ISSN 1896-4923
e-ISSN 2956-8536

2024/45
KWARTALNIK

BEZPIECZEŃSTWO NARODOWE

BBN

2024/45
KWARTALNIK

BEZPIECZEŃSTWO NARODOWE

Adres redakcji:
ul. Karowa 10, 00-315 Warszawa
Tel.: +48 22 695 18 96, Faks: +48 22 695 18 01
E-mail: redakcja@bbn.gov.pl

Projekt graficzny okładki: Tomasz Czapski

Wydawca: Biuro Bezpieczeństwa Narodowego
ul. Karowa 10, 00-315 Warszawa

Numer ISSN 1896-4923
Numer e-ISSN 2956-8536

Elektroniczna wersja czasopisma dostępna jest na stronie https://www.bezpieczenstwo-narodowe.pl oraz www.bbn.gov.pl

Nakład: 250 sztuk

Artykuły zamieszczone w czasopiśmie są recenzowane.

Opinie wyrażone w artykułach są poglądami autorów i nie muszą odzwierciedlać oficjalnego stanowiska Biura Bezpieczeństwa Narodowego.

Spis treści

Od redakcji 5

Krzysztof Kaczmarek
Konsekwencje dezinformacji: przegląd wybranych narzędzi i technik manipulacji 11

Łukasz Dryblak
Rola i znaczenie rosyjskich dokumentów doktrynalnych, ze szczególnym uwzględnieniem doktryn bezpieczeństwa informacyjnego z 2000 i 2016 roku 29

Marek Wrzosek
Rosyjska dezinformacja w konflikcie zbrojnym w Ukrainie 61

Paweł Pelc
Cyberprzestrzeń jako element walki informacyjnej – doświadczenia z konfliktu w Ukrainie 89

Stanisław Waszczykowski
Sztuczne obiekty i sprzęt wojskowy jako element dezinformacji wojskowej. Przykłady zastosowanych celów pozornych przez Siły Zbrojne Ukrainy podczas konfliktu zbrojnego z Federacją Rosyjską 111

Notka biograficzna 133

Table of content

Editorial 5

Krzysztof Kaczmarek
Consequences of disinformation: overview of selected manipulation tools and techniques 11

Łukasz Dryblak
The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016 29

Marek Wrzosek
Russian disinformation in the armed conflict in Ukraine 61

Paweł Pelc
Cyberspace as an element of information warfare – experience from the conflict in Ukraine 89

Stanisław Waszczykowski
Artificial military objects and equipment as an element of military deception. Examples of using dummy targets by the Ukrainian Armed Forces during the armed conflict with the Russian Federation 111

About the Authors 133

Od Redakcji

Szanowni Państwo,
dezinformacja staje się obecnie jednym z istotniejszych wyzwań bezpieczeństwa dla państw, rządów, instytucji międzynarodowych oraz społeczeństw na całym świecie. W dobie powszechnej informatyzacji, dynamicznie rozwijającej się sztucznej inteligencji i mediów społecznościowych rozprzestrzenianie fałszywych danych i informacji prowadzi do różnego rodzaju form destabilizacji politycznej, podważania społecznego zaufania, a także wzrostu polaryzacji i podziałów międzyludzkich. W rezultacie mamy do czynienia z trwałymi i systematycznymi działaniami, które osłabiają bezpieczeństwo narodowe i międzynarodowe.

Wypracowanie skutecznych strategii ochrony społeczeństw przed manipulacją informacyjną wymaga zastosowania wielowymiarowego podejścia i kompleksowych działań łączących wysiłki edukacyjne, prawne czy też technologiczne wielu podmiotów i instytucji. Jednym ze środków służących rozwojowi skutecznych strategii jest z pewnością podnoszenie świadomości naszego społeczeństwa na temat współczesnej dezinformacji. Te działania pozwalają na ograniczenie jej negatywnego wpływu i budowanie odporności na fałszywe treści. Temu celowi służy również niniejsza publikacja.

W artykule autorstwa dr. Krzysztofa Kaczmarka pt. „Konsekwencje dezinformacji: przegląd wybranych narzędzi i technik manipulacji" została podkreślona istotność dezinformacji i konieczność podjęcia działań zwiększających odporność społeczną na manipulację. Zwrócona została uwaga na stosowanie szerokiej gamy technik dezinformacyjnych, których celem jest wywoływanie chaosu informacyjnego i destabilizacja społeczeństw oraz brak skutecznych narzędzi pozwalających na pełne wyeliminowanie tego zagrożenia.

Podkreślono również wagę budowania świadomości społecznej i kontynuacji edukacji w zakresie przeciwdziałania dezinformacji czy cyberzagrożeniom, co stanowi stały element strategii obronnej.

Dr Łukasz Dryblak w kolejnym opracowaniu pt. „Rola i znaczenie rosyjskich dokumentów doktrynalnych, ze szczególnym uwzględnieniem doktryn bezpieczeństwa informacyjnego z 2000 i 2016 roku" zawraca uwagę na wciąż obecne w rosyjskich doktrynach oraz dokumentach strategicznych elementy sowieckiej filozofii informacyjnego wpływu. Stosując dezinformację i kontrolę informacyjną, Rosja prowadzi politykę odbudowy swojej strefy wpływów. Wykorzystuje przy tym panslawistyczne i eurazjatyckie narracje będące przeciwwagą dla kultury „dekadenckiego" Zachodu. To podejście jest wykorzystywane do prowadzenia dezinformacji skierowanej zarówno do własnego społeczeństwa, jak i zewnętrznego odbiorcy. Autor podkreśla również fakt nadania w Rosji wysokiego priorytetu kontroli informacyjnej, która jest realizowana poprzez rozwój własnego przemysłu nowych technologii informatycznych oraz ograniczanie wpływów zachodnich.

Prof. Marek Wrzosek w opracowaniu „Rosyjska dezinformacja w konflikcie zbrojnym w Ukrainie" przekonuje, że rosyjska dezinformacja jest kluczowym elementem operacji informacyjnych prowadzonych równolegle z działaniami militarnymi w Ukrainie. Ukierunkowana na destabilizację sytuacji oraz osłabianie morale zarówno Ukraińców, jak i społeczności międzynarodowej, wykorzystuje różnorodne kanały medialne, by wzbudzać strach przed rzekomym zagrożeniem ze strony Ukrainy i NATO, jak również zdyskredytować ukraińskie władze, przedstawiając je jako nielegalne i niekompetentne, niezdolne do samodzielnego rządzenia oraz winne prześladowania rosyjskich mniejszości. Autor podkreśla, że z biegiem trwania konfliktu Rosja wprowadza nowe wątki narracyjne, m.in. sugerując możliwość użycia broni nuklearnej, wyolbrzymiając własne zdolności bojowe przy jednoczesnym umniejszaniu skuteczności działaniom ukraińskim czy też sugeruje ambicje terytorialne Polski względem Ukrainy.

Paweł Pelc w artykule „Cyberprzestrzeń jako element walki informacyjnej – doświadczenia z konfliktu w Ukrainie" przekonuje, że od 2014 r. Rosja wykorzystuje cyberprzestrzeń do prowadzenia wojny informacyjnej, oddziałując zarówno na Ukrainę, jak i kraje trzecie. Twierdzi, że rosyjskie działania w cyberprzestrzeni służą dezinformacji, zdobywaniu dostępu do infrastruktury krytycznej, a także zasobów informacyjnych Ukrainy. Cyberataki, skoordynowane z operacjami kinetycznymi, wzmacniają efektywność rosyjskich działań wojennych oraz skutecznie wpływają na destabilizację państwa ukraińskiego i kształtowanie zachodniej opinii publicznej. Autor podkreśla również znaczenie i konieczność implementacji zbieranych doświadczeń z wojny w Ukrainie dla systemu bezpieczeństwa Polski, wskazując jednocześnie konieczność rozwoju narodowych zdolności obronnych w cyberprzestrzeni oraz gotowość do przeciwdziałania kampaniom dezinformacyjnym.

W ostatnim opracowaniu, „Sztuczne obiekty i sprzęt wojskowy jako element dezinformacji wojskowej. Przykłady zastosowanych celów pozornych przez Siły Zbrojne Ukrainy podczas konfliktu zbrojnego z Federacją Rosyjską", Stanisław Waszczykowski przekonuje, że zastosowanie sztucznych obiektów jako środka pozoracji w dalszym ciągu stanowi skuteczne narzędzie dezinformacji wojskowej i jest kluczowym elementem obrony. Autor dowodzi, że Ukraina stosując liczne środki maskujące – makiety systemów rakietowych, radarowych, artyleryjskich, czołgów – skutecznie chroni własny sprzęt wojskowy i tym samym zmusza Rosjan do marnowania znacznych i kosztownych zasobów bojowych. Z kolei produkcja makiet, która jest relatywnie tania, sprzyja rozwojowi przemysłowego potencjału obronnego i wzmacnia współpracę cywilno-wojskową. Autor przekonuje, że doświadczenia z wykorzystania sztucznych obiektów i sprzętu wojskowego mogą stanowić cenny wkład w rozwój Sił Zbrojnych RP oraz systemu obronnego.

Szanowni Państwo, choć jako Redakcja jesteśmy świadomi, że zamieszone w Kwartalniku opracowania tylko w nieznaczny sposób poruszają złożoną materię współczesnego zjawiska dezinformacji, niemniej jednak są w stanie w pewien sposób uwrażliwić nasze

społeczeństwo na tę problematykę. Poddając ją pod namysł, inspirujemy również naszych decydentów politycznych i wojskowych do objęcia jej szczególną uwagą i trwałego uwzględnienia w pracach przy budowie odporności państwa, by móc skutecznie stawić czoło obecnym i przyszłym zagrożeniom bezpieczeństwa.

Z życzeniami inspirującej lektury

gen. bryg. dr hab. inż. Mariusz Fryc

Redaktor Naczelny

Szanowni Państwo,
pełniona przeze mnie funkcja redaktora naczelnego kwartalnika „Bezpieczeństwo Narodowe” dobiegła końca. Z tej okazji chciałbym serdecznie podziękować wszystkim, którzy wspierali mnie w tym niezwykle ważnym i inspirującym przedsięwzięciu.

Pragnę wyrazić wdzięczność Autorom, Recenzentom i całemu mojemu Zespołowi redakcyjnemu za Państwa profesjonalizm, zaangażowanie i wsparcie. Dzięki Państwa pracy mogliśmy wspólnie tworzyć platformę wymiany myśli strategicznej na najwyższym poziomie, przyczyniając się tym samym do rozwoju wiedzy oraz jej praktycznej implementacji w dziedzinie bezpieczeństwa narodowego.

Szczególne podziękowania kieruję także do Czytelników Kwartalnika, których zainteresowanie i zaufanie były dla mnie nieustannym źródłem motywacji oraz satysfakcji.

Życzę sukcesów mojemu następcy oraz dalszego rozwoju Kwartalnika. Jestem przekonany, że pod nowym kierownictwem czasopismo będzie kontynuowało swoją dotychczasową misję z równie wielką pasją i profesjonalizmem.

Z wyrazami szacunku,

gen. bryg. dr hab. inż. Mariusz Fryc

DOI:10.59800/bn/196693

dr Krzysztof Kaczmarek[1]
Wydział Humanistyczny, Politechnika Koszalińska, Polska

KONSEKWENCJE DEZINFORMACJI: PRZEGLĄD WYBRANYCH NARZĘDZI I TECHNIK MANIPULACJI

CONSEQUENCES OF DISINFORMATION: OVERVIEW OF SELECTED MANIPULATION TOOLS AND TECHNIQUESI

Abstrakt: Prawidłowe funkcjonowanie współczesnych społeczeństw, państw i struktur ponadnarodowych bazuje na dostępie do informacji. Wolny obieg informacji jest efektem rozwoju cywilizacyjnego. Przestrzeń informacyjna stała się zaś naturalnym środowiskiem człowieka ery cyfrowej. Ze wszystkimi swoimi korzyściami poznawczymi niesie to za sobą jednak różne niebezpieczeństwa, w tym rozprzestrzenianie się dezinformacji. Mimo że to zjawisko stanowi poważne zagrożenie, państwa demokratyczne nie dysponują żadnym narzędziem pozwalającym na skuteczną obronę przed nim. Dezinformacja, jako element oddziaływania psychologicznego, jest niekinetyczną bronią wykorzystywaną w czasie wojny, w związku z tym istotne staje się znalezienie sposobu na zwiększenie na nią odporności społeczeństwa.

Słowa kluczowe: socjotechnika, oddziaływanie psychologiczne, manipulacja, dezinformacja, postęp technologiczny

Abstract: The proper functioning of modern societies, states, and supranational entities is based on access to information. The free flow of information is a result of civilization's development, and the information space has become a natural environment for humans in the digital era. For all its cognitive benefits, it still carries various risks, including the risk of spreading misinformation. Even though this phenomenon constitutes

[1] https://orcid.org/0000-0001-8519-1667, krzysztof.kaczmarek@tu.koszalin.pl

a serious threat, democratic countries do not have any tool to effectively defend against it. As an element of psychological impact, disinformation is a non-kinetic weapon, used in times of war. It is, therefore, important to find a way to increase society's resistance to disinformation.

Keywords: social engineering, psychological impact, manipulation, disinformation, technological progress

Wprowadzenie

Pojęcie dezinformacji powstało w XIX w. w Rosji[2]. Nie jest ono jednoznacznie zdefiniowane w literaturze naukowej i bywa zamiennie używane z takimi terminami, jak fałszywa informacja i propaganda[3]. James Henry Fetzer określa dezinformację jako intencjonalne wprowadzanie odbiorców w błąd, często w kontekstach politycznych, religijnych i ideologicznych. Fetzer opisuje również różnicę między dezinformacją a fałszywą informacją i podkreśla, że różnice wynikają z intencji. Nieprawdziwe informacje mogą być bowiem rozpowszechniane przez osoby, które same zostały wprowadzone w błąd[4].

Wykorzystywanie narzędzi socjotechnicznych w celu kształtowania opinii, poglądów i zachowań społecznych miało swój początek w czasach kształtowania się pierwszych organizmów państwowych[5]. Na początku celem manipulacyjnych działań, odnoszących się najczęściej do świata nadprzyrodzonego, była legitymizacja władzy. Rozwój cywilizacyjny i postęp technologiczny powodowały jednak,

[2] M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, t. 266–267, nr 1–2, s. 227.

[3] N. Persily, J.A. Tucker, *Introduction*, w: N. Persily, J.A. Tucker (red.), *Social media and democracy: The State of the Field and Prospects for Reform*, Cambridge University Press, Cambridge 2020, s. 10.

[4] J.H. Fetzer, *Disinformation: The use of false information*, "Minds and machines" 2004, nr 14.

[5] Zob.: M. Nieć, *Kampania wyborcza – uwagi politologa o genezie idei*, „Roczniki Nauk Społecznych" 2012, t. 4, nr 3; M. Wolny, *Nauka Hipokratesa i rzymska propaganda. Zaraza na Sycylii w relacji Liwiusza (Liv. 25.26. 7–15)*, „Echa Przeszłości" 2016, t. 17.

że ewoluowały również wykorzystywane techniki wpływania na społeczeństwo.

Gdy uzyskanie społecznego poparcia okazało się konieczne do zdobycia władzy, opinia publiczna stała się areną manipulacji. Od połowy XVIII do początków XIX w. gazety były organami partii politycznych, odpowiednio dopasowującymi publikowane treści[6]. Później ich dochody zaczęły w coraz większym stopniu pochodzić z reklam. Część tytułów w dalszym ciągu opowiadała się za określonymi frakcjami politycznymi, ale deklarowała obiektywizm. Do końca XX w. gazety, magazyny, stacje radiowe i telewizyjne były dla społeczeństw jedynym źródłem informacji o świecie. Media określały parametry, według których definiowano to, co odbiegało od normy i było niedopuszczalne. Skrajne poglądy rzadko pojawiały się w mediach informacyjnych, chyba że jako przykłady tego, co wykraczało poza granice „normalności". Chociaż media miały rzekomo przedstawiać pełen zakres spraw społecznych, cechował je konformizm[7].

W kontekście działań manipulacyjnych i dezinformacyjnych największe jakościowe zmiany nastąpiły na początku XX w. wraz z upowszechnieniem się Internetu i szerszym dostępem do informacji. Przekaz, wcześniej jednokierunkowy, nabrał charakteru interaktywnego, a powszechny dostęp do sieci skutkował możliwością nie tylko uzyskania wiedzy na niemal każdy temat, lecz także dzielenia się własnymi poglądami i opiniami. Przestrzeń informacyjna stała się naturalnym środowiskiem człowieka ery cyfrowej. Wolny obieg informacji jest efektem rozwoju cywilizacyjnego, ale dodatkowo ze wszystkimi swoimi korzyściami poznawczymi niesie za sobą różne zagrożenia, w tym ryzyko rozprzestrzeniania się dezinformacji[8].

[6] C. Dornan, *Dezinformatsiya: The past, present and future of 'fake news'*, A Reflection Paper for the Canadian Commission for UNESCO, marzec 2017 r., s. 5, https://www.researchgate.net/profile/Christopher-Dornan/publication/335881115_Dezinformatsiya_The_past_present_and_future_of_'fake_news'_A_Reflection_Paper_for_the_Canadian_Commission_for_UNESCO/links/5d81a738a6fdcc12cb989feb/Dezinformatsiya-The-past-present-and-future-of-fake-news-A-Reflection-Paper-for-the-Canadian-Commission-for-UNESCO.pdf (dostęp: 29 marca 2024 r.).

[7] *ibidem.*

[8] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Institute for Local Self-Government Maribor, Maribor 2023, s. 89.

Należy jednak podkreślić, że korporacje, podmioty państwowe i politycy zawsze rozpowszechniali fałszywe i wprowadzające w błąd narracje, aby osiągnąć swoje cele ideologiczne. Nie jest to tylko problem internetowych platform informacyjnych i mediów społecznościowych[9]. Rozwój technologii informacyjnych i komunikacyjnych (*Information and Communication Technologies*, *ICT*) spowodował, że zmienił się sposób produkcji, dystrybucji i konsumpcji informacji. Powstały nowe narzędzia, oparte na ICT, mogące być wykorzystywane w działaniach dezinformacyjnych. Same cele tych działań jednak się nie zmieniły.

Pomimo wielu badań i analiz dotyczących zarówno dezinformacji, jak i wszelkich innych form wpływania na zachowania społeczne nie opracowano skutecznych środków obrony przed nimi. Nie wiadomo, czy w ogóle możliwe jest stworzenie skutecznych narzędzi ochrony przed dezinformacją i manipulacją. Jednocześnie pojawiają się poważne wątpliwości, czy wśród decydentów istnieje rzeczywista chęć walki z tymi zjawiskami.

Mimo że kampanie dezinformacyjne stanowią poważne zagrożenie, polityka Unii Europejskiej w tym zakresie opiera się na założeniu, że dezinformacja nie jest sama w sobie nielegalna, lecz szkodliwa[10]. Część badaczy tej problematyki zauważa, że nawet silne gospodarczo i militarnie państwa demokratyczne nie posiadają skutecznych narzędzi do zwalczania dezinformacji, a ich działania prewencyjne polegają jedynie na kampaniach informacyjno-edukacyjnych[11].

Głównym celem niniejszego artykułu jest znalezienie odpowiedzi na pytanie dotyczące skutecznej walki z dezinformacją. Hipoteza badawcza zakłada, że można jedynie ograniczyć wpływ dezinformacji na postawy i zachowania społeczne, oraz przyjmuje, że nie istnieje możliwość całkowitego wyeliminowania negatywnych konsekwencji

[9] R. Kuo, A. Marwick, *Critical disinformation studies: History, power, and politics*, "Harvard Kennedy School Misinformation Review" 2021, t. 2, nr 4, s. 3.

[10] R. Ó Fathaigh, N. Helberger, N. Appelman, *The perils of legally defining disinformation,* "Internet policy review" 2021, t. 10, nr 4, s. 2.

[11] K. Wasilewski, *Fake News and the Europeanization of Cyberspace*, "Polish Political Science Yearbook" 2021, t. 50, nr 4, s. 9.

tego zjawiska, zwłaszcza że dezinformacja ewoluuje i dostosowuje się do zmieniającego się środowiska informacyjnego.

W celu weryfikacji powyższej hipotezy zostanie przeprowadzone badanie literatury przedmiotu, co posłuży za podstawę teoretyczną badań. Większość danych i informacji dotyczących dezinformacji jest wprawdzie powszechnie dostępna, jednak analizy przeprowadzone w niniejszym artykule pozwolą je usystematyzować i dadzą możliwość wyciągnięcia nowych wniosków. Aby zobrazować możliwe skutki dezinformacji, zostanie dokonana interpretacja konkretnych przypadków.

Mechanizmy i narzędzia dezinformacji

Naturalne środowisko działań dezinformacyjnych to chaos informacyjny i emocjonalny charakter przekazów medialnych[12], a wywoływanie emocji to jeden z aspektów będących elementem wojny hybrydowej, wojny informacyjnej[13]. Jednocześnie nasilenie działań dezinformacyjnych może być sygnałem poprzedzającym inne negatywne zdarzenia. Jednak takie przesłanki często są ignorowane, a ich oczywistość dostrzegana dopiero po fakcie[14]. Tymczasem dezinformacja, jako element oddziaływania psychologicznego, jest niekinetyczną bronią wykorzystywaną w czasie wojny[15]. Znaczny wzrost działań dezinformacyjnych w polityce międzynarodowej

[12] K. Chałubińska-Jentkiewicz, *Disinformation–and what else?*, "Cybersecurity and Law" 2022, t. 6, nr 2, s. 14.

[13] K. Kaczmarek, *Appealing to compassion as an element of Russia's hybrid warfare against the West*, „Cybersecurity and Law" 2022, t. 7, nr 1, s. 52; A. Makuch, *„Psychological judo" Seftona Delmera – brytyjskie techniki dezinformacji w okresie II wojny światowej*, "Cybersecurity and Law" 2021, t. 5, nr 1, s. 163.

[14] B. Ćwik, *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, "Modern Management Review" 2017, t. 22, nr 3, s. 28.

[15] K.E. Derlatka, *Wielowymiarowość dezinformacji w wojnie – wybrane przykłady stosowania dezinformacji jako narzędzia wojny*, „Acta Universitatis Lodziensis. Folia Historica" 2023, nr 114, s. 226.

zaobserwowano od wybuchu pandemii COVID-19 w 2021 r.[16], a zetem w okresie niemal bezpośrednio poprzedzającym agresję Rosji na Ukrainę.

Podstawą skutecznej dezinformacji jest zbudowanie wiarygodności jej źródła[17]. Jednocześnie forma komunikatu musi być dostosowana do odbiorców. Wyniki badań wskazują na istnienie tendencji do łatwiejszego przyjmowania informacji zgodnych z wcześniejszymi przekonaniami i odrzucania lub unikania tych, które im zaprzeczają[18].

Obecnie do najczęściej wykorzystywanych metod i technik dezinformacyjnych należą:

- fałszywe wiadomości (*fake news*): tworzenie i rozpowszechnianie fałszywych informacji przypominających te prawdziwe i dotyczących sytuacji, które mogą wystąpić;
- propaganda: szeroko zakrojone działania oparte na emocjach, mające na celu promowanie określonego punktu widzenia. Propaganda może wykorzystywać zarówno prawdziwe, fałszywe, jak i zmanipulowane informacje;
- trolling i hejt: celowe wywoływanie konfliktów i nawoływanie do nienawiści poprzez umieszczanie kontrowersyjnych treści na platformach internetowych. Celem jest skompromitowanie dyskusji lub zdyskredytowanie określonych osób czy grup społecznych;
- astroturfing: tworzenie pozoru (sztucznego) poparcia dla jakiejś kwestii lub sprzeciwu wobec niej. Najczęściej odbywa się przez fałszywe konta w mediach społecznościowych;

[16] E.M. Włodyka, *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce*, w: M. Karpiuk (red.), *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024, s. 104.

[17] K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, t. 51, nr 2, s. 21.

[18] W.L. Bennett, S. Livingston, *A Brief History of the Disinformation Age: Information Wars and the Decline of Institutional Authority*, w: L. Bennett, S. Livingston (red.), *The Disinformation Age*, Cambridge University Press, Cambridge 2020, s. 5–6.

- selektywne dobieranie danych (*cherry picking*): dobór danych i informacji w taki sposób, aby potwierdziły one określoną tezę. Jednocześnie ignorowane są te, które mogłyby ją podważyć;
- teorie spiskowe: promowanie poglądu tłumaczącego niektóre zjawiska społeczne istnieniem spisku;
- szum informacyjny: zalew odbiorców dużą liczbą często sprzecznych lub mylących informacji;
- deep fake: wykorzystanie zaawansowanych narzędzi sztucznej inteligencji (*artificial intelligence,* AI) do tworzenia realistycznych, ale fałszywych obrazów przedstawiających sytuacje, które w rzeczywistości nigdy nie miały miejsca. Mogą to być wypowiedzi lub czynności, które stawiają określone osoby w kompromitującym je kontekście. Obecnie jest to najbardziej zaawansowane pod względem technologicznym narzędzie dezinformacji i manipulacji;
- gaslighting: psychologiczna technika manipulacji powodująca, iż ofiara kwestionuje swoją pamięć, percepcję i zdrowie psychiczne.

Często tłumaczenie zjawisk społecznych przy pomocy narzędzi i technik dezinformacji ma charakter pozornie logiczny. Należy jednak pamiętać, że wszelkie wywody przeprowadzone w takich kontekstach mają charakter sofizmatu.

Wydaje się, że świadomość zagrożeń związanych z dezinformacją oraz najczęściej stosowanych narzędzi i technik może stanowić jeden z elementów ograniczających jej konsekwencje. Jednak w rzeczywistości tak nie jest. Mimo że każdy odbiorca ma możliwość sprawdzenia wiarygodności źródła informacji, robi to zaledwie kilkanaście procent[19]. Jednocześnie osoby, które wierzą w teorie spiskowe, często są zmanipulowane w takim stopniu, że nie ma możliwości, by przyjęły do wiadomości jakiekolwiek logiczne argumenty[20], tym bardziej że pewne formy dezinformacji są wykorzystywane również przez państwa demokratyczne, np. na potrzeby polityki historycznej. Przykład

[19] *Polacy są świadomi dezinformacji, lecz i tak ulegają fake newsom*, Demagog, 23 lutego 2022 r., https://demagog.org.pl/analizy_i_raporty/polacy-sa-swiadomi-dezinformacji-lecz-i-tak-ulegaja-fake-newsom/ (dostęp: 29 marca 2024 r.).

[20] K. Kaczmarek, *Dezinformacja jako czynnik…*, *op. cit.*, s. 24.

stanowi Wielka Brytania, w której istnieje nawet sieć *History & Policy*, składająca się z ponad 500 historyków oferujących swoją wiedzę decydentom i dziennikarzom[21]. Ten przykład pokazuje, że przeciętny odbiorca może mieć trudności w odróżnieniu tego, co jest prawdziwą i obiektywną informacją, od tego, co zmanipulowane.

Prawidłowe funkcjonowanie współczesnych społeczeństw, państw i struktur ponadnarodowych w znacznym stopniu wynika z dostępu do wiarygodnych informacji[22]. Tempo rozpowszechniania się fałszywych informacji i potencjalne konsekwencje tego zjawiska sprawiają jednak, że jest ono porównywane do pandemii[23]. Fałszywe informacje mogą dotyczyć m.in. sposobów odżywiania się[24] czy leczenia[25]. Eksperci z dziedziny medycyny zwracają uwagę na zagrożenia, jakie niezweryfikowane informacje niosą na zdrowie i życie[26].

Można zatem postawić tezę, że dezinformacja jest integralną częścią infosfery i próbuje oddziaływać na społeczeństwa informacyjne, a jedyne, co można zrobić, to nauczyć się funkcjonować ze świadomością jej istnienia. Należy jednocześnie kontrolować i neutralizować te źródła dezinformacji, które mogą zagrażać bezpieczeństwu społeczeństwa i państwa. Zbyt radykalne wyeliminowanie wszystkich źródeł fałszywych i zmanipulowanych treści mogłoby wywołać efekt odwrotny do zamierzonego i dać pożywkę dla teorii spiskowych. Walka z dezinformacją powinna uwzględniać metody i cele atakującego. Podjęte kroki musi poprzedzać analiza przypadków,

[21] H. Tworek, *Disinformation: It's History*, Centre for International Governance Innovation, 14 lipca 2021 r., https://www.cigionline.org/articles/disinformation-its-history/ (dostęp: 29 marca 2024 r.).

[22] M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, "International Journal of Legal Studies" 2023, t. 14, nr 2, s. 647.

[23] E. Aïmeur, S. Amri, G. Brassard, *Fake News, Disinformation and Misinformation in Social Media: a Review*, "Social Network Analysis and Mining" 2023, t. 13, nr 1, s. 29–30.

[24] Por.: C. Diekman, C.D. Ryan, T.L. Oliver, *Misinformation and disinformation in food science and nutrition: impact on practice*, "The Journal of Nutrition" 2023, t. 153, nr 1, s. 3–4.

[25] Por.: J.H. Neylan, S.S. Patel, T.B. Erickson, *Strategies to counter disinformation for healthcare practitioners and policymakers*, "World medical & health policy" 2022, t. 14, nr 2, s. 428–429.

[26] Zob.: A.S. Kanekar, A. Thombre, *Fake medical news: avoiding pitfalls and perils*, "Family Medicine and Community Health" 2019, t. 7, nr 4, s. 1–2.

która nie tylko pozwoli na zidentyfikowanie atakującego, lecz także da możliwość przewidzenia jego następnych ruchów.

Studia przypadków

Najwięcej źródeł dezinformacji i manipulacji jest powiązanych z Federacją Rosyjską, co wynika z obecnej sytuacji międzynarodowej i agresywnych działań tego państwa. Zgodnie z praktykami wywiadu radzieckiego, a później rosyjskiego, dezinformacja zajmuje uprzywilejowaną pozycję w działaniach wywiadowczych i jest zintegrowana z funkcjonowaniem tego instrumentu państwowego. Zgodnie z modelem sowiecko-rosyjskim podstawowym celem działań wywiadowczych nie jest gromadzenie konkretnych informacji, ale wykorzystanie dezinformacji w taki sposób, aby osiągnąć pożądane cele strategiczne, operacyjne lub taktyczne[27]. Odbywa się to poprzez wpływanie na politykę innych rządów, podważanie zaufania do ich przywódców i instytucji, zakłócanie stosunków międzynarodowych oraz dyskredytowanie i osłabianie przeciwników[28].

Fałszywe treści i sposób ich rozpowszechniania zależą od celu ataku oraz aktualnego kontekstu politycznego, społecznego i ekonomicznego. Cechą wspólną tego typu działań jest wykorzystanie wcześniej utworzonych i uwiarygodnionych dla części odbiorców źródła informacji. W rzeczywistości informacje przez jakiś czas dostępne w tych źródłach mogą dotyczyć różnych dziedzin i zawierać zweryfikowane, prawdziwe treści. Dezinformacja może zacząć się w nich pojawiać niezauważalnie albo nagle i dotrzeć do dużej grupy odbiorców, z których część uzna je za sprawdzone i wiarygodne.

Jedną z cech fałszywej wiadomości jest to, że budzi ona skrajne emocje, najczęściej negatywne. W przypadku zaplanowanej akcji dezinformacyjnej mogą to być insynuacje lub oskarżenia określonej

[27] J. Mandić, D. Klarić, *Case study of the Russian disinformation campaign during the war in Ukraine – propaganda narratives, goals, and impacts*, "National security and the future" 2023, t. 24, nr 2, s. 100.

[28] H.R. Shultz, R. Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, Pergamon-Brassey's, Washington 1984, s. 2.

grupy społecznej o czyny nieakceptowane społecznie. Często celem dezinformacji nie jest atakowana w przekazach grupa, ale osłabienie państwa przez wywoływanie, podtrzymywanie i pogłębianie podziałów społecznych.

Jako przykład może posłużyć historia mieszkającej w Berlinie 13-letniej Lisy, która w 2016 r. została rzekomo porwana i wielokrotnie zgwałcona przez arabskiego uchodźcę. Wiadomość o tym wydarzeniu podały działające wówczas w Niemczech rosyjskie media. W efekcie doszło do antyimigranckich demonstracji, które transmitowano najpierw przez rosyjskie, a później ogólnoniemieckie i zagraniczne media. Mimo że do opisanego wydarzenia nigdy się nie doszło, spowodowało ono zaostrzenie społecznej i politycznej debaty na temat przyjmowania uchodźców[29].

Kampanie dezinformacyjne mogą również poprzedzać inne agresywne działania. W ciągu 48 godzin poprzedzających atak Rosji na Ukrainę (24 lutego 2022 r.) Instytut Badań Internetu i Mediów Społecznościowych (IBIMS) zaobserwował ponadnormatywną aktywność publikacyjną w polskiej przestrzeni informacyjnej treści, które miały wywołać poczucie zagrożenia ze strony obywateli Ukrainy[30]. Jedne z najczęściej pojawiających się w kontekście Ukrainy zwrotów to „banderowcy", „UPA", „rzeź Polaków", „ludobójstwo". Do dystrybucji tego tupu treści zostały wykorzystane konta wcześniej propagujące postawy antyszczepionkowe i/lub negujące istnienie wirusa SARS-CoV-2[31]. Inną kwestią są prorosyjskie działania np. Facebooka (Mety), który blokuje informacje o rzeczywistym przebiegu wojny[32]. Firma w oficjalnych komunikatach zapewnia, że udoskonala swoje

[29] S. Meister, *„Sprawa Lisy": Niemcy na celowniku rosyjskiej dezinformacji*, NATO review, 25 lipca 2016 r., https://www.nato.int/docu/review/pl/articles/2016/07/25/sprawa-lisy-niemcy-na-celowniku-rosyjskiej-dezinformacji/index.html (dostęp: 29 marca 2024 r.).

[30] *Komunikat ws. dezinformacji ws. sytuacji na Ukrainie w internecie*, Instytut Badań Internetu i Mediów Społecznościowych, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ (dostęp: 2 kwietnia 2024 r.).

[31] *ibidem.*

[32] *Więcej prorosyjskich, mniej proukraińskich treści. Tak Rosjanie oszukują Facebooka*, PolskieRadio.pl, 18 grudnia 2022 r., https://www.polskieradio.pl/399/7977/Artykul/3089097,Wiecej-prorosyjskich-mniej-proukrainskich-tresci-Tak-Rosjanie-oszukuja-Facebooka (dostęp: 2 kwietnia 2024 r.).

programy sprawdzania faktów i walki z dezinformacją, a treści są moderowane przez algorytmy AI[33]. Wydaje się jednak, że po dwóch latach od wybuchu wojny korporacje technologiczne wciąż nie są zainteresowane walką z rosyjską ani jakąkolwiek inną dezinformacją[34]. Nic nie wskazuje również na to, żeby sytuacja miała się w najbliższym czasie zmienić.

Kolejną akcją dezinformacyjną, która ma na celu zniechęcenie mieszkańców UE do wspierania Ukrainy, jest rozpowszechnianie fałszywych informacji o katastrofalnej sytuacji ekonomicznej wspólnoty, do której doszło na skutek ogromnych kosztów ponoszonych na rzecz pomocy Ukraińcom. Przykładem jest „ujawniony tajny plan" dotyczący zajmowania kont bankowych obywateli UE[35]. Tego typu informacje zostają przyjęte za wiarygodne przez tę część społeczeństwa, która jest podatna na teorie spiskowe.

Każda fałszywa informacja może być częścią szerszej kampanii dezinformacyjnej. Jak wskazują wymienione przykłady, konsekwencje fake newsów dotyczą całego społeczeństwa, nawet jeżeli w ich prawdziwość wierzy jedynie niewielka jego część. Dotyczy to zwłaszcza ustrojów demokratycznych, w których nawet mała zmiana preferencji wyborczych jest w stanie zadecydować o przyszłych kierunkach polityki zagranicznej i bezpieczeństwa. Fałszywa informacja powoduje czasem również niepokoje społeczne i osłabienie wewnętrzne państwa, co jest najczęściej głównym celem akcji dezinformacyjnej.

[33] J. Burke, *Facebook struggles as Russia steps up presence in unstable west Africa*, „The Guardian", 17 kwietnia 2022 r., https://www.theguardian.com/world/2022/apr/17/facebook-struggles-as-russia-steps-up-presence-in-unstable-west-africa (dostęp: 2 kwietnia 2024 r.).

[34] *Walka z algorytmami. UE wzywa Google i Facebook, aby promowały niezależne media*, Belsat.eu, 8 stycznia 2024 r., https://belsat.eu/pl/news/08-01-2024-walka-z-algorytmami-ue-wzywa-google-i-facebook-aby-promowaly-niezalezne-media (dostęp: 2 kwietnia 2024 r.).

[35] A. Wolska, *Fejk tygodnia: UE jest na krawędzi bankructwa, więc będą zajmowane oszczędności obywateli*, EURACTIV.pl, 15 marca 2024 r., https://www.euractiv.pl/section/demokracja/news/fejk-tygodnia-ue-jest-na-krawedzi-bankructwa-wiec-beda-zajmowane-oszczednosci-obywateli/ (dostęp: 2 kwietnia 2024 r.).

Wnioski i podsumowanie

Każda teoria spiskowa ma swoich zagorzałych wyznawców. Również każda fałszywa wiadomość jest przyjmowana za prawdę przez jakąś część jej odbiorców. Podatność społeczeństwa na fake newsy zależy od wielu czynników, takich jak wykształcenie, sytuacja ekonomiczna, wyznawane wartości, stan zdrowia czy poczucie bezpieczeństwa. Podejmowane są pewne próby zbadania sposobu, w jaki społeczeństwa postrzegają dezinformację. Według Eurostatu w 2021 r. w Unii Europejskiej 47 proc. osób w wieku od 16 do 74 lat spotkało się z fałszywymi informacjami, lecz jedynie 23 proc. je zweryfikowało. Odsetek osób, które weryfikowały informacje znalezione w internetowych serwisach informacyjnych lub mediach społecznościowych, był największy w Holandii (45 proc.), Luksemburgu (41 proc.) i Irlandii (39 proc.), a najmniejszy na Litwie (11 proc.), w Rumunii (12 proc.) i Polsce (16 proc.)[36].

Te wyniki w żaden sposób nie opisują podatności społeczeństwa na dezinformację. Niski odsetek weryfikujących może świadczyć o tym, że członkowie danego społeczeństwa wierzą w większość informacji, które do nich docierają, ale może również dowodzić krytycznego podejścia do wiadomości i samodzielnego identyfikowania fake newsów.

Analizy przeprowadzone w niniejszym artykule wskazują na to, że obecnie nie istnieje możliwość całkowitego wyeliminowania wypływu dezinformacji na społeczeństwa demokratyczne – da się jedynie ograniczyć ich wpływ. Postawiona na początku artykułu hipoteza badawcza została zatem zweryfikowana pozytywnie.

Należy podkreślić, że głównym źródłem informacji dla społeczeństwa cyfrowego jest Internet. Walka z dezinformacją powinna dlatego wpisywać się w strategie cyberbezpieczeństwa, a akcje dezinformacyjne należy traktować jako formę cyberataku. Zdecydowana większość skutecznych cyberataków jest wynikiem błędu człowieka, a nie

[36] *How many people verified online information in 2021?*, Eurostat, 16 grudnia 2021 r., https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211216-3 (dostęp: 3 kwietnia 2024 r.).

nieprawidłowo działających technicznych zabezpieczeń[37]. Wobec tego jedynym sposobem walki z dezinformacją wydaje się budowanie społecznej świadomości cyberzagrożeń, co z kolei wymaga odpowiedniego modelu kształcenia zawodowego i uniwersyteckiego[38]. Kształcenie powinno opierać się na praktycznej wiedzy i umiejętnościach osób je prowadzących. Nie wystarczą bowiem same założenia i programy nauczania. W przypadku kiedy prowadzący zajęcia lub kursy dysponuje jedynie wiedzą teoretyczną, nie ma możliwości przekazania odpowiednich wiadomości i ukształtowania umiejętności.

Obecnie cały zachodni świat jest w stanie wojny z totalitarnymi reżimami. Ten konflikt toczy się w większości w cyberprzestrzeni, ale niesie za sobą rzeczywiste negatywne konsekwencje, dlatego w każdej sytuacji należy brać pod uwagę, że jest się celem dezinformacji. Jedynie założenie, że każda informacja czy wiadomość jest potencjalnie fałszywa, pozwala zmniejszyć podatność na dezinformację. W takich przypadkach trzeba brać pod uwagę również szybkość postępu technologicznego, który pozwala tworzyć fake newsy w jakości niemal uniemożliwiającej ich samodzielną weryfikację. Jednocześnie nawet wcześniej pozytywnie zweryfikowane źródło informacji może stać się źródłem dezinformacji.

[37] E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, "Cybersecurity and Law" 2022, t. 7, nr 1, s. 216.

[38] M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, "Cybersecurity and Law" 2021, t. 5, nr 1, s. 48.

Bibliografia
Referencs List

Aïmeur E., Amri S., Brassard G., *Fake News, Disinformation and Misinformation in Social Media: a Review*, "Social Network Analysis and Mining" 2023, t. 13, nr 1.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Institute for Local Self-Government Maribor, Maribor 2023.

Bennett W.L., Livingston S., *A Brief History of the Disinformation Age:Information Wars and the Decline of Institutional Authority*, w: Bennett L., Livingston S. (red.), *The Disinformation Age*, Cambridge University Press, Cambridge 2020.

Burke J., *Facebook struggles as Russia steps up presence in unstable west Africa*, "The Guardian", 17 kwietnia 2022 r., https://www.theguardian.com/world/2022/apr/17/facebook-struggles-as-russia-steps-up-presence-in-unstable-west-africa (dostęp: 2 kwietnia 2024 r.).

Chałubińska-Jentkiewicz K., *Disinformation–and what else?*, "Cybersecurity and Law" 2022, t. 6, nr 2.

Ćwik B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, "Modern Management Review" 2017, t. 22, nr 3.

Derlatka K.E., *Wielowymiarowość dezinformacji w wojnie – wybrane przykłady stosowania dezinformacji jako narzędzia wojny*, „Acta Universitatis Lodziensis. Folia Historica" 2023, nr 114.

Diekman C., Ryