie to jest budowane za pośrednictwem różnego rodzaju klubów, fundacji i stowarzyszeń intelektualistów, np. Fundacja Kultury Strategicznej, Stowarzyszenie Ekspertów Prawosławnych. Dużą aktywność w mediach, zwłaszcza w telewizji publicznej, przejawiają kluby i ośrodki partyjne, np. Państwowo-Patriotyczny Klub przy Partii Jedinaja Rossija[42] oraz działający przy tejże partii Narodowy Instytut Rozwoju Współczesnej Ideologii[43]. Ich przedstawiciele pojawiają się w mediach jako liderzy opinii. Są też inicjatorami propagandowych wydarzeń, takich jak: konferencje, marsze pokoju i koncerty. Tego rodzaju kluby i stowarzyszenia są z jednej strony platformami ideowymi do walki z liberalizmem i „atlantyzmem" oraz budowania sieci „wrogów" Zachodu (np. Klub Zinowjewowski[44], a z drugiej – do budowania sieci „przyjaciół" (np. Instytut Wysokiego Komunitaryzmu[45]). Komunitaryzm to współczesny nurt filozoficzny na Zachodzie podkreślający wagę wspólnot w społecznym życiu człowieka. Rosyjski komunitarianizm, podobnie jak większość prokremlowskich inicjatyw, jest zorientowany na efekt synergii: odwołując się do krytyki liberalizmu, zwraca się zarazem do środowisk na Zachodzie deklarujących przyjazną Rosji filozofię polityczną. Projekty te są ukierunkowane na działanie. Spektakularne akcje prowadzi Antyglobalistyczny Ruch Rosji[46]. Na zorganizowaną 20 września 2015 r. konferencję ekspercką „Dialog narodów. Prawo narodów do samostanowienia" zaprosił separatystów z Europy Zachodniej (przedstawicieli irlandzkiej Sinn Fein, włoskiego Milenium, katalońskiej Solidarności), a także separatystów z Puerto Rico, Naddniestrza, Osetii Południowej, Abchazji oraz tzw. DNR i ŁNR (odpowiednio: Donieckiej i Ługańskiej Republiki Ludowej).

[39] Zob. www.eurasian-defence.ru.

[40] Zob. http://association-analytic.ru.

[41] Zob. K. Chawryło, M. Domańska, *Obcy wśród swoich. Organizacje pozarządowe w Rosji*, „Komentarze OSW" 2015, nr 184, www.osw.waw.pl [dostęp: 28 IX 2015].

[42] Zob. http://www.gpclub.ru.

[43] Zob. http://www.nirsi.ru/.

[44] Zob. *„Зиновьевский клуб" сформирует справедливый образ России в мире*, RIA Novosti z 2 VII 2014 r. [online], http://ria.ru/religion/20140702/1014473326.html [dostęp: 28 IX 2015].

[45] Zob. http://communitarian.ru/instityt/council/.

[46] Zob. http://anti-global.ru/.

Szczególną pozycję zajmuje Klub Izborski, znany także pod nazwą Instytut Dynamicznego Konserwatyzmu[47], powołany w 2012 r. jako przeciwwaga dla Klubu Wałdajskiego. Zrzesza on naukowców (m.in. Natalię Narocznicką, Michaiła Dielagina, Siergieja Głazjewa, Władimira Owczinskiego), dziennikarzy (Michaiła Leontjewa, Maksima Szewczenkę), ideologów i działaczy (Aleksandra Prochanowa, Aleksandra Dugina, Leonida Iwaszowa, Nikołaja Starikowa), w tym działaczy cerkiewnych (archimandrytę Tichona, członka Prezydenckiej Rady ds. Kultury, którego rosyjskie media przedstawiają jako „spowiednika" W. Putina). Izborczycy popierają projekt Unii Eurazjatyckiej, widząc w nim namiastkę odrodzenia imperium. Środowisko to doprowadziło do przebicia się idei nacjonalistyczno-imperialnych, znajdujących się wcześniej na marginesie dyskursu politycznego, do jego głównego nurtu, spopularyzowało także problematykę wojen informacyjnych przez organizowanie konferencji i publikowanie raportów na ten temat. W jednym z nich czytamy:

> (…) Prawdziwa wojna cywilizacyjna (mimo iż jej atakom poddawane są reżimy polityczne, elity i biznes) toczy się o orientacje, o podstawowe wartości, kryteria dobra i zła, o rozumienie roli człowieka w świecie i obraz przyszłości (…). Stworzenie bieguna sensu (modelu człowieka, systemu sensów i wartości) da Rosji i państwom niechcącym wspierać obecnego porządku na świecie szansę obrony własnej niezależności cywilizacyjnej[48].

Szczególnie aktywne w ostatnim czasie jest środowisko związane z Fundacją Wspierania Inicjatyw Obywatelskich „Dyplomacja Publiczna" i CIS-EMO. Ta ostatnia zajmowała się dotychczas głównie monitorowaniem wyborów; zorganizowała także międzynarodową misję obserwacyjną podczas referendum na Krymie. Od 2014 r. CIS-EMO śledzi również ekstremizm w Rosji oraz „ekstremizm w ukraińskiej polityce, społeczeństwie, mediach i strukturach siłowych". W sieciach społecznościowych zainicjowała ponadto akcję „Międzynarodowa kampania na rzecz monitoringu przejawów rusofobii"[49].

Instrumentalizowanie 30-milionowej diaspory rosyjskiej

W ostatnim czasie nastąpiła zmiana podejścia Kremla do diaspory. Wcześniej rządowa agencja Rossotrudniczestwo wraz ze wspomagającą ją fundacją Russkij Mir zajmowały się głównie rejestrowaniem Rosjan za granicą i uspójnianiem działalności diaspory na jednolitych platformach koordynacyjnych w celu – jak napisano na oficjalnym portalu Rossotrudniczestwa – (…) *budowania rosyjskiej soft power, między innymi po to, by donosić prawdę o Rosji do szerokiego audytorium zagranicznego*. Dziś diaspora jest policzona (20 mln Rosjan w krajach WNP i 10 mln w krajach „dalszej zagranicy") i poinformowana o przysługujących jej prawach. Przygotowano także projekt ustawy *O Karcie Rosjanina*. Policzono osoby władające językiem rosyjskim na świecie – 260 mln, w tym 140 mln w FR. Zasięg „rosyjskiego świata" i aspekty prawne jego funkcjonowania omawiano na wspólnym seminarium Instytutu Historii Rosji RAN wraz

[47] Zob. www.dynacon.ru.

[48] К. Черемных, М. Восканян, *Анонимная война. Доклад Изборскому клубу* [online], http://www.dynacon.ru/content/articles/1467/ [dostęp: 28 IX 2015].

[49] Na temat rusofobii na Białorusi zob. www.vk.com/public103223775.

z ośrodkiem Rusrand[50]. Jego uczestnicy zaaprobowali szerszą interpretację pojęć r o s y j s k i ś w i a t i r o d a c y. Rosyjski świat – jak czytamy na portalu www.russkiymir.ru – to:

> (…) *rodacy w krajach bliskiej i dalszej zagranicy, emigranci z Rosji, ich potomkowie, zagraniczni obywatele mówiący po rosyjsku, studenci i wykładowcy języka rosyjskiego i wszyscy ci, którzy szczerze interesują się Rosją*. Analogicznie *rodakiem staje się każda osoba utożsamiająca się z „rosyjskim światem", niezależnie od narodowości i obywatelstwa. Jeśli zwróci się o pomoc do Fundacji Wspierania i Obrony Praw Rodaków za Granicą – może na nią liczyć*[51].

W 2014 r. inicjatywy rządowej agencji Rossotrudniczestwo i fundacji Russkij Mir koncentrowały się wokół wychowania patriotycznego, pamięci historycznej, szkolenia do działań w przestrzeni informacyjnej i inicjowania apeli poparcia dla władz FR po aneksji Krymu, tegoroczne – zdominowały obchody 70. rocznicy zakończenia drugiej wojny światowej i walka z rusofobią. Znalazło to m.in. wyraz podczas I Regionalnej Konferencji Rosyjskich Rodaków z Krajów Regionu Morza Bałtyckiego i Europy Północnej (Warszawa, 15–16 kwietnia 2015). W deklaracji końcowej uczestnicy wyrazili (…) *troskę w związku z polityką wrogości i wzrostem nastrojów rusofobicznych i neonazistowskich w krajach bałtyckich i krajach Europy Północnej*. Zadeklarowali (…) *kontynuację wysiłków na rzecz przeciwdziałania falsyfikacji historii drugiej wojny światowej i pomniejszania decydującego wkładu ZSRR w zwycięstwo nad nazizmem*[52].

Podsumowanie

W teorii i praktyce oddziaływania informacyjnego nagminnie jest wykorzystywana retoryka socjotechniki. Politycznym manipulacjom podlega także stosowany w debacie politycznej aparat pojęciowy. Zawiera on mnóstwo pojęć sloganów, w rodzaju „broń informacyjna", „broń cywilizacyjna", „broń historyczna", „informacyjny specnaz", „analityczny specnaz", „bezpieczeństwo analityczne" itp. Nacechowanym funkcjonalnie tego typu wyrażeniem jest także „wojna informacyjna", którym na co dzień szermują rosyjscy analitycy, politolodzy i dziennikarze. Te „zmilitaryzowane" pojęcia kształtują postawy konfrontacyjne oraz narzucają własnej i światowej opinii kremlowską wizję świata: (…) *Zachód wydał Rosji wojnę informacyjną*; *przedstawia Rosjan jako agresorów*; *sztucznie tworzy lobby rusofobów*. Grono teoretyków stosujących taki aparat pojęciowy powiększa się, symulując obraz rozbudowanego kolektywnego frontu wsparcia władz FR.

Pojęcia te pojawiły się w czasie pierwszej kadencji prezydentury W. Putina, co potwierdza tezę, że wojnę Rosji z Zachodem zaplanowano jako długofalową operację. Jest ona prowadzona zarówno na froncie zewnętrznym, jak i wewnętrznym (gdzie wykazuje zdecydowanie większą skuteczność). Fronty te cechuje brak jednej linii, mogą być rozwijane we własnym kraju i w dowolnym państwie świata; przeciwnikiem może

[50] Zob. *Правовые аспекты формирования русского мира* [online], http://rusrand.ru/docconf/pravovye-aspekty-formirovanija-russkogo-mira [dostęp: 28 IX 2015].

[51] J. Zabrodina, *Po imieni i otczestwu*, „Rossijskaja gazieta" z 10 IX 2015 r.

[52] *Россияне из Прибалтики и Северной Европы озабочены ростом русофобии*, RIA Novosti z 16 IV 2015 r. [online], http://ria.ru/world/20150416/1059072889.html [dostęp: 28 IX 2015].

być rodak, a sojusznikiem obcokrajowiec twierdzący np., że rusofobia pomaga elitom rządzącym w jego kraju utrzymać się u władzy. Na Zachodzie skuteczność tych operacji jest mniejsza. Imponująca skala działań organizacyjnych nie przesłania bowiem anachronicznych metod, wśród których podstawowymi pozostają dywersja, dezinformacja, prowokacja, specpropaganda – „brudne" dziedzictwo z czasów ZSRR. Niezbyt atrakcyjne, niewytłumaczalne na gruncie teorii realizmu politycznego są także geopolityczne koncepcje Wielkiej Eurazji czy Wielkiej Rosji.

W swym dążeniu do konfrontacji z Zachodem Rosja ma wiele atutów. Są nimi przede wszystkim własna kontrolowana przestrzeń informacyjna, rozbudowane instrumentarium socjotechniczne, zaplecze eksperckie, dziennikarskie i wykonawcze, a także wieloletnia praktyka prowadzenia operacji informacyjnych. W reakcji na zachodnią krytykę po aneksji Krymu Kreml wzmacnia swój imperialny dyskurs oraz rozbudowuje zaplecze do działań informacyjnych na Zachodzie. Zaprezentowane geopolityczne doktryny (eurazjatyzmu, „rosyjskiego świata") i projekty obliczone na budowanie na Zachodzie sieci przyjaciół Rosji oraz sieci przeciwników Zachodu są w rzeczywistości konkretnymi programami działania. Są to działania zmasowane, wykorzystujące platformy cyfrowe i upowszechniające treści zgodne z polityką Kremla. Ich celem jest nie tylko pożądane, tj. zgodne z interesami Federacji Rosyjskiej, modelowanie wewnętrznej i zagranicznej opinii publicznej. Jak pokazała aneksja Krymu, ich celem jest także kształtowanie nowej rzeczywistości.

Paradoksalnie siłą Rosji jest europejska kultura politycznego kompromisu, traktowana przez Kreml jako słabość Zachodu. Za słabość Zachodu Rosja uważa wolność mediów i pluralizm opinii. Państwa zachodnie nie mogą też wejść w instytucjonalne „starcie" informacyjne z Rosją, która działa w sposób niebezpośredni, asymetryczny pod pretekstem obrony praw człowieka czy operacji humanitarnych. Słabością Zachodu jest także słaba znajomość Rosji: przedwcześnie zlikwidował ośrodki badań sowietologicznych, ulegając jej propagandowym tezom o „partnerstwie strategicznym", „partnerstwie dla modernizacji" itp. Racjonalizuje rosyjskie idee, nie dostrzega skali dezinformacji ani stopnia symulacji rzeczywistości. Nie zauważa, że prowadzona przez Rosję „wojna informacyjna" jest wojną ideologiczną, powrotem do myślenia blokowego.

Na rosyjską propagandę na Zachodzie podatne są różne środowiska, które odnoszą odmienne korzyści (ekonomiczne – biznes; polityczne – partie radykalne krytykujące NATO, UE i USA, bo na tej krytyce zbijają kapitał polityczny). Rosyjskie oddziaływanie informacyjne skutecznie uwzględnia zachodnią specyfikę: powojenną kulturę pacyfizmu, wszelkie napięcia związane z separatyzmem czy np. napięcie w UE związane z kryzysem uchodźczym. Wykorzystuje także wszelkie napięcia wewnątrzpolityczne w poszczególnych krajach. Duch polityki ustępstw pobrzmiewa w wystąpieniach europejskich polityków, którzy podkreślają, że Rosja jest potrzebna Zachodowi do rozwiązywania problemów globalnych, przestrzegają przed *upokarzaniem Rosji* i *demonizowaniem Putina*, gdyż wzmacnia to antyzachodnie nastroje w Rosji. Takie głosy ośmielają Kreml do kontynuowania agresji, oszustwa i logiki „kto kogo przechytrzy".

U podstaw polityki ustępstw leży przekonanie, że Rosja ma prawo do obrony własnych interesów i *soft power*. Rosyjska i zachodnia *soft power* różnią się jednak w sposób zasadniczy. Nosiciele rosyjskiej *soft power* zorganizowali i sfałszowali referendum na Krymie, destabilizują wschodnie regiony Ukrainy, „upokarzają" władze Ukrainy. *Soft power* promująca określone wartości i legitymizująca politykę zagraniczną FR ma siłę niszczącą, dewastującą obce systemy wartości: otumania, straszy, podważa zaufa-

nie społeczeństw do polityki władz państw Zachodu, burzy zaufanie między państwami zachodniej wspólnoty. Przede wszystkim jednak, nie licząc się z istniejącym stanem faktycznym oraz prawem międzynarodowym, tworzy nową rzeczywistość. Rosyjskie *soft power*, organizacje społeczeństwa obywatelskiego, sieci eksperckie czy szkoły analityczne nie są odpowiednikami zachodnich tego rodzaju pojęć i instytucji. Spełniają inne funkcje – agentów Kremla do realizacji projektów specjalnych, w tym operacji informacyjnych. „Dialog kultur" w ich wykonaniu przekształca się w konfrontację z kulturą Zachodu i narzucanie światu stereotypu, że krytyka Kremla jest przejawem rusofobii. Wymuszając posłuszeństwo obywatelskie w Rosji, na Zachodzie inspirują obywatelskie nieposłuszeństwo. Są one organizowane odgórnie, wspierane finansowo przez rosyjskie państwo i przez państwo instrumentalizowane. Pogłębiają i tworzą nowe linie podziału w społeczeństwach zachodnich, co potwierdza choćby zróżnicowane stanowisko wobec działań Rosji na Ukrainie czy zastosowanych wobec Rosji sankcji.

Wchodząc w konfrontację z Zachodem, Rosja uruchomiła jednocześnie procesy, których konsekwencje ekonomiczne i polityczne mogą być odwrotne do zamierzonych (także operacja wobec Ukrainy świadczy o tym, że jej polityczne i ekonomiczne koszty zostały błędnie skalkulowane). Obecnie Rosja dąży do przełamania izolacji i poprawy relacji z Zachodem. Wydaje się, że trwała ich poprawa będzie trudna. Jeśli uważniej przeanalizuje się przyczyny powracających fal ochłodzenia w tych relacjach, to można się przekonać, że leżą one po stronie rosyjskiej elity władzy. Poprawa relacji musiałaby się wiązać ze zmianą jej percepcji rzeczywistości międzynarodowej, z odrzuceniem myślenia kategoriami polityki siły i wytyczania stref wpływów czy nowych granic cywilizacyjnych. Dopóki Rosja będzie powtarzała, że Zachód (…) *wydał jej wojnę*, *dąży do przekodowania rosyjskiego społeczeństwa*, *cynicznie i nieprofesjonalnie zdestabilizował sytuację na Ukrainie*, *dąży do rewolucji kolorowej w Rosji* (wyrażenia W. Putina), szanse na pozytywne zmiany są znikome. Stąd wniosek, że Zachód powinien przystąpić raczej do adekwatnej, skutecznej „polityki powstrzymywania". Powinna to być polityka spójna i konsekwentna.

Piotr Żochowski

Rosyjska „niewypowiedziana wojna” – konsekwencje dla sektora siłowego FR

Wasza praca (jest) *skomplikowana, sytuacja nie jest prosta. Ale Rosja, jak to mówią, jest „w marszu”, staje się silniejsza. I wiele będzie zależeć od rezultatów Waszej pracy.*

Władimir Putin do odznaczanych oficerów i prokuratorów. Kreml, 9 kwietnia 2015 r.

Kryzys ukraiński i pogwałcenie przez Rosję integralności terytorialnej Ukrainy ujawniły metody działania i potencjał rosyjskiego sektora bezpieczeństwa poza granicami kraju. Unaoczniły, że czynnik militarny jest traktowany przez Rosję jako jedno z podstawowych narzędzi osiągania celów politycznych. Upływ prawie dwóch lat od aneksji Krymu pozwala z dystansu spojrzeć na aktywność bloku siłowego FR. Czy i jak konflikt rosyjsko-ukraiński, który od końca lutego 2014 r. przerodził się w stan niewypowiedzianej wojny, wpłynął na kondycję rosyjskiego „bloku siłowego” i czy wychodzi on z niego wzmocniony, czy osłabiony?

Podejmując próbę odpowiedzi na zadane pytania, trzeba podkreślić, że sposób wykorzystania rosyjskiego sektora siłowego jest ściśle skorelowany z zadaniami polityki zagranicznej i wewnętrznej FR, a jego aktywność wpisuje się w podejmowane od wielu lat przez Kreml próby zdekonstruowania obecnego europejskiego i globalnego ładu politycznego. Głównym celem polityki wobec państw NATO i UE jest dążenie do uznania przez nie dominującej roli Rosji na obszarze poradzieckim. W stosunkach z Zachodem polityka Kremla sprowadza się do uzyskania przez Rosję pozycji państwa mającego istotny wpływ na kształt sytuacji na kontynencie europejskim w wymiarach politycznym i wojskowym oraz umocnienia stałej obecności gospodarczej. Kontekst globalny tej polityki można w uproszczeniu sprowadzić do tezy o dążeniu do odzyskania pozycji państwa zdolnego modyfikować politykę USA. Co charakterystyczne, rosyjscy politycy jednoznacznie odrzucają pojęcie „wojny hybrydowej” jako określenie charakteryzujące kroki podejmowane przez FR, stosując je jedynie do opisania rzekomej agresji Zachodu wobec Rosji, a wszystkie podejmowane przez siebie działania siłowe przedstawiają jako konieczną obronę.

Uwarunkowania i konsekwencje

Od 2000 r. decyzje związane z realizacją polityki zagranicznej i wewnętrznej FR posiadają politycy wywodzący się z rosyjskiego sektora siłowego. Warunkuje to sposób myślenia o polityce zagranicznej przede wszystkim jako operacji specjalnej, gdzie użycie siły jest jednym ze standardowych narzędzi realizacji celu. Ten sposób myślenia jest również widoczny w sposobie zarządzania bezpieczeństwem wewnętrznym kraju. Ma on charakter „kontrwywiadowczy”, ochrona społeczeństwa i aparatu państwowego

przed wpływami zewnętrznymi stała się fundamentalnym zadaniem sektora bezpieczeństwa. W praktyce tego rodzaju podejście ograniczyło się do uznania represyjności i indoktrynacji jako podstawowych instrumentów kontroli społeczeństwa.

Najbardziej istotną zmianą, która nastąpiła w rosyjskim sektorze bezpieczeństwa od 2014 r., jest jego otwarte włączenie do systemu bezpieczeństwa militarnego Rosji. Od początku 2013 r. Siły Zbrojne FR, realizujące nieprzerwanie kolejne zadania szkoleniowe obejmujące rotacyjnie kolejne regiony Rosji, znajdują się w stanie permanentnej gotowości bojowej. Aktywności sił zbrojnych towarzyszyło angażowanie instytucji siłowych, wspomagających działania różnych rodzajów wojsk. Zwiększono też zakres ćwiczeń związanych z mobilizacją administracji cywilnej i weryfikacją zdolności jej funkcjonowania w czasie wojny.

Z przyczyn oczywistych wzrosła aktywność wywiadowcza. Otwarcie przez Rosję frontów konfliktu i rywalizacji od Arktyki po basen Morza Śródziemnego nasuwa pytanie, czy Służba Wywiadu Zagranicznego jest w stanie zachować wystarczającą zdolność informacyjną. Ujawnione w państwach bałtyckich zaangażowanie FSB w wywiad polityczny może świadczyć o tym, że służba ta, zajmująca się dotąd działalnością wywiadowczą jedynie w państwach WNP, prowadzi obecnie działalność operacyjną na terytorium wszystkich państw sąsiadujących z Rosją.

Wzrosło znaczenie aktywności w sferze tzw. wojny informacyjnej inspirowanej przez blok siłowy. Podczas konfliktu na Ukrainie wykorzystywanie przez Rosję znanych wcześniej metod związanych m.in. z dezinformacją czy oddziaływaniem psychologicznym na społeczeństwo przeciwnika ułatwiło realizację zadań wykonywanych przez siły zbrojne bądź służby specjalne[1]. Posłużyły one również jako środek do wyolbrzymiania zaangażowania resortów siłowych i skali ich oddziaływania na umownego przeciwnika. W tym kontekście specyficzną rolę odgrywa polityka informacyjna rosyjskich mediów mająca ugruntować u odbiorcy przekonanie, że rywalizacja z Rosją jest skazana na porażkę i może się spotkać ze zdecydowaną, brutalną odpowiedzią.

Analizując aktywność rosyjskich instytucji bezpieczeństwa zarówno na obszarze innych państw, jak i w samej Rosji, można stwierdzić, że nowe zadania nie spowodowały istotnych modyfikacji w ich systemie. Jak do tej pory nie doszło do zmian strukturalnych mogących świadczyć o jego złym funkcjonowaniu, a zmiany organizacyjne były rezultatem dostosowywania się do aktualnych wyzwań. Również kryzys finansowy, który wymógł na władzach wprowadzenie cięć budżetowych, w ograniczony sposób dotknął blok siłowy, w praktyce redukcje kadrowe odnotowano w resorcie spraw wewnętrznych. Co prawda większość resortów siłowych zadeklarowała redukcje budżetowe i kadrowe, ale zapowiedzi te nie zostały do tej pory zrealizowane. Świadczy to o tym, że kwestie cięć finansowych w bloku siłowym należy traktować jako element polityki medialnej władz zapewniających, że w obliczu kryzysu wszystkie instytucje państwowe wprowadzają programy oszczędnościowe.

Nie zmieniły się również zasady polityki kadrowej. Na szczeblu lokalnym nadal jest stosowana zasada „karuzeli", czyli okresowe przenoszenie funkcjonariuszy do innych regionów kraju. W tym kontekście dużym wyzwaniem pozostaje obsadzenie struktur siłowych anektowanego Krymu osobami cieszącymi się ograniczonym zaufaniem byłych pracowników służb ukraińskich. Uboczną konsekwencją wzmożonej aktywności

[1] Szerzej zob. J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku* [online], http://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2014-05-22/anatomia-rosyjskiej-wojny-informacyjnej-operacja-krymska [dostęp: 8 X 2015].

resortów siłowych są sygnały o przypadkach rywalizacji między nimi o wzmocnienie swojej pozycji w systemie bezpieczeństwa państwa. Za przejaw sytuacji konfliktowych można uznać pogłoski o likwidacji jako samodzielnych podmiotów Federalnej Służby Kontroli Obrotu Narkotykami czy Federalnej Służby Migracyjnej i przejęciu ich przez FSB bądź MSW. Kolejnym przykładem jest skuteczne sabotowanie przez inne resorty wspieranego przez Ministerstwo Obrony projektu ustawy o legalizacji prywatnych firm wojskowych mających prawo do działania poza granicami Rosji. Ambicje poszczególnych graczy są ostatecznie hamowane przez Kreml, choć nie oznacza to, że szefowie poszczególnych instytucji zrezygnują z chęci wykorzystania kryzysu międzynarodowego do umocnienia własnej pozycji w elicie władzy.

Usztywnienie podejścia doktrynalnego, poszerzenie katalogu zadań

Konsekwencją konfliktu z Ukrainą było skorygowanie percepcji zagrożeń w rosyjskim myśleniu doktrynalnym opartym na fundamentalnym założeniu, że Rosja stała się obiektem agresji Zachodu, i uznanie czynnika militarnego za trwały element instrumentarium polityki zagranicznej. Przejawem tego było opublikowanie 29 grudnia 2014 r. na nowo zredagowanej *Doktryny wojennej Federacji Rosyjskiej*. Konieczność dokonania zmian w dokumencie przedstawiciele resortu obrony FR uzasadniali m.in. stosowaniem przez Zachód nowych metod walki z Rosją mających charakter wojny hybrydowej[2]. Zmusiło to stronę rosyjską do opracowania (...) *nowych, nietradycyjnych metod łączących środki wojskowe i niewojskowe w czterowymiarowej przestrzeni walki*[3]. Położenie akcentu na tzw. środki niewojskowe świadczy o usankcjonowaniu doktrynalnym pozycji tzw. cywilnych służb specjalnych i innych resortów siłowych jako podmiotów funkcjonujących w logice kompleksu działań militarnych, a często odgrywających w nich główną rolę[4]. W tekście doktryny dokonano również korekt wprowadzających listę potencjalnych zagrożeń wewnętrznych, których eliminacja jest bezpośrednio związana z realizacją ustaw kompetencyjnych resortów siłowych[5]. Charakterystyczne jest również to, że uzupełniając katalog zagrożeń zewnętrznych, uwzględniono obszary dotąd niekojarzone z zagrożeniem militarnym. Są nimi np.: działalność dywersyjna obcych służb specjalnych, oddziaływanie informacyjne na ludność, przede wszystkim na młodych obywateli, mające na celu podważenie historycznych, duchowych i patriotycznych tradycji obrony ojczyzny czy prowokowanie napięć społecznych.

[2] *Военная доктрина Российской Федерации* [online], http://www.rg.ru/2014/12/30/doktrina-dok.html [dostęp: 8 X 2015].

[3] Tamże.

[4] W dokumencie można napotkać opis potencjalnych działań, których realizacja wymusza udział służb specjalnych. Są to m.in.: „(...) kompleksowe użycie sił zbrojnych, jak również politycznych, ekonomicznych, informacyjnych i innych środków niewojskowych, realizowanych przy szerokim wykorzystaniu potencjału protestu i sił operacji specjalnych; wpływanie na przeciwnika na całej głębokości jego terytorium, w globalnej przestrzeni informacyjnej, w przestrzeni powietrzno-kosmicznej, na lądzie i morzu; udział w działaniach wojennych nieregularnych formacji zbrojnych i prywatnych firm wojskowych; stosowanie niebezpośrednich i asymetrycznych metod działań; wykorzystanie sił politycznych i ruchów społecznych finansowanych i zarządzanych z zewnątrz".

[5] Do zagrożeń wewnętrznych zaliczono: działalność zorientowaną na obalenie ustroju konstytucyjnego Federacji Rosyjskiej siłą, destabilizację sytuacji wewnątrzpolitycznej i społecznej w kraju, dezorganizację funkcjonowania organów władzy państwowej, ważnych obiektów państwowych i wojskowych oraz infrastruktury informacyjnej; działalność organizacji terrorystycznych i poszczególnych osób, ukierunkowaną na naruszenie suwerenności i integralności terytorialnej Federacji Rosyjskiej.

Analizując rosyjskie dokumenty doktrynalne i uwzględniając przy tym ich rolę propagandową wpisującą się w schemat odstraszania przeciwnika, warto podkreślić, że wprowadzane w nich zmiany świadczą o sposobie myślenia elit siłowych. Nadal podkreślają one swoją rolę w utrzymaniu stabilności systemu politycznego oraz dbają, aby przy podejmowaniu decyzji politycznych czy gospodarczych szczególne znaczenie miało uwzględnianie potencjalnych zagrożeń. Utrzymanie stworzonego przez siebie autorytarnego systemu politycznego elity polityczne uznają za cel gwarantujący zachowanie silnej pozycji Rosji na świecie[6]. Równie ważne jest podejście do zagrożeń wewnętrznych – trwałe przyjęcie tezy o naruszeniu przez Zachód żywotnych interesów Rosji nasiliło aktywność służb specjalnych dążących do izolowania społeczeństwa od wpływów zewnętrznych.

O praktycznym podejściu rosyjskiego bloku siłowego do bieżących problemów bezpieczeństwa państwa świadczy katalog zagadnień objętych tzw. priorytetem operacyjnym[7]. Ich hierarchia jest ustalana w ogólnych zarysach przez Radę Bezpieczeństwa FR i akceptowana przez Kreml. Tradycyjnie główne zadania bloku siłowego formułuje prezydent i wyżsi urzędnicy państwowi podczas dorocznych spotkań z kierownictwami poszczególnych resortów[8]. Większość z nich to zadania standardowe, m.in. walka z korupcją, zorganizowaną przestępczością czy też kontynuowanie współpracy ze służbami partnerskimi (w tym kontekście wymieniana jest Białoruś i Kazachstan). Wzrósł udział służb specjalnych w prowadzeniu tzw. wojny informacyjnej. Niektóre obszary aktywności nabrały szczególnego znaczenia po rozpoczęciu konfliktu z Ukrainą. Poniżej omówiono niektóre z nich.

Neutralizacja struktur ekstremistycznych

Przeciwdziałanie ekstremizmowi stało się w omawianym okresie jednym z głównych przejawów aktywności FSB i MSW na terytorium Rosji. Hasło zwalczania ekstremizmu politycznego jest świadomym zabiegiem służb mającym w ich mniemaniu z jednej strony zakamuflować działania charakterystyczne dla policji politycznej, a z drugiej budować atmosferę zagrożenia zewnętrznego – ekstremizm zazwyczaj jest przedstawiany jako zjawisko o obcych, nierosyjskich korzeniach. Definicja ekstremizmu jest interpretowana przez rosyjskie służby bardzo szeroko i w praktyce wszystkie przejawy nieposłuszeństwa zagrażające stabilności politycznej państwa mogą zostać zakwalifikowane do tej kategorii przestępstwa. W dużej mierze realizacja tego zadania ma charakter polityki ograniczania aktywności społecznej, m.in. związanej z krytyką postępowania władz. Z inicjatywy resortów siłowych zaostrzono penalizację przestępstw ekstremistycznych. Rozważa się również wzmocnienie komórek zwalczających ekstremizm w MSW. Na początku lutego i w czerwcu 2015 r. wprowadzono zmiany do kodeksu karnego zwiększające karę za *organizację stowarzyszenia ekstremistycznego* czy wzywanie do działalności ekstremistycznej za pośrednictwem Internetu z trzech do sześciu lat pozbawienia wolności. O znaczeniu zwalczania ekstremizmu w katalogu priorytetów sektora siłowego świadczy podpisanie przez prezydenta *Strategii przeciwdziałania ekstremizmowi do 2025 r.*[9]

[6] Szerzej zob. J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji* [online], http://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2015-05-19/diabel-tkwi-w-szczegolach-wojna-informacyjna-w-swietle-doktryny [dostęp: 8 X 2015].

[7] Katalog priorytetów został opracowany na podstawie rozproszonych wypowiedzi rosyjskich polityków i przedstawicieli kierownictwa służb specjalnych kolportowanych w mediach od marca 2014 r.

[8] M.in. wystąpienie prezydenta FR na kolegium FSB w marcu 2015 r., zob. *Заседание коллегии ФСБ* [online], http://kremlin.ru/events/president/news/49006 [dostęp: 8 X 2015].

[9] Szerzej zob. artykuł w niniejszej publikacji autorstwa J. Darczewskiej, *Rosyjska strategia walki*

Zwalczanie terroryzmu

W omawianym okresie znacznie spadło zagrożenie aktywnością terrorystyczną na obszarze Kaukazu Północnego i w regionach południowych FR. Jest to wynik zarówno zintensyfikowanych działań o charakterze antyterrorystycznym, jak i nasilającego się dołączania osób zaangażowanych w terroryzm do formacji działających pod egidą ISIS. W konsekwencji została zmarginalizowana rola Emiratu Kaukaskiego jako organizacji zbrojno-terrorystycznej i projektu politycznego (niepodległe państwo islamskie obejmujące cały Kaukaz Północny)[10]. Zagrożenie wsparciem ISIS przez obywateli FR zostało nagłośnione przez kierownictwo służb i stało się elementem wspierającym działania dyplomatyczne na rzecz udziału Rosji w rozwiązywaniu konfliktu na Bliskim Wschodzie. Według informacji przekazanych przez szefa FSB Aleksandra Bortnikowa w szeregach ISIS walczy około 2400 obywateli FR i 3000 obywateli państw poradzieckiej Azji Centralnej[11]. Odnotowano przy tym informacje, że są prowadzone działania filtrujące środowiska deklarujące sympatię dla islamu. Wejście Rosji w aktywną fazę konfliktu syryjskiego nadało problematyce walki z terroryzmem szczególnego znaczenia, nie jest przy tym wykluczone, że służby rosyjskie od dłuższego czasu infiltrują szeregi ISIS, wykorzystując do tego mieszkańców Czeczenii i współpracując ze służbami kontrolowanymi przez Ramzana Kadyrowa.

Działania kontrwywiadowcze

Kwestie przeciwdziałania aktywności obcych wywiadów (ze szczególnym uwzględnieniem zwalczania zachodnich służb specjalnych) to podstawowe zadanie FSB stanowiące wizytówkę jej działalności. Elementem działań kontrwywiadowczych pozostaje paraliżowanie zagranicznych organizacji pozarządowych, których aktywność jest jednoznacznie uznana za sprzeczną z interesem państwa.

Od 2014 r. aktywność kontrwywiadu FSB jest elementem propagandy państwowej mającej utrwalić w społeczeństwie wizerunek przeciwnika. W tym celu są nagłaśniane wybrane operacje kontrwywiadowcze, których przedmiotem jest zwalczanie aktywności służb państw NATO. Przykładem takiej sprawy było uprowadzenie jesienią 2014 r. oficera estońskich służb specjalnych Estona Kohvera. Charakterystyczne, że operacja FSB była skorelowana z kalendarzem wydarzeń politycznych. Do uprowadzenia doszło tuż po zakończeniu wizyty prezydenta USA w Tallinie i w trakcie trwania szczytu NATO, a incydent został wykorzystany do nasilenia propagandy antyzachodniej. Nie był to pierwszy przypadek realizowania operacji kontrwywiadowczej w kontekście wydarzeń politycznych. W maju 2013 r. FSB zatrzymała w Moskwie amerykańskiego dyplomatę pod zarzutem próby werbunku oficera rosyjskich służb specjalnych. Nastąpiło to po zamachu terrorystycznym w Bostonie i po pierwszych sygnałach o możliwości aktywizacji przez USA dialogu z Rosją.

z ekstremizmem w teorii i praktyce, s. 59–73.

[10] Szerzej zob. M. Falkowski, *Kaukaz Północny, między Rosją, Emiratem a Kalifatem* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2015-07-01/kaukaz-polnocny-miedzy-rosja-emiratem-i-kalifatem [dostęp: 8 X 2015].

[11] *Some 2,400 Russians and 3,000 Central Asia citizens fighting for ISIL* [online], http://rbth.co.uk/news/2015/09/18/some_2400_russians_and_3000_central_asia_citizens_fighting_for_isil_49356.html [dostęp: 8 X 2015].

Wywiad zagraniczny

Głównymi zadaniami wywiadu rosyjskiego pozostają: działania na rzecz tworzenia grup wpływu wspierających rosyjskie interesy, prowadzenie wywiadu politycznego oraz wspieranie rozwiązań biznesowych pozwalających umieszczać rosyjskie aktywa poza granicami kraju. Nowym wyzwaniem dla rosyjskich służb wywiadowczych jest sytuacja operacyjna na Ukrainie. Po zerwaniu kontaktów z ukraińskimi instytucjami bezpieczeństwa ich infiltracja jest utrudniona, a sama Ukraina jest uznawana przez rosyjskie służby jako miejsce rywalizacji ze służbami zachodnimi. W kontekście realizacji zadań wywiadowczych istnieje nadal podział „regionalny". Wywiad na terytorium poradzieckim prowadzi Federalna Służba Bezpieczeństwa przy niewielkim wsparciu Służby Wywiadu Zagranicznego, która koncentruje swoją uwagę na państwach niewchodzących w bezpośrednią strefę wpływów Rosji.

Stworzenie zintegrowanego systemu informacyjnego oraz systemu wykrywania, uprzedzania i odpierania ataków komputerowych na państwowe zasoby informacyjne FR

Zwalczanie zagrożeń cybernetycznych oraz kwestia kontroli Internetu jest jednym z podstawowych zadań rosyjskich służb specjalnych. W omawianym okresie odnotowano dwa wydarzenia mające wpływ na sprawy organizacyjne związane z tą sferą. W dniu 12 grudnia 2014 r. Władimir Putin zatwierdził przygotowaną przez Radę Bezpieczeństwa FR *Koncepcję państwowego systemu wykrywania, zapobiegania i likwidacji skutków ataków komputerowych na zasoby informacyjne FR*. Zgodnie z założeniami dokumentu główny ciężar odpowiedzialności za zapewnienie sprawnego funkcjonowania systemu spoczywa na FSB. Zwraca jednak uwagę, że choć ma być on oparty na sieci organizacyjnej centrów bezpieczeństwa komputerowego FSB, to jego istotnymi elementami mają być podobne struktury znajdujące się w dyspozycji innych organów państwowych. Taki model organizacyjny, nieprzesądzający o nadrzędnej roli FSB, będzie rodził konflikty kompetencyjne, a w rezultacie może osłabić sprawność modelu systemowego. Na możliwość wystąpienia tego rodzaju zakłóceń wskazuje również analiza kolejnego dokumentu. W dniu 22 maja 2015 r. prezydent FR podpisał dekret *O niektórych problemach bezpieczeństwa informacyjnego FR*. Zapowiedziano w nim podjęcie działań na rzecz stworzenia i zabezpieczenia informatycznego segmentu Internetu przeznaczonego dla instytucji państwowych FR. Zgodnie z posiadanymi kompetencjami za realizację tego zadania ma odpowiadać wyłącznie Federalna Służba Ochrony i wchodząca w jej skład Służba Łączności Specjalnej.

Integracja Krymu

Aneksja Krymu i wzmocnienie Floty Czarnomorskiej postawiły szczególne zadania przed rosyjskim blokiem siłowym. Są nimi: przymuszenie społeczeństwa do integracji z Rosją, wspieranie deukrainizacji Krymu przez utrudnianie kontaktów transgranicznych, marginalizowanie tendencji autonomicznych reprezentowanych przez krymskich Tatarów, ochrona kontrwywiadowcza sił zbrojnych oraz zbudowanie przyczółka regionalnej aktywności wywiadowczej. Specyficznym problemem jest sposób wykorzystania byłych funkcjonariuszy ukraińskich struktur siłowych, którzy przyjęli propozycje pracy w instytucjach rosyjskich. Większość pracowników służą-

cych w ukraińskim MSW kontynuuje pracę w strukturach rosyjskiego odpowiednika, zajmując stanowiska w kierownictwie zarządu regionalnego. Inna sytuacja rysuje się w FSB, gdzie byli funkcjonariusze SBU są traktowani nieufnie, a często kieruje się ich do pracy w innych regionach Rosji.

Sektor bezpieczeństwa – trwałość systemu, minimalizowanie strat

Jak wspomniano na wstępie niniejszego artykułu, konflikt na Ukrainie nie spowodował zmian w systemie bezpieczeństwa FR, którego konstrukcja jest trwała, a jego hipotetyczne modyfikacje mogą nastąpić jedynie w wyniku narastania złej sytuacji finansowej w Rosji czy też trudnej do przewidzenia walki o wpływy w elitach siłowych. Hierarchia odzwierciedlająca znaczenie każdej ze służb wiąże się z posiadanymi kompetencjami oraz stawianymi zadaniami, a zmiany zachodzące wewnątrz służb nie sygnalizują poważniejszych korekt[12]. Analizując jawne informacje dotyczące aktywności poszczególnych instytucji, uwzględniając przy tym stopień ich zaangażowania w działania poza granicami oraz ich aktywność na obszarze Rosji, można podjąć próbę krótkiej oceny bieżącej sytuacji w każdej z nich.

Federalna Służba Bezpieczeństwa (FSB). Pozostaje służbą o najszerszym obszarze kompetencyjnym, obejmującym całościową kontrolę systemu politycznego, ekonomicznego i społecznego FR. Pozycja jej szefa, urzędującego od 2008 r. Aleksandra Bortnikowa, jest nadal silna. Należy on do wąskiej elity politycznej, co potwierdza sprawowanie przez niego funkcji stałego członka Rady Bezpieczeństwa FR.

Najbardziej istotną zmianą kadrową, do jakiej doszło w kierownictwie FSB, była zmiana na stanowisku szefa kontrwywiadu. Objął je 7 kwietnia 2015 r. 55-letni Władisław Mienszczikow, dotychczasowy szef Głównego Zarządu Programów Specjalnych przy prezydencie FR (GUSP). Jego poprzednik, 62-letni Oleg Syromołotow, został w marcu br. skierowany do MSZ, gdzie objął funkcję wiceministra ds. przeciwdziałania terroryzmowi. Mianowanie Mienszczikowa jest przykładem trwałości modelu zmian kadrowych w rosyjskich służbach. Obsada kluczowego pionu w FSB była konsultowana z szefem Administracji Prezydenta FR Siergiejem Iwanowem, a sam mianowany pochodzi z Petersburga, gdzie w latach 90. XX w. nawiązał kontakt z członkami obecnej kremlowskiej elity. Przejście jego poprzednika do MSZ jest przykładem angażowania ludzi wywodzących się ze służb specjalnych do realizacji zadań politycznych. Walka z terroryzmem, jak również próby intensyfikowania współpracy w tej dziedzinie z USA i innymi partnerami zachodnimi mają służyć przełamywaniu izolacji Rosji.

Konflikt na Ukrainie, który zaangażował struktury FSB w bezpośrednie działania w Donbasie, ujawnił zdolność ofensywną tej służby. Z informacji ukraińskich służb wynika, że FSB nadal prowadzi szeroko zakrojone operacje dywersyjne i wywiadowcze na terytorium Ukrainy. Na terenie Donbasu odnotowano obecność funkcjonariuszy FSB uczestniczących w organizacji samozwańczych struktur bezpieczeństwa, a także podejmujących działania je dyscyplinujące, włącznie z aresztowaniami osób niepoddających się kontroli rosyjskich służb. FSB poszerza również zakres działań o prowadzenie wywiadu, nie tylko w państwach WNP. Zostało to ujawnione po zatrzymaniu przez litewskie służby obywatela Litwy, pozyskanego do współpracy przez FSB w obwodzie kaliningradzkim, który otrzymał zadania wywiadowcze.

[12] Szerzej zob. J. Darczewska, P. Żochowski, *Rola służb specjalnych w systemie politycznym FR*, *Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne,* Z. Nawrocki (red.), Warszawa 2013, s. 7–30.

W wymiarze wewnętrznym FSB stale wykorzystuje swoją silną pozycję w strukturze służb do poszerzania swoich kompetencji. Przykładem potwierdzającym tę tezę jest wprowadzenie pod koniec czerwca 2015 r. zmian do ustawy *O działalności operacyjno-rozpoznawczej* dotyczących organizacji przedsięwzięć związanych z prowadzeniem tajnej obserwacji[13]. Resortom uprawnionym do prowadzenia tego rodzaju działań pozostawiono prawo do samodzielnej organizacji obserwacji zewnętrznej, wszystkie natomiast przedsięwzięcia związane z zastosowaniem techniki operacyjnej oraz kontroli środków łączności mają być uzgadniane bądź realizowane przy wykorzystaniu potencjału technicznego FSB. Uboczną konsekwencją tego rozwiązania, jak należy zakładać, będzie poszerzenie wiedzy FSB co do przedmiotu spraw operacyjnych prowadzonych przez MSW, FSKN czy służbę celną.

Służba Wywiadu Zagranicznego (SWR). Aktywność tej służby została objęta ścisłą ochroną kontrwywiadowczą. Od 2011 r., kiedy to przeprowadzono akcję promowania współpracującej z rosyjskim wywiadem, a wydalonej z USA Anny Chapman, SWR nie przeprowadza operacji wizerunkowych. Jedyne informacje o jej aktywności, jakie przedostają się do otwartej przestrzeni publicznej, pochodzą z jawnych raportów zachodnich służb specjalnych. Zawarte w nich informacje wskazują, że zainteresowania operacyjne SWR pozostają niezmienne. Uwzględniając specyfikę każdego z państw, koncentruje ona swoje działania na prowadzeniu klasycznego wywiadu politycznego i gospodarczego, inspiruje miejscowe elity intelektualne do propagowania tez zbieżnych z interesami Rosji oraz jest zaangażowana w działania dezinformacyjne realizowane za pomocą kontrolowanych środków informacji.

Od 2007 r. szefem SWR pozostaje 65-letni Michaił Fradkow (uprzednio premier FR). Jak dotąd nie pojawiły się spekulacje co do możliwości mianowania jego następcy. Biorąc jednak pod uwagę wiek Fradkowa, nie jest wykluczone, że w najbliższym czasie dojdzie do zmiany na stanowisku szefa tej służby.

Główny Zarząd Wywiadowczy (GRU). Podobnie jak w przypadku SWR, aktywność GRU nie jest ujawniana, a wszelkie informacje o kierunkach jej zainteresowań pochodzą ze źródeł zewnętrznych. Pozycja służby w systemie pozostaje niezmienna. Od grudnia 2011 r. szefem GRU jest 58-letni Igor Siergun służący w wywiadzie wojskowym od 1984 r. W dniu 21 lutego 2015 r. został on awansowany do stopnia generała pułkownika, a awans ten można interpretować jako wyraz pozytywnej oceny aktywności służby w czasie kryzysu ukraińskiego.

Pod względem organizacyjnym GRU podlega szefowi Sztabu Generalnego (SG) i jest zadaniowany przez szefa SG i ministra obrony. Do jego zadań należy m.in. pozyskiwanie informacji istotnych z punktu widzenia potencjału obronnego i bezpieczeństwa FR, zwłaszcza pozyskiwanie nowych technologii i wspieranie eksportu rosyjskiego uzbrojenia. W stałym zainteresowaniu GRU pozostaje również rozpoznawanie sytuacji w sferze międzynarodowego terroryzmu, m.in. badanie źródeł finansowania organizacji terrorystycznych[14]. Konflikt na Ukrainie ujawnił wykorzystanie operacyjne jednostek (brygad) specnazu GRU jako istotnego komponentu batalionowych grup taktycznych wspierających rebeliantów oraz powierzanie im

[13] *Федеральный закон Российской Федерации от 29 июня 2015 г. N 170-ФЗ „О внесении изменения в статью 4 Федерального закона «Об оперативно-розыскной деятельности»* [online], http://m.rg.ru/2015/07/03/zuchok-dok.html [dostęp: 8 X 2015].

[14] *Начальник ГРУ рассказал о доходах радикальных исламистов от наркоторговли* [online], http://lenta.ru/news/2015/04/16/narco/ [dostęp: 8 X 2015].

zadań dywersyjnych (głównie związanych z paraliżowaniem szlaków komunikacyjnych na zapleczu frontu).

Federalna Służba Ochrony (FSO). Służba zachowuje kluczową pozycję w sferze ochrony obiektowej i fizycznej funkcjonariuszy państwa i zarządza kompleksem łączności specjalnej federalnych oraz regionalnych organów władzy państwowej. Duże znaczenie dla zapewnienia sprawnego przepływu informacji mają regionalne centra łączności specjalnej podlegające wchodzącej w skład FSO autonomicznej Służbie Łączności Specjalnej. Szczególny status zajmuje także będąca częścią FSO Służba Bezpieczeństwa Prezydenta (SBP). Od 2000 r. dyrektorem FSO jest 69-letni (!) Jewgienij Murow. Od początku 2014 r. nie odnotowano wydarzeń świadczących o zmianie profilu służby, nie doszło również do zmian organizacyjnych. Poszerzane są jej kompetencje związane z zarządzaniem rządowym segmentem Internetu oraz ochroną jego bezpieczeństwa.

Federalna Służba Kontroli Obrotu Narkotykami (FSKN). Pozostaje sprofilowaną służbą, posiadającą specjalne pełnomocnictwa do zwalczania przestępczości narkotykowej i zapobiegania narkomanii. Od 2008 r. służbą kieruje 65-letni Wiktor Iwanow. Służbę dotknęły efekty kryzysu finansów publicznych Rosji, który wymusił na władzach podjęcie kroków oszczędnościowych. W lipcu 2014 r. zapowiedziano 10-procentowe redukcje kadrowe w FSKN (ok. 3000 etatów), których wymiar został zaakceptowany przez szefa służby. Sytuację tę próbował wykorzystać szef MSW Władimir Kołokolcew. Na przełomie lat 2014 i 2015 rosyjskie media obiegła informacja, że w porozumieniu z resortem finansów zaproponował on likwidację FSKN jako samodzielnej służby i włączenie jej do struktury MSW. Na początku marca 2015 r. Kreml podjął decyzję o zachowaniu służby w istniejącym kształcie[15]. Odrzucenie planów W. Kołokolcewa wiązało się bezpośrednio z korzyściami, jakie płyną z aktywności międzynarodowej FSKN. Jej samodzielność pozwala na podejmowanie inicjatyw w zakresie współpracy międzynarodowej, co służy, podobnie jak w przypadku walki z terroryzmem, przełamywaniu izolacji politycznej Rosji.

Główny Zarząd Programów Specjalnych Prezydenta FR (GUSP). Jak dotąd informacje o służbie realizującej zadania związane z przygotowaniami mobilizacyjnymi i zarządzaniem kryzysowym w czasie wojny i sytuacji nadzwyczajnych były objęte ścisłą tajemnicą. Przejawem militarnego podejścia do funkcjonowania instytucji państwowych było medialne nagłośnienie aktywności GUSP. W 2015 r. przy okazji manewrów wojskowych odbywających się w środkowej Rosji ujawniono, że struktury GUSP przeprowadziły próbną ewakuację i rozproszenie lokalnych organów państwowych do zapasowych ośrodków pobytu.

Ministerstwo Spraw Wewnętrznych. Choć MSW tradycyjnie nie jest zaliczane do kategorii służb specjalnych, to w istocie jego działalność często ma charakter wspomagający ich aktywność. Resort ten równolegle do FSB zajmuje się zwalczaniem ekstremizmu politycznego, co sprawia, że trudno traktować MSW jako instytucję policyjną, do której zadań należy jedynie ochrona porządku publicznego. O systemowej sile MSW decyduje również posiadany potencjał o znaczeniu militarnym, jaki stanowią Wojska Wewnętrzne MSW (WW MSW). Od chwili mianowania w 2013 r. ich dowódcą, a później również I zastępcą szefa resortu byłego szefa Służby Bezpieczeństwa Prezydenta FR Wiktora Zołotowa nie ustają spekulacje co do wpływu tej nominacji

[15] Н. Березина, Е. Антонова, *Виктор Иванов поставил точку в истории с ликвидацией ФСКН* [online], http://top.rbc.ru/politics/06/03/2015/54f96e519a7947ec467900ad [dostęp: 8 X 2015].

na rozwój sytuacji w resorcie. Abstrahując od typowych interpretacji zapowiadających zmiany kadrowe w kierownictwie, aktywność W. Zołotowa była związana z uporządkowaniem sytuacji w wojskach wewnętrznych. Ich pozycja w strukturze instytucji bezpieczeństwa została umocniona, czego przejawem jest brak cięć budżetowych i kadrowych dotykających MSW oraz stałe zakupy nowego sprzętu. Część rosyjskich mediów rozpowszechnia opinię, że poprawiająca się kondycja liczących 170 tys. ludzi WW MSW jest oznaką przygotowywania się Kremla do potencjalnych protestów społecznych. Obserwacja aktywności szkoleniowej formacji prowadzi jednak do wniosku, że od początku 2014 r. została ona włączona do planu mobilizacji sił zbrojnych i jest przygotowana do działań stricte militarnych. W kwietniu 2015 r. wojska wewnętrzne (40 tys. ludzi) brały udział w manewrach „Zasłon 2015", podczas których przy wykorzystaniu ciężkiego sprzętu bojowego ćwiczono walkę uliczną w miejscowościach opanowanych przez „umownych terrorystów".

Ministerstwo Spraw Wewnętrznych, jako najliczniejszy resort (około 1 100 000 funkcjonariuszy, bez wojsk wewnętrznych), stało się obiektem najbardziej dotkliwych z pozoru redukcji kadrowych spowodowanych kryzysem finansowym. Cięcia, które miały objąć 100 000 etatów, zostały zredukowane do 70 000. Nie jest przy tym jasne, czy dokonane w ten sposób oszczędności finansowe zmniejszyły deficyt budżetowy, czy też środki te nie zostały przeniesione do innych działów budżetu związanych z finansowaniem bloku siłowego. Z drugiej strony trudno mówić o znaczącym osłabieniu MSW, bardziej właściwe wydaje się mówienie o optymalizacji struktury. Zlikwidowano pion ochrony obiektów pozaresortowych, nieodgrywający istotnej roli w kontekście zadań operacyjnych resortu. Zwolnieni funkcjonariusze w większości zasilili prywatne agencje ochroniarskie kontrolowane przez MSW. Wymiar redukcji w organach milicji został osłabiony przez wyłączenie z niej części regionalnych struktur MSW (np. nie dotyczyły one organów spraw wewnętrznych anektowanego Krymu).

Fiasko legalizacji prywatnych firm wojskowych

Kończąc opis aktualnych uwarunkowań funkcjonowania rosyjskiego bloku siłowego, warto zwrócić uwagę na przejawy partykularyzmu i rywalizacji między jego podmiotami. Przykładem wewnętrznych sporów jest los ustawy *O prywatnych firmach wojskowych*, której założenia zostały opracowane jeszcze w 2012 r. Inicjatywa wspierana zakulisowo przez resort obrony została podjęta przez członków fasadowej partii Sprawiedliwa Rosja, napotykała jednak niejasne przeszkody proceduralne. W 2014 r., na kanwie wydarzeń w Donbasie, autorzy projektu podjęli kolejną próbę zakończenia procesu legislacyjnego. Istotą inicjatywy było umożliwienie resortowi obrony stworzenia legalnych formacji ochotniczych, mogących wypełniać zadania militarne m.in. na terytorium państw, które zwróciłyby się do Rosji o tego rodzaju pomoc[16]. Wydawałoby się oczywiste, że w sytuacji militaryzacji rosyjskich struktur państwowych inicjatywa ta powinna zostać zrealizowana. Tak się jednak nie stało, a główną przyczyną porażki był sprzeciw wyrażony oficjalnie przez przedstawicieli FSB. Służba zgłosiła poprawki do ustawy, których wprowadzenie sankcjonowało kontrolę FSB nad funkcjono-

[16] W Rosji istnieją komercyjne prywatne firmy wojskowe, których działalność jest oparta na ogólnych zasadach przyjętych na świecie, nie jest jednak zalegalizowana w prawie rosyjskim. Jedną z nich jest RSB-Group posiadająca biura kontaktowe w Niemczech, Włoszech, Turcji i na Cyprze (strona internetowa firmy http://rsb-group.ru/).

waniem firm (np. dzięki odpłatnemu licencjonowaniu usług czy kontroli zatrudnianych osób). W rezultacie doszło do pata legislacyjnego i projekt ustawy został skierowany ponownie do tzw. zamrażarki. Zawieszenie projektu nastąpiło ostatecznie po bezpośredniej ingerencji Kremla. Dnia 17 września 2015 r. rzecznik prasowy prezydenta FR Dmitrij Pieskow oświadczył, że administracja prezydenta nie zajmuje się tym problemem[17]. Jego wypowiedź jest przykładem sposobu zarządzania blokiem siłowym przez Kreml, który nadal zachowuje pozycję niekwestionowanego arbitra, choć niewątpliwie na stanowisko administracji prezydenta miały nieformalny wpływ osoby związane z FSB.

Perspektywy

Wzrost agresywności rosyjskiej polityki zagranicznej i pogarszająca się sytuacja ekonomiczna kraju umocniły rosyjski sektor siłowy. Zachowanie jego stabilności jest nadal traktowane przez władze jako jedna z podstawowych gwarancji niezmienności systemu politycznego. Od początku 2014 r. blok siłowy przeszedł przyśpieszoną mobilizację i przystosował się do prowadzenia działań w realiach niewypowiedzianego konfliktu militarnego. Bezpośrednią tego konsekwencją była modyfikacja hierarchii strategicznych priorytetów działania w sferze bezpieczeństwa. W wymiarze wewnętrznym jest nim ograniczanie wolności jednostki i sterowanie procesami społeczno-politycznymi. W zewnętrznym – podejmowanie działań ofensywnych wobec państw zachodnich przypominających metody stosowane w czasach zimnej wojny. Rosyjski sektor siłowy, pomimo obserwowanych przedsięwzięć dostosowawczych (m.in. przez stosowanie technologii informatycznych czy uczynienie z problematyki bezpieczeństwa oferty współpracy międzynarodowej), kultywuje doświadczenia i wzorce znane z czasów istnienia KGB i tradycji funkcjonowania w państwie autorytarnym. W 2013 r., opisując system służb specjalnych FR, pisaliśmy:

> Znacząca część „tradycyjnych" działań rosyjskich służb jest pochodną reżimu politycznego i wiąże się z udziałem poszczególnych instytucji sektora bezpieczeństwa w politycznych projektach Kremla. W tym kontekście można się pokusić o tezę, że pełni on swoistą funkcję „moderacyjną", która polega na kreowaniu zjawisk i zachowań pożądanych z punktu widzenia reżimu, w tym informacyjne wsparcie władz i marketing polityczny[18].

Trudno zmodyfikować tę diagnozę. Konflikt z Ukrainą i rozpoczęcie „siłowej" rywalizacji z Zachodem ujawniły jedynie niepokojącą prawidłowość. Zaostrzenie języka polityków oraz wzrost napastliwości propagandy poprzedzały zazwyczaj agresywne działania służb specjalnych. Należy również założyć, że możliwe zmiany kadrowe w kierownictwie służb, które nastąpią w najbliższych kilku latach (głównie z powodu przechodzenia kolejnych osób na emerytury), nie wpłyną na kształt systemu instytucji bezpieczeństwa FR. Jego zmiana mogłaby nastąpić jedynie w wyniku poważnego kryzysu władzy, który wydaje się mało prawdopodobny. Należy raczej oczekiwać, że w Rosji nastąpi powolna wymiana elit politycznych oparta na zasadzie kontrolowanego dopuszczania do władzy nowych osób powiązanych z instytucjami bezpieczeństwa.

---

[17] *Песков: частные военные компании – Кремлю сейчас не до этого* [online], http://rueconomics.ru/99755-peskov-chastnyie-voennyie-kompanii-kremlyu-seychas-ne-do-etogo/ [dostęp: 8 X 2015].

[18] J. Darczewska, P. Żochowski, *Rola służb specjalnych*..., s. 30.

Kamil Kucharski

Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej

Strategia wojny polega na przebiegłości i stwarzaniu złudzeń. Dlatego, jeśli jesteś do czegoś zdolny, udawaj niezręcznego, jeśli jesteś aktywny, stwarzaj pozory bierności. Jeśli jesteś blisko, stwórz pozory dużej odległości, jeśli uwierzą, że jesteś daleko, znajdź się niespodziewanie blisko. Staraj się wprowadzić wroga w błąd, stwórz dezorganizację w jego armii i dopiero wtedy uderzaj.

Sun Tzu, *Sztuka wojny*[1]

Bezpieczeństwo to subiektywny stan poczucia braku zagrożeń, który, zgodnie z kategoryzacją Abrahama Maslowa, jest niezbędny do stabilnej i zrównoważonej realizacji potrzeb wyższego rzędu (np. przynależności, szacunku czy samorealizacji)[2]. Warto zauważyć, że w obliczu aktywności organizacji terrorystycznych, sytuacji na wschodzie Ukrainy czy konfliktów prowadzonych np. w Syrii i Afryce, kategoria bezpieczeństwa nabiera coraz większego znaczenia dla społeczeństw współczesnego świata. Jest to zagadnienie wielowymiarowe i interdyscyplinarne. W literaturze przedmiotu wyróżnia się m.in. bezpieczeństwo wewnętrzne, zewnętrzne, polityczne, społeczne, gospodarcze, energetyczne. W ostatnich latach szczególnego znaczenia nabrał obszar cyberprzestrzeni, który ze względu na postęp techniczny i technologiczny warunkujący ciągłe zmiany i zakres funkcjonowania obejmujący cały glob, stał się również istotnym problemem w aspekcie bezpieczeństwa państwa i społeczeństwa.

Stara-nowa wojna hybrydowa

Pojęcie „wojny hybrydowej", które w ostatnim czasie stało się popularne w mediach i opracowaniach naukowych, jest zjawiskiem trudnym do zdefiniowania. Nie oznacza to jednak, że ludzkość wcześniej nie doświadczyła tego rodzaju konfliktu. Jacek Reginia-Zacharski trafnie zauważył, że błędem jest traktowanie wojen hybrydowych jako czegoś nowego. Zaznaczył, że (…) *konflikty zbrojne zawsze były w pewnym sensie „hybrydowe", bądź mogły się nimi stać*[3]. Wzrost liczby tego rodzaju działań jest spowodowany postępującym procesem globalizacji i rewolucji telein-

[1] Tekst dostępny online na stronie: http://www.lazarski.pl/pl/pobierz/837/ [dostęp: 1 IX 2015].

[2] L. Hostyński, Wartości w świecie konsumpcji, Lublin 2006, s. 24–30.

[3] J. Reginia-Zacharski, *Wojna w świecie współczesnym. Uczestnicy, cele, modele, teorie*, Łódź 2014, s. 303–304.

formatycznej oraz technologicznej, co jednocześnie upowszechnia nowe rozwiązania w sztuce wojennej.

Problemy w zdefiniowaniu wojny hybrydowej sprawiły, że wciąż nie jest jasne, co należy rozumieć pod tym pojęciem. Mogą to być klasyczne operacje z wykorzystaniem sił zbrojnych, połączone z przestępczością zorganizowaną prowadzoną na terenie państwa przeciwnika, mające na celu osłabienie aparatu państwowego tego państwa. Mogą to być również ataki teleinformatycze na systemy infrastruktury krytycznej oraz działania z zakresu tzw. *soft power*[4]. Literatura przedmiotu podkreśla jednak istotną cechę wspólną wojen hybrydowych – ich uczestnikami są podmioty państwowe oraz inne (niesymetryczne), których działania nie zawsze są związane ze sferą stricte militarną[5].

Założony w 1966 r. Sztokholmski Międzynarodowy Instytut Badań nad Pokojem (Stockholm International Peace Research Institute – SIPRI), w opublikowanym roczniku *SIPRI Yearbook 2015 Armaments, Disarmament and International Security*, zwraca uwagę, że od 2010 r. liczba konfliktów określanych mianem *non-state conflict* wzrasta[6] (wykres 1). Do tej kategorii zalicza się m.in. ataki ugrupowań terrorystycznych, ekstremistów, separatystów, a także ataki teleinformatyczne i inne, które nie są jasno definiowane jako międzypaństwowe.

Wykres 1. Liczba konfliktów zbrojnych w latach 2004–2013.

Źródło: *SIPRI Yearbook - Summary* [online], s. 7, www.sipri.org/yearbook/2015 [dostęp: 1 IX 2015].

[4] Więcej o *soft power* zob. P. Olszewski, *Strategia soft power Unii Europejskiej a euroatlantycka współpraca w wielobiegunowym świecie*, w: *System euroatlantycki w wielobiegunowym ładzie międzynarodowym*, J.M. Fiszer, P. Olszewski (red.), Warszawa 2013, s. 41–48.

[5] J. Reginia-Zacharski, *Wojna w świecie współczesnym*..., s. 295–298.

[6] www.sipri.org/yearbook/2015 [dostęp: 1 IX 2015].

Oblicza konfliktów zmieniały się na przestrzeni lat, co doskonale zauważył Alvin Toffler w swojej koncepcji fal. Autor wyróżnił trzy rodzaje fal (związanych z okresami w historii świata), które wpływały na obraz świata i toczących się wojen:

1) fala agrarna,
2) fala industrialna,
3) fala informacyjna.

Pierwszy z definiowanych przez Tofflera okresów to czas rewolucji agrarnej, który doprowadził do powstania przednowoczesnych społeczeństw. Autor zaznaczał, że fala agrarna przyczyniła się do szybszego rozwoju państw oraz pojawienia się wielu nowych zjawisk społecznych i politycznych. Adekwatnie do tego okresu prowadzone wojny charakteryzowały się ograniczeniami w technice, komunikacji, organizacji, logistyce czy administracji[7]. Jak pisze Stanisław Koziej, wojna w fali agrarnej polegała na (…) *bezpośredniej walce człowieka z człowiekiem przy wykorzystaniu prostych narzędzi walki*[8].

Druga fala, powiązana bezpośrednio z rewolucją przemysłową, przyniosła zupełnie nowy sposób postrzegania wojny. Warto zaznaczyć, że w tym okresie obraz wojny i przemiany industrialne wzajemnie na siebie oddziaływały. Nie tylko postęp przemysłowy wpływał na sposób prowadzenia konfliktu zbrojnego, lecz także sama wojna determinowała zmiany w procesach gospodarczych i wytwórczych. W tym czasie upowszechniono m.in. stosowanie standaryzacji oraz wykorzystywanie części zamiennych. Druga fala to etap, w którym stworzono broń i narzędzia zwiększające siłę rażenia państw zaangażowanych w konflikt. Ostatecznie, zdaniem Tofflera, (…) *masowe zniszczenie zaczęło odgrywać taką samą rolę w doktrynie wojskowej, jak masowa produkcja w gospodarce*[9]. Osiągnięto wówczas swoisty szczyt rozwojowy w zakresie tworzenia broni o możliwie największej sile rażenia, którego przejawem było zastosowanie broni jądrowej.

Trzecia fala opisywana w tofflerowskiej koncepcji to w rzeczywistości połączenie fali drugiej (produkcji masowej) oraz rewolucji technologicznej i informacyjnej. Wówczas powstały również pojęcia takie, jak „kultura informacyjna" i „cywilizacja informacyjna". Informacja stała się towarem, który ma swoją wartość i określa rzeczywistość. Zmieniło się oblicze prowadzonych wojen. Coraz częściej, w działaniach zbrojnych jest wykorzystywana nowoczesna technika wojskowa (bezzałogowe obiekty latające, rakiety dalekiego zasięgu, lokalizatory itp.)[10]. Wraz z pojawieniem się trzeciej fali wzrosło znaczenie działań niemilitarnych i nieregularnych, które ostatecznie doprowadziły do popularyzacji pojęć: „wojna hybrydowa" i „zagrożenie asymetryczne". Na tej podstawie można wnioskować, że trudne do jednoznacznego zdefiniowania komponenty wojny hybrydowej zależą od poziomu rozwoju społeczeństw będących stroną konfliktu. Pojawił się nowy obszar ruchów wojennych – przestrzeń teleinformatyczna. Popularna sieć Internet stała się doskonałym środkiem do ataków, które mogą być brzemienne w skutki (wywołując np. chaos informacyjny albo paraliż komunika-

[7] A. Toffler, H. Toffler, *Wojna i antywojna*. *Jak przetrwać na progu XXI wieku?*, Poznań 2006, s. 41–44.

[8] S. Koziej, *Wstęp do teorii i historii bezpieczeństwa (skrypt internetowy)*, Warszawa 2010, s. 22; koziej.pl/materialy–dydaktyczne [dostęp: 1 IX 2015].

[9] A. Toffler, H. Toffler, *Wojna i antywojna*..., s. 46–51.

[10] Tamże, s. 75–80. Zob. także A. Toffler, H. Toffler, *Trzecia fala*, Poznań 2006, s. 179–185.

cyjny), a są stosunkowo bezpieczne dla agresora (ze względu na odległość i poczucie bezkarności). W dobie postępu technicznego i informacyjnego oczywiste stało się wykorzystywanie np. ataków hakerskich, które wspierają działania konwencjonalne i pomagają osiągnąć założony cel.

Cyberprzestrzeń jako nowy obszar działań w wojnie hybrydowej

Zdaniem organizacji międzynarodowej Internet Society zajmującej się m.in. popularyzacją World Wide Web (…) *Internet daje możliwość, jednocześnie na całym świecie, nadawania i rozpowszechniania informacji. Jest medium współpracy i interakcji między ludźmi a komputerami, bez względu na położenie geograficzne*[11]. Wykorzystanie World Wide Web stało się więc jednym z obszarów zainteresowań krajów zaangażowanych w prowadzenie działań wojennych. Popularność tego medium gwarantuje dostęp do dużej liczby odbiorców przy jednocześnie niskich kosztach prowadzonych operacji. Doskonałym przykładem działalności informacyjno-propagandowej w przestrzeni teleinformatycznej, która ma za zadanie wspierać politykę stosującego ją państwa, jest zalew informacyjny i propaganda rozprzestrzeniana przez Federację Rosyjską. Zjawisko działalności informacyjno-propagandowej, tak jak i wojna hybrydowa, nie jest nowe. Operacje psychologiczne (PSYOPS) oraz operacje informacyjne (INFOOPS) funkcjonują w wielu krajach na świecie. Niemniej jednak to Rosja w ostatnim czasie jest najlepszym przykładem potwierdzającym istotę działań propagandowych dla realizacji własnych celów. Jak podkreśla Gabriel Nowacki, (…) *rosyjscy teoretycy rozumieją, że w dobie informacyjnej wszyscy do pewnego stopnia są podatni na manipulacje*[12]. Autor podaje przykład działań informacyjno-propagandowych Moskwy za czasów drugiej operacji czeczeńskiej w latach 1999–2000. Wówczas retorykę Kremla rozpowszechniano za pomocą ulotek perswazyjnych, programów radiowych (w języku czeczeńskim i rosyjskim) oraz przy okazji bezpośrednich spotkań z ludnością cywilną (podczas których jednocześnie przekazywano materiały drukowane i retransmitowano programy radiowe)[13].

Dla Federacji Rosyjskiej (ale nie tylko dla tego kraju[14]) szczególnego znaczenia w kontekście prowadzenia działań informacyjnych nabrała cyberprzestrzeń. Jak podkreśla Yannick Harrel, (…) *cyberprzestrzeń pozwala korzystać z relatywnej dyskrecji, umożliwia uderzenie szybkie bądź z opóźnieniem, prowadzenie działań synchronicznych czy też asynchronicznych, osłabiających siły wroga*[15]. Zaangażowanie się Kremla w operacje informacyjne (propaganda, dezinformacja i ataki teleinformatyczne) wspierające prorosyjskich separatystów podczas konfliktu we wschodniej części Ukrainy jest powszechnie znane. W tym kontekście szczególnie popularna była

[11] D. Marczuk, K. Kucała, *Wolność słowa w świecie wirtualnym – wartość nadużywana*, w: *Zagrożenia cyberprzestrzeni i świata wirtualnego*, J. Bednarek, A. Andrzejewska (red.), Warszawa 2014, s. 148.

[12] G. Nowacki, *Organizacja i prowadzenie działań psychologicznych w wybranych państwach*, Toruń 2004, s. 145–146.

[13] Tamże, s. 148–151.

[14] Na przykład Chińska Republika Ludowa dysponuje organem Zongcan Sanbu, który jest odpowiedzialny za prowadzenie tzw. CyberPsyOps (Cyber Psychological Operations). Polskę reprezentuje w tym zakresie założona w 2002 r. w Bydgoszczy Centralna Grupa Działań Psychologicznych, która odpowiada m.in. za wsparcie Sił Zbrojnych RP oraz wojsk Sojuszu Północnoatlantyckiego podczas realizowanych operacji. Więcej na ten temat na portalu www.jednostki-wojskowe.pl/index.php?option=com_content&view=article&id=311&Itemid=27 [dostęp: 1 IX 2015].

[15] Y. Harrel, *Rosyjska cyberstrategia*, Warszawa 2014, s. 149.

aktywność grupy hakerów Cyberberkut, która m.in. masowo umieszczała w Internecie autentyczne wiadomości z pominięciem istotnych faktów, które zupełnie zmieniały obraz konfliktu[16].

Rewolucja informacyjna, która m.in. determinuje intensywność procesu globalizacji, w istotny sposób wpłynęła na zmianę modelu komunikacji społecznej, ułatwiając nawiązywanie kontaktu pomiędzy ludźmi, przy jednoczesnym ograniczaniu bezpośredniej interakcji. Internet, telefon i telewizja tworzą sferę masowego przekazu, który zalewa społeczność na całym świecie. Środki te (…) *poszerzają możliwości percepcji, zwiększają szanse wyrażania opcji politycznych, kulturowych, filozoficznych, interakcji z innymi, rozumienia procesów społecznych, reakcji na zmiany itp.*[17] Naturalne więc stało się wykorzystanie nowych form komunikacji do prowadzenia działań wpisujących się w koncepcję wojny hybrydowej. Istotnym problemem pozostaje jednak anonimowość w sieci, która sprawia, że przekaz staje się trudny do zwalczenia, a autorzy i mocodawcy trudni do ustalenia.

Narzędzia służące do anonimizacji aktywności w Internecie

Zachowanie anonimowości w sieci to narastający problem współczesnego społeczeństwa. Coraz częściej podejmuje się dyskusję na temat internetowej prywatności, a incydenty, takie jak ujawnienie przez Edwarda Snowdena skali inwigilacji w World Wide Web, intensyfikują debatę publiczną. Najprostszym sposobem na pozostanie incognito jest zwyczajna ostrożność. Sami decydujemy, czy w cyberprzestrzeni posługujemy się własnym imieniem i nazwiskiem, czy też internetowym nickiem[18]. Literatura przedmiotu wskazuje, że najlepszym sposobem na zachowanie prywatności jest kontrola nad przepływem informacji. Prosta zasada – myślenie przed opublikowaniem – to klucz do zachowania bezpieczeństwa swoich danych[19]. Aktorzy sceny międzynarodowej oraz organizacje pozapaństwowe zainteresowane prowadzeniem działań informacyjnych, mając do dyspozycji potęgę cyberprzestrzeni, również stoją przed problemem maskowania swojej działalności. W odpowiedzi na potrzeby nie tylko zwykłych użytkowników, lecz także tych zainteresowanych aktywnością z zakresu wojny hybrydowej, powstały narzędzia, które mogą pomóc ochronić tożsamość internauty. Wśród nich wyróżnia się: TOR, System TAILS, serwery proxy, generatory tożsamości oraz anonimowe skrzynki e-mail.

TOR

The Onion Router (TOR) to projekt zapobiegający analizie ruchu sieciowego. Doskonałym słowem opisującym funkcjonowanie TOR jest „cebula". Metafora ta, nie bez przyczyny wykorzystana w nazwie projektu, odwołuje się do warstwowej budowy cebuli, która tak jak TOR uniemożliwia sprawdzenie tego, co znajduje się w środku. Inaczej mówiąc, pod każdą warstwą znajduje się kolejna. Stąd też przesyłanie pa-

[16] Tamże, s. 12–13.

[17] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 2009, s. 40.

[18] Tzn. pseudonimem.

[19] Ł. Kołodziejczyk, *Prywatność w Internecie: postawy i zachowania dotyczące ujawniania danych prywatnych w mediach społecznościowych*, Warszawa 2014, s. 66.

kietów danych w TOR określono jako „trasowanie cebulowe" (*onion routing*). Przez TOR użytkownik sieci ma dostęp do ukrytej treści Internetu, tzw. Deep Web lub Dark Web. Jest to niezwykle ważna część sieci, gdyż według „The Guardian" – znane silniki wyszukiwarek internetowych, takie jak Google czy Yahoo, mają dostęp jedynie do 0,03 proc. zasobów Internetu[20]. Pozostała część to głęboka sieć, do której dostęp mają użytkownicy korzystający z odpowiedniego oprogramowania i posiadający właściwą wiedzę.

Inicjatorami sieci TOR byli programiści Roger Dingledine, Nick Mathewson oraz Paul Syverson, którzy przy wsparciu Centrum Badawczego Marynarki Wojennej USA rozpoczęli w 2002 r. pracę nad projektem[21]. Serwery tworzące sieć w pierwszym okresie jej działania były umiejscowione jedynie w Stanach Zjednoczonych oraz Niemczech. Wówczas, co okazało się szczególnie istotne, powstały pierwsze ukryte usługi dla użytkowników sieci (specjalne portale i kanały wymiany informacji). W 2004 r. sieć została przejęta przez prywatny podmiot – firmę Electronic Frontier Foundation. Obecnie rozwijają ją sami użytkownicy (współtworzący organizację non profit o nazwie TOR Project), którzy podłączając się do TOR, tworzą kolejne warstwy tej najpopularniejszej sieci anonimizujacej na świecie. Siedziba TOR Project znajduje się w Stanach Zjednoczonych[22].

Zabezpieczenie ruchu sieciowego w TOR przebiega w kilku etapach. Pierwszym krokiem jest uruchomienie aplikacji TOR Browser, która jest przeglądarką przypominającą wizualnie zmodyfikowany program Mozilla Firefox. Po uruchomieniu użytkownik pobiera listę węzłów z oficjalnego serwera. Użytkownik sieci, próbując połączyć się z innym serwerem (np. udostępniającym usługę witryny internetowej), łączy się z losowym węzłem.

Na początku każdy pakiet danych ma ustalaną drogę wybieraną z listy węzłów. Istotnym jest, że żaden węzeł nie zapamiętuje tego, co otrzymał, odkodował i przesłał dalej. Generalnie ujmując w strukturze TOR, należy wyróżnić trzy rodzaje węzłów:

1. Wejściowy – Entry Node,
2. Przekaźnikowy – Relay Node,
3. Wyjściowy – Exit Node[23].

Następnie zaszyfrowany pakiet danych jest przesyłany do innych losowo wybranych węzłów przekaźnikowych, aby ostatecznie tzw. węzeł brzegowy (wyjściowy) połączył się z serwerem. Warto zaznaczyć, że połączenie między ostatnim węzłem a serwerem jest jawne (ostatni węzeł rozszyfrowuje dane), wszystkie natomiast połączenia między węzłami przekaźnikowymi są chronione kryptograficznie. Cała sieć TOR jest zdecentralizowana.

Charakterystyczną cechą witryn w sieci jest alias domeny (alternatywna nazwa domeny internetowej – przyp. red.). W Internecie przyjęło się wiele oznaczeń, które zwykle utożsamiają domenę z krajem lub prowadzoną działalnością. Przykładem jest: *.pl dla Polski, *.de dla Niemiec czy *.co.uk dla Wielkiej Brytanii. Inne aliasy to

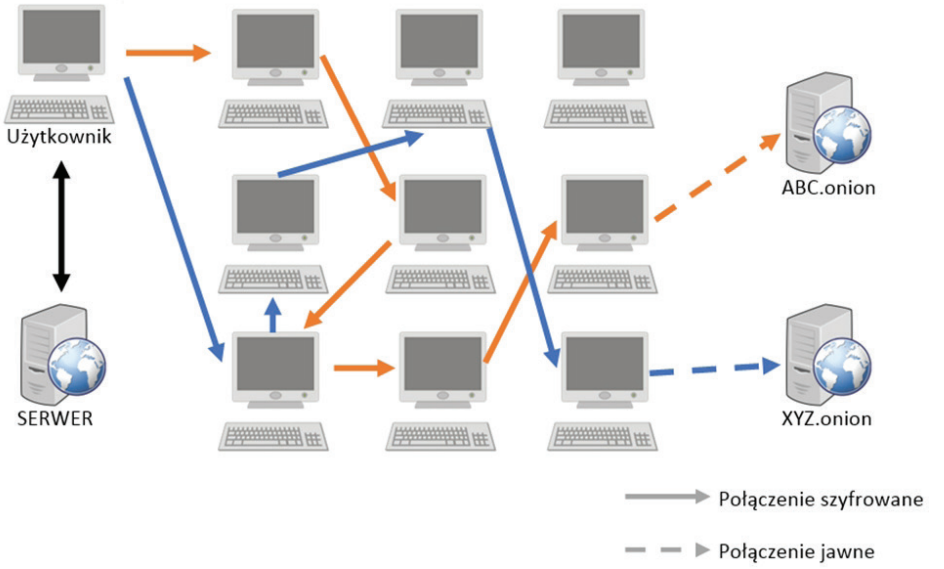
[20] www.sickchirpse.com/deep–web–guide/ [dostęp: 1 V 2015].

[21] T. Ciborski, *Ukryta tożsamość. Jak się obronić przed utratą prywatności?*, Gliwice 2015, s. 91.

[22] www.onion–router.net/History.html [dostęp: 1 V 2015].

[23] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Warszawa 2014, s. 37.

np. *.org dla organizacji lub *.gov dla witryn rządowych. Sieć TOR posiada swój indywidualny alias: *.onion, który znajduje się za dodatkową zaporą sieciową (firewallem) oraz jest ukryty przed Network Address Translation (NAT[24]), tj. mówiąc w uproszczeniu – usługą, która zmienia adres strony na bardziej czytelny. W konsekwencji adresy w sieci TOR to ciągi losowych znaków, co dodatkowo utrudnia znalezienie odpowiedniej witryny. Mówiąc inaczej, dostęp do właściwych treści mają osoby, które wiedzą, jak ich szukać. W odpowiedzi na to powstały serwisy funkcjonujące zarówno w sieci TOR, jak i w ogólnodostępnym Internecie, które zawierają listy serwerów TOR. W przeciwnym razie dostęp do niektórych usług byłby praktyczne niemożliwy[25]. Sposób działania sieci TOR został przedstawiony na rysunku 1.



Rys. 1. Przepływ pakietu danych w sieci TOR.

Źródło: Opracowanie własne na podstawie M. Górka, *Cyberbezpieczeństwo jako podstawa...*, s. 35–38.

Użytkownik po pobraniu listy dostępnych węzłów (czarna strzałka) wpisuje w przeglądarkę adres, z którym chce się połączyć (np. ABC.onion – połączenie pomarańczowe). Następnie pakiet danych jest wysyłany do losowo wybranego węzła, który przekazuje go do kolejnego losowo wybranego węzła i tak aż do trafienia na węzeł brzegowy. Węzeł brzegowy, po rozszyfrowaniu danych, zwraca się do serwera o udostępnienie usługi, np. witryny. Wówczas na ekranie użytkownika pojawia się obraz domeny (w pierwszym przypadku ABC.onion).

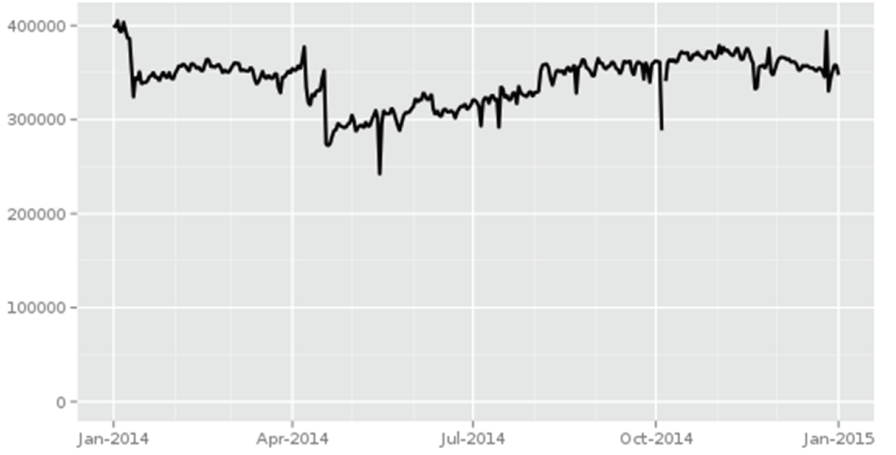
Kiedy użytkownik chce otworzyć inną witrynę (np. XYZ.onion – strzałki niebieskie) wszystkie czynności wykonywane są analogicznie, ale zmienia się trasa przesyłanego pakietu danych. Co więcej – nawet powtórne połączenie się z przykładową

[24] *Network Address Translation* – usługa konwertująca adres IP na inny. Więcej na ten temat: P.G. Sery, J. Beale, *Serwery internetowe Red Hat Linux*, Gliwice 2004, s. 88–89.

[25] M. Górka, *Cyberbezpieczeństwo jako podstawa...*, s. 37–38.

witryną ABC.onion nie odbywa się dwa razy przez taką samą trasę węzłów. Takie zasady funkcjonowania TOR sprawiają, że przeanalizowanie ruchu sieciowego, a co za tym idzie – zidentyfikowanie osoby, która wysyła zapytanie do sieci, jest niemożliwe.

TOR tworzą użytkownicy, którzy podłączają się do sieci. Każdy dodatkowy komputer korzystający z TOR może być węzłem przekaźnikowym lub brzegowym. W związku z tym sieć się rozrasta, tworząc pajęczynę powiązań uniemożliwiających zidentyfikowanie jej poszczególnych użytkowników. Skalę przedsięwzięcia obrazuje wykres 2 przedstawiający liczbę użytkowników TOR w USA w okresie od 1 stycznia 2014 r. do 1 stycznia 2015 r.



Wykres 2. Liczba użytkowników TOR w USA od 1 stycznia 2014 do 1 stycznia 2015 r.
Źródło: https://metrics.torproject.org [dostęp: 1 V 2015].

Jak widać, popularność usługi nie jest stała, ale wciąż utrzymuje się na wysokim poziomie. Tylko w Stanach Zjednoczonych liczba użytkowników wynosi ponad 300 tys. TOR działa w każdym kraju na świecie, w którym są dostępne Internet i komputery. Oznacza to, że zidentyfikownie osoby znajdującej się po drugiej stronie monitora jest prawie niemożliwe. Trzeba jednak pamiętać o kilku podstawowych zasadach, których należy przestrzegać podczas korzystania z TOR[26].

Przede wszystkim twórcy TOR zwracają uwagę na konieczność korzystania wyłącznie z oprogramowania projektu. Oznacza to, że użytkownik, chcąc zachować anonimowość, nie powinien łączyć przeglądarki obsługującej TOR z innymi aplikacjami. TOR Browser (aplikacja obsługująca sieć) jest jedynym i oficjalnym narzędziem do poruszania się po anonimowej sieci. Korzystanie z zamienników i innych rozwiązań może narazić na zdemaskowanie, ponieważ nie ma pewności, czy wykorzystywane narzędzie jest odpowiednio skonfigurowane.

Drugim zaleceniem twórców jest niewykorzystywanie transmisji danych torrent przez sieć TOR. Torrent to protokół służący do wymiany plików, działający tak, że

[26] www.torproject.org/download/download.html.en#warning [dostęp: 10 V 2015].

konkretne dane są udostępniane przez użytkowników sieci, a nie serwer. Członkowie TOR Project zwracają uwagę, że nawet jeśli program wymiany plików torrent pracuje wyłącznie w sieci TOR, to bardzo często zmusza on użytkownika do udostępnienia swojego prawdziwego adresu IP komputera, po którym można zostać zidentyfikowanym.

Kolejnym działaniem, któremu należy zapobiegać w aplikacji TOR, jest instalowanie wtyczek użytkownika. Popularne *pluginy*, takie jak Flash (odpowiedzialny za wyświetlanie treści flash) czy JavaScript, są często niedopracowane i niezabezpieczone pod kątem użytkowania sieci TOR. Oznacza to, że mogą być tzw. wąskim gardłem zachowania prywatności i narazić użytkowanika na zdemaskowanie.

Czwartą zasadą korzystania z TOR jest upewnienie się, czy nawiązywane połączenie przebiega za pomocą protokołu SSL. (...) *Używanie protokołu SSL zapewnia większą prywatność i bezpieczeństwo niż nieszyfrowane połączenie sieciowe. Ogranicza ryzyko przechwycenia informacji i wykorzystania ich do niewłaściwych celów przez osoby trzecie. Wielu internautów czuje się bardziej komfortowo, kiedy udostępniają dane dotyczące płatności lub inne dane osobiste, korzystając z połączenia SSL*[27]. Mimo że połączenie między węzłami przekaźnikowymi w sieci jest szyfrowane, to ostateczny wynik tego, co ukazuje się na monitorze, całkowicie zależy od strony internetowej, na którą użytkownik wchodzi. Inaczej mówiąc, jeśli strona, z którą następuje połączenie, jest szyfrowana protokołem SSL (początek adresu zaczyna się od https), to można być pewnym bezpieczeństwa tego połączenia.

Piąta zasada korzystania z TOR Browser dotyczy zachowania się w stosunku do pobranych plików. Członkowie projektu zalecają otwieranie pobranych danych dopiero po wylogowaniu się z sieci. Szczególnie niebezpieczne są pliki pakietu Office oraz popularne PDF, ponieważ te dokumenty mogą zawierać źródła i hiperłącza odnoszące do pobrania danych przez program działający poza siecią TOR. Warto zaznaczyć, że przeglądarka sieci TOR ostrzega komunikatem przed próbą otwarcia pliku bezpośrednio po jego ściągnięciu.

Ostatnia zasada korzystania z TOR dotyczy samego ruchu sieciowego. Twórcy tego projektu nie wykluczają, że urządzenia monitorujące sieć będą w stanie nauczyć się mapy węzłów i rozróżnić użytkowników, którzy z niej korzystają. Rozwiązaniem tego problemu jest połączenie się z TOR w trybie przekaźnika. Wówczas również przez nasz adres IP będą przesyłane pakiety danych innych użytkowników z całego świata. Tym samym twórcy zachęcają do popularyzacji TOR wśród znajomych, ponieważ im więcej użytkowników, tym sieć jest bardziej bezpieczna.

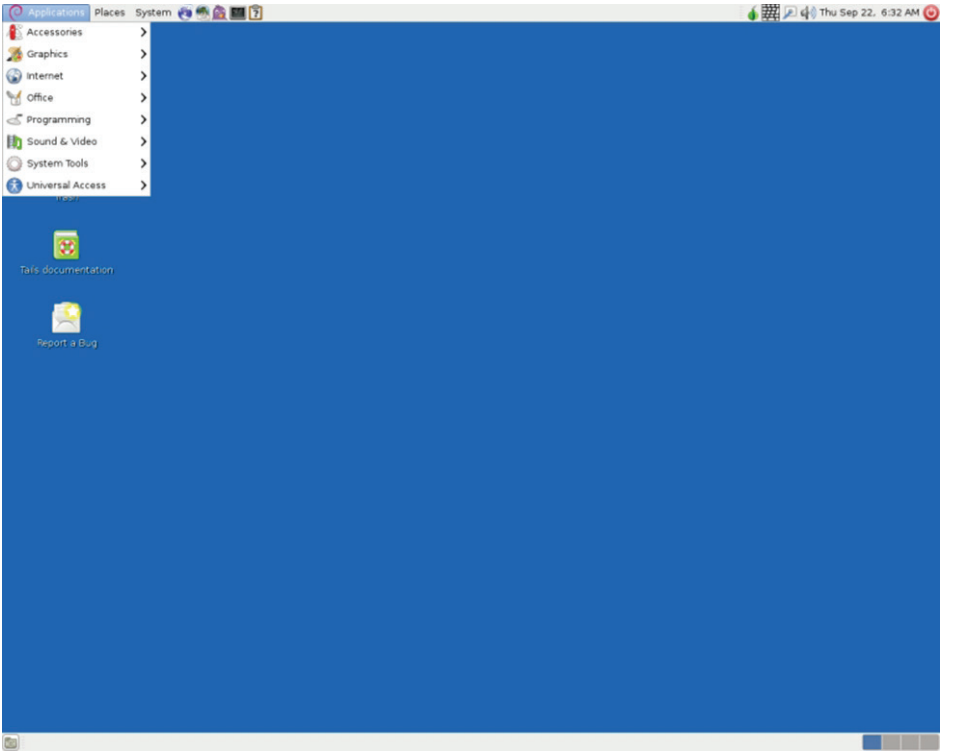
System Linux TAILS

Z siecią TOR jest ściśle związany system The Amnesic Incognito Live System, znany jako TAILS. Jest to produkt oparty na darmowym systemie operacyjnym Debian GNU/Linux. Warto zaznaczyć, że TAILS można uruchomić z płyty DVD, pamięci USB lub karty SD na dowolnym komputerze, niezależnie od przeinstalowanego systemu. Ogromną jego zaletą jest również fakt, że nie pozostawia po sobie śladów użytkowania.

[27] http://support.google.com/adwords/answer/2580401?hl=pl [dostęp: 12 V 2015].

TAILS to system operacyjny (podobnie jak Windows firmy Microsoft, Mac OS firmy Apple lub Ubuntu – jedna z najbardziej popularnych dystrybucji Linuxa), który jest specjalnie stworzony i skonfigurowany do wykorzystywania sieci TOR oraz I2P[28]. Zawiera on takie narzędzia, jak komunikator, przeglądarka internetowa lub program pocztowy, które działają wyłącznie w sieciach anonimizujących, zapewniając tym samym pełną prywatność jego użytkownikom. Istotną cechą TAILS jest to, że system automatycznie blokuje próbę uruchomienia aplikacji działającej poza siecią anonimizującą. Dzięki temu wyklucza on możliwość popełnienia prostych błędów, które mogłyby doprowadzić do ujawnienia tożsamości osoby po drugiej stronie monitora.

Tomasz Ciborski zwrócił uwagę, że (…) *TAILS, dzięki swoim gwarancjom bezpieczeństwa, stał się jednym z obiektów zainteresowań NSA. Anonimowy pracownik Agencji* (…) *nazwał go oprogramowaniem polecanym na forach o tematyce ekstremistycznej*[29]. Ekran startowy systemu TAILS został przedstawiony na rysunku 2.



Rys. 2. Wygląd systemu TAILS.

Źródło: http://i1-linux.softpedia-static.com/screenshots/Tails_1.png [dostęp: 1 IX 2015].

Jak widać, system jest wyposażony w skatalogowany zestaw oprogramowania, które zapewnia nie tylko anonimowość, lecz także wszelkie podstawowe funkcjonal-

[28] Druga po TOR popularna sieć do anonimizacji. Więcej o I2P na stronie projektu: https://geti2p.net/en/about/intro [dostęp: 1 IX 2015] oraz w publikacji T. Ciborski, *Ukryta tożsamość*..., s. 156–160.

[29] T. Ciborski, *Ukryta tożsamość*…, s. 163–164.

ności systemu operacyjnego (edytory graficzne, tekstowe, odtwarzacze plików multimedialnych). W górnym pasku narzędzi użytkownik ma dostęp m.in. do przeglądarki TOR, aplikacji e-mail oraz komunikatora, który ochrania tożsamość osoby korzystającej z TAILS. Konfiguracja przebiega automatycznie. Po podłączeniu się do sieci Wi-Fi użytkownik dostaje powiadomienie, że komputer i system są skonfigurowane do działania w sieci TOR. Co ciekawe – żadne treści zapisane w systemie TAILS nie są dostępne na użytkowanej jednostce z pozycji innego systemu (włącznie z plikami tekstowymi czy obrazami).

Serwery proxy

Analizując działanie serwerów proxy oraz sieci TOR, należy stwierdzić, że występuje wiele podobieństw między tymi rozwiązaniami. Proxy to inaczej serwer przekaźnikowy, który pośredniczy w przesyłaniu informacji. Obrazując działanie proxy, można powiedzieć, że odbiera on żądanie wyświetlenia strony WWW o określonym adresie, a następnie zwraca się do serwera strony WWW, przekazując to żądanie jako swoje własne. W rezultacie serwer WWW przesyła pakiet danych do proxy, a ten przekazuje je do użytkownika. Jak pisze Witold Wrotek, (…) *jednym z zastosowań serwera proxy jest ukrywanie tożsamości komputera. W tym przypadku serwer proxy powinien znajdować się jak najdalej od komputera*[30]. Najlepszym rozwiązaniem jest wykorzystanie serwera proxy znajdującego się w innym kraju. Wówczas administrator, który bada ruch sieciowy, jest przekonany, że zapytanie dotyczące wyświetlenia strony, opublikowane komentarze lub inne treści jest umieszczone przez użytkownika, przebywającego w rzeczywistości na terenie Federacji Rosyjskiej, pochodzą ze Stanów Zjednoczonych, Ukrainy, Niemiec czy też z Polski.

Wpisując w wyszukiwarkę Google hasło „free proxy server", otrzymuje się ponad 7 mln wyników. Jedne z najpopularniejszych to serwery hide.me/en/proxy oraz anonproxy.eu. Nie należy jednak korzystać z tych konkretnych dwóch serwisów, ponieważ ich popularność zależy m.in. od prędkości wyświetlania danych, obsługiwanych formatów oraz dostępności (tzn. czasu online), tj. cech, które mogą ulec zmianie. Jeśli użytkownikowi zależy, aby jego adres IP był utożsamiany z konkretnym państwem, do wyszukiwanego hasła można dodać kraj, np. „free proxy Ukraine" lub „free proxy UK", a w rezultacie opublikowane z wykorzystaniem tych serwerów treści będą widoczne jako ukraińskie lub brytyjskie.

Warto zaznaczyć, że ukrywanie tożsamości za pośrednictwem proxy nie wymaga korzystania jedynie z listy serwerów, które zwraca wyszukiwarka. Dostawcy oprogramowania wśród najpopularniejszych darmowych przeglądarek (Chrome, Mozilla Firefox, Opera) udostępniają wtyczki (wspomniane wcześniej *pluginy*), które po uruchomieniu zmieniają użytkownikowi automatycznie serwer proxy. Tym samym korzystanie z tego rozwiązania jest jeszcze łatwiejsze. Dla przykładu, w przeglądarce Mozilla Firefox użytkownik ma do dyspozycji m.in. wtyczki Best Proxy Switcher, Elite Proxy Switcher, Proxy Selector oraz Proxy Tool.

[30] W. Wrotek, *Sieci komputerowe*, Gliwice 2008, s. 274–275.

Generatory tożsamości i anonimowe skrzynki e-mail

Swoistym uzupełnieniem opisanych powyżej narzędzi są generatory fałszywych tożsamości oraz anonimowe skrzynki e-mail. Generator tożsamości to proste narzędzie działające w ramach aplikacji webowej. Jak sama nazwa wskazuje, tworzy on spójne zestawienie informacji osobowych, które można wykorzystać w procesie np. rejestracji do różnych serwisów. Przykładowym, sprawnie działającym generatorem tożsamości, jest FakeNameGenerator (fakenamegenerator.com). Witryna ta, przed procesem tworzenia danych, umożliwia m.in. wybór płci oraz kraju zamieszkania fałszywej tożsamości. Program wyświetla takie informacje, jak: imię, nazwisko, PESEL, numer telefonu, adres e-mail, a nawet dane karty kredytowej. Przykład działania fakenamegenerator.com przedstawia rysunek 3.

Seweryn Jasiński
ul. Józefa 146
92-207 Łódź

Curious what **Seweryn** means? Click here to find out!

Mother's maiden name	Szczepańska
PESEL	811213[redacted]
Geo coordinates	51.682584, 19.537246

PHONE

Phone	[redacted]
Country code	48

BIRTHDAY

Birthday	December 13, 1981
Age	33 years old
Tropical zodiac	Sagittarius

ONLINE

Email Address	SewerynJasinski@dayrep.com *This is a real email address. Click here to activate it!*
Username	Prect1981
Password	eeW6ohjaigh

Rys. 3. Wynik działania Fake Name Generator przy danych wejściowych: Male, Polish, Poland.
Źródło: Opracowanie własne. Ewentualna zbieżność danych przypadkowa. Wygenerowany numer PESEL oraz numer telefonu zostały wymazane.

Próba wygenerowania i sprawdzenia numerów telefonów kilku fałszywych tożsamości kończyła się zwykle komunikatem „wybrany abonent jest w tym momencie nieosiągalny", lub „numer nie istnieje"[31]. Podobna sytuacja dotyczyła weryfikacji

[31] Stan na 1 IX 2015 r.

numeru PESEL w oficjalnej bazie. Generator nie jest jednak doskonały – zdarzało się, że łączono się telefonicznie z przypadkową osobą lub wynik sprawdzenia w bazie PESEL przedstawiał faktycznie istniejącą osobę (należy jednak podkreślić, że jej dane różniły się od tych generowanych przez program). Mimo to, przy mało wnikliwej weryfikacji tożsamość proponowana przez generator wydaje się być prawdziwa. Dla osoby, która nie ma dostępu do właściwych baz mogących potwierdzić konkretne dane, fałszywa tożsamość sprawia wrażenie rzeczywistej.

Fake Name Generator to narzędzie działające kompleksowo. Tworzy fikcyjne dane osobowe, którymi użytkownik może się bez większych konsekwencji posługiwać w sieci. W wielu przypadkach nie musi on jednak wykorzystywać generatora tożsamości do anonimowej aktywności w Internecie. Witryny wymagają często od użytkownika jedynie podania adresu e-mail lub innej prostej rejestracji. W tym przypadku przydatne okazują się takie narzędzia, jak mailinator.com[32] czy notsharingmy.info.

Mailinator to serwis służący do jednorazowego odbioru poczty. Usługa ta jest szczególnie przydatna do szybkich rejestracji w dowolnych serwisach. Warto zaznaczyć, że konta pocztowe w Mailinatorze są publiczne – każda osoba, która zna nazwę konta, może na nie wejść. Wiadomości wysyłane na pocztę w tym serwisie są usuwane po jednym dniu. Aby stworzyć własną skrzynkę pocztową, wystarczy wpisać nazwę użytkownika (może to być dowolny ciąg znaków). Dla wybranej przez użytkownika frazy serwis zakłada szybkie konto kończące się adresem: @mailinator.com. Wówczas, za pomocą stworzonego e-maila, użytkownik może odbierać wiadomości.

Innym ciekawym narzędziem służącym do zachowania prywatności jest usługa notsharingmy.info, która tworzy swoisty system przekazywania wiadomości. Aby skorzystać z tego rozwiązania, należy podać swój prawdziwy adres poczty elektronicznej. Następnie strona zmienia rzeczywisty adres e-mail użytkownika na wersję skróconą, która maskuje nasze dane[33]. Ostatecznie otrzymuje się losowy ciąg znaków zakończony: @notsharingmy.info. Wszystkie wiadomości przesłane na wygenerowane konto pocztowe będą przekazane na prawdziwy adres. Notsharingmy.info, podobnie jak Mailinator, nie pozwala na wysyłanie wiadomości.

Wykorzystanie narzędzi anonimizujących do aktywności w ramach wojny hybrydowej

Rafał Brzeski wyróżnił dwa rodzaje wojen – energetyczne (czyli te, w których wykorzystuje się siłę fizyczną i uzbrojenie) oraz informacyjne (polegające na działaniach w sferze informacyjnej, takich jak wywiad, agentura wpływu oraz szeroko zakrojona propaganda i dezinformacja)[34]. Hybrydowość współczesnych konfliktów polega na połączeniu wymienionych sił i środków dla osiągnięcia przyjętych celów. Naturalne wydaje się to, że wykorzystanie specjalnych narzędzi służących do anonimizacji (m.in. danych, aktywności, jakichkolwiek działań w sieci) jest konieczne do prowadzenia skutecznych działań informacyjnych w cyberprzestrzeni, które mogą wpłynąć na ostateczne rozstrzygnięcie konfliktu.

[32] Polskim odpowiednikiem Mailinatora jest np. serwis: koszmail.pl [dostęp: 5 IX 2015].

[33] Przykład: nasz adres e-mail to XYZ@gmail.com. Wpisujemy go do serwisu *notsharingmy.info* i strona generuje e-mail 123abc@notsharingmy.info. Każda wiadomość wysłana na konto 123abc@notsharingmy.info zostanie przekazana na prawdziwy adres XYZ@gmail.com.

[34] R. Brzeski, *Wojna informacyjna – wojna nowej generacji*, Komorów 2014, s. 25–26.

Wykorzystanie TOR w ramach wojny hybrydowej to prosty sposób na anonimową aktywność o charakterze dezinformacyjnym i propagandowym. Właściwe stosowanie się do zasad obowiązujących w tej sieci pozwala na ochronę tożsamości i jednocześnie zapobiega dekonspiracji wysyłanego przekazu. TOR to narzędzie łączące prostotę z funkcjonalnością. Początkowo właściwe skonfigurowanie aplikacji wymagało ponadprzeciętnej wiedzy z zakresu informatyki. Obecnie praktycznie każdy może uruchomić program, wybrać sposób połączenia (rodzaj węzła) i korzystać zupełnie anonimowo ze wszystkich zasobów Internetu (jawnych oraz ukrytych). Internauta oprócz treści cebulowej (*.onion) może przeglądać ogólnodostępne fora internetowe, prowadzić blog, udzielać się w sieci i być przy tym całkowicie nierozpoznawalnym.

Szczególnie istotne jest to, że coraz więcej usług dostępnych w ramach zwyczajnego Internetu ma swoje odwzorowanie w sieci TOR. Doskonałym przykładem jest najpopularniejszy na świecie serwis społecznościowy Facebook (facebook.com), który umożliwia swoim użytkownikom korzystanie z oferowanych usług w sposób anonimowy za pośrednictwem swojego odpowiednika TOR dostępnego pod adresem facebookcorewwwi.onion. Mimo to, należy zaznaczyć, że cała aktywność użytkownika konta Facebook przy wykorzystaniu TOR jest wciąż monitorowana i po właściwym umotywowaniu, może zostać przekazana służbom bądź organom ścigania.

Poza działaniami ściśle informacyjnymi TOR stwarza możliwość przeprowadzania ataków hakerskich, które są bezpieczne dla agresorów. Przykład takiego rozwiązania opisał w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 r.* zespół CERT.GOV.PL działający w ramach Agencji Bezpieczeństwa Wewnętrznego. Z informacji zawartych w *Raporcie* wynika, że 23 października 2014 r. indeksy stron: gpwcatalyst.pl oraz newconnect.pl, związane z Giełdą Papierów Wartościowych, zostały zamienione przez hakerów. W serwisach tych pojawiły się zdjęcia dżihadystów oraz napis: *TO BE CONTINUED…* Zespół CERT.GOV.PL poinformował, że w związku z atakiem upubliczniono około 52 MB danych, a działania te zostały przeprowadzone z wykorzystaniem sieci TOR[35].

Sieć ta była wykorzystywana również przy okazji ataku na serwery Krajowego Biura Wyborczego. Wówczas (…) *wykonano kilkaset specjalnie spreparowanych zapytań przez adresy IP, które w większości należały do sieci anonimizującej TOR. Atakujący podejmowali wielokrotne, nieskuteczne próby przełamania zabezpieczeń w celu uzyskania nieautoryzowanego dostępu do zasobów*[36].

TAILS jako system operacyjny, kompleksowo obsługujący osoby zainteresowane utrzymaniem pełnej prywatności w Internecie, to również doskonałe narzędzie do eksploracji sieci. Wykorzystując generator fałszywej tożsamości oraz anonimowy adres e-mail w systemie TAILS lub w ramach TOR, można być pewnym, że nie ma możliwości ustalenia danych lub zlokalizowania prawdziwego autora publikowanego przekazu.

Serwery przekaźnikowe, które działają na podobnych zasadach do sieci TOR, to narzędzie, które doskonale sprawdza się przy wykonywaniu prostych czynności w Internecie (komentowania, publikowania artykułów). Serwery te umożliwiają maskowanie państwa, z którego faktycznie pochodzi udostępniana treść. Użytkownik

[35] CERT.GOV.PL, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 r.*, Warszawa 2015, s. 50.
[36] Tamże, s. 39.

jest w stanie podszyć się pod osobę znajdującą się w dowolnym kraju. Jest to o tyle istotne (i różni się od sieci TOR), że komentator może sam wybrać kraj, który ma być identyfikowany z publikowanym komentarzem (co w obliczu aktywności informacyjnej w ramach wojny hybrydowej ma duże znaczenie). Tylko głębsza analiza pozwala zdemaskować wpis umieszczony przy wykorzystaniu serwera przekaźnikowego.

Aktywność dezinformacyjna i propagandowa w Internecie jest w ostatnim czasie coraz częściej odnotowywana. O przykładzie takich działań pisała m.in. gazeta „The Washington Post", która zwróciła uwagę na wzrost liczby prorosyjskich komentarzy na stronach „The Washington Post", „The New York Times", CNN oraz „The Huffington Post". Publikowane treści charakteryzowały się słabym poziomem językowym, wulgaryzmami oraz prowokacyjną treścią, która jednoznacznie wychwalała politykę Kremla[37].

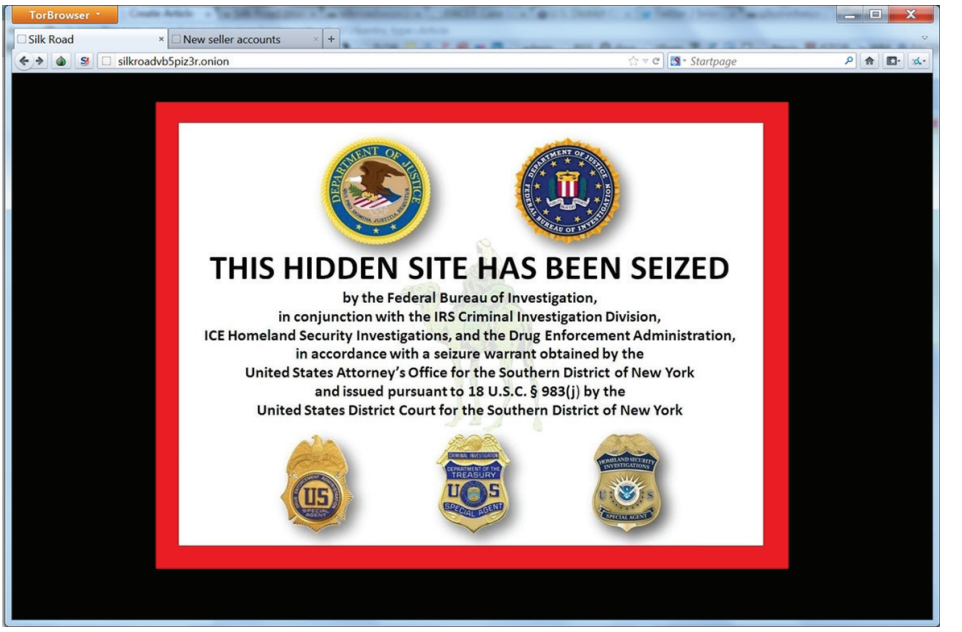
Problemy wynikające z wykorzystania narzędzi do anonimizacji działań w Internecie

Oprócz wielu zalet, które daje możliwość zabezpieczenia własnej prywatności, narzędzia służące do anonimizacji są doskonałym sposobem na prowadzenie działań propagandowych, dezinformacyjnych lub nielegalnych, np. przestępczości zorganizowanej (sprzedaż narkotyków, fałszywych dokumentów, pornografii).

Doskonałym przykładem problemu, który narodził się w wyniku powstania sieci TOR, jest działalność tzw. czarnych sklepów funkcjonujących w ramach anonimowej infrastruktury. Najbardziej znanym serwisem oferującym nie tylko narkotyki, lecz także pornografię dziecięcą, materiały wybuchowe oraz rozwiązania dotyczące oszustw podatkowych, był Silk Road założony przez Rossa Ulbricha[38]. Forum funkcjonowało od 2011 r. Na początku października 2013 r. każdy użytkownik korzystający z sieci TOR, który próbował połączyć się z forum Silk Road, uzyskiwał informację, że forum przejęło i zamknęło Federalne Biuro Śledcze (FBI). Komunikat pojawiający się przy próbie połączenia się z Silk Road przedstawia rysunek 4.

[37] www.washingtonpost.com/news/the-intersect/wp/2014/06/04/hunting-for-paid-russian-trolls-in-the-washington-post-comments-section/ [dostęp: 1 IX 2015]. Temat ten poruszyła również gazeta „Rzeczpospolita": www.rp.pl/artykul/1118117.html [dostęp: 1 IX 2015].

[38] www.freeross.org/ [dostęp: 13 V 2015].



Rys. 4. Informacja FBI o zamknięciu forum Silk Road.
Źródło: niebezpiecznik.pl [dostęp: 1 V 2015].

Sytuacja ta wywołała dyskusję, czy TOR jest faktycznie dobrym narzędziem do zachowania anonimowości w sieci? Okazało się, że tak, ponieważ opublikowane dokumenty dotyczące zatrzymania twórcy Silk Road pokazały, że do przejęcia forum doszło nie przez błędy sieci TOR, ale przez nieuwagę samego Rossa Ulbrichta. Analiza materiałów wskazała, że podstawowym błędem administratora Silk Road był brak zdolności rozdzielenia działalności w sieci TOR od działalności w jawnym Internecie. Do jego dekonspiracji doprowadziło m.in. to, że w obu sieciach korzystał z takich samych pseudonimów. Punktem zwrotnym w śledztwie prowadzonym przez FBI było zatrzymanie przesyłki adresowanej do Rossa, która zawierała dziewięć fałszywych dowodów tożsamości. Wówczas administrator miał się tłumaczyć, że zamówił je na forum Silk Road[39].

Funkcjonowanie tzw. czarnych sklepów pozwala postawić hipotezę, że w TOR mogą działać (lub już działają) także inne kanały komunikacyjne, które umożliwiają nie tylko przestępcom, lecz także ugrupowaniom terrorystycznym lub separatystycznym utrzymywanie kontaktu i koordynację działań. Ponadto można stwierdzić, że aktywność tzw. trolli, którzy są oskarżani o rozprzestrzenianie płatnych, pisanych na zamówienie komentarzy i artykułów, nie musi mieć swojego źródła w kraju zalewanym tą propagandą. Równie dobrze przekaz ten może mieć swoje źródło w każdym innym państwie korzystającym z właściwych programów i usług.

W aspekcie prawnym TOR, TAILS i proxy to narzędzia legalne. T. Ciborski podkreśla, że anonimowa sieć (…) *służy wolności słowa, prywatności i prawom*

[39] niebezpiecznik.pl/post/silk–road–największy-sklep-z-narkotykami-w-internecie-zamkniety-fbi-namierzylo-i-aresztowalo-jego-tworce/ [dostęp: 1 V 2015].

człowieka[40]. Rosnąca popularność tych narzędzi sprawia jednak, że organy właściwe do demaskowania zalewu propagandowego, zwalczania przestępstw komputerowych oraz przestępczości zorganizowanej w sieci znajdują się w trudnej sytuacji.

W związku z tym pojawia się pytanie, jak walczyć z elementami wojny hybrydowej, które mają ścisły związek z agresją informacyjną? R. Brzeski stworzył swoisty katalog zaleceń, wśród których wymienia m.in.[41]:

- ostrożność przed akceptowaniem wszystkiego, co się czyta, słyszy i widzi,
- poszerzanie wiedzy (na każdy temat) w możliwie największym zakresie,
- weryfikację informacji w różnych źródłach,
- prowadzenie tzw. kontrpropagandy.

W Internecie pojawiają się takie ruchy, jak serwis stopfake.org założony 2 marca 2014 r. Witryna ta zrzesza ludzi, którzy odnajdują kłamstwa w przekazie[42]. Niemniej jednak, w przypadku braku skutecznych narzędzi do wykrywania i zwalczania źródeł dezinformacji, działalność informacyjna w cyberprzestrzeni będzie najprawdopodobniej nadal wykorzystywana w ramach wojen hybrydowych.

[40] T. Ciborski, *Ukryta tożsamość…*, s. 108.
[41] R. Brzeski, *Wojna informacyjna…*, s. 271–286.
[42] www.stopfake.org/en/about–us/ [dostęp: 7 IX 2015].

O autorach

Jolanta Darczewska – dr, Ośrodek Studiów Wschodnich im. Marka Karpia.

Kamil Kucharski – Agencja Bezpieczeństwa Wewnętrznego.

Krzysztof Liedel – dr, dyrektor Centrum Badań nad Terroryzmem Collegium Civitas.

Łukasz Skoneczny – Agencja Bezpieczeństwa Wewnętrznego.

Michał Wojnowski – dr, Instytut Pamięci Narodowej, Oddział w Rzeszowie

Piotr Żochowski – Ośrodek Studiów Wschodnich im. Marka Karpia.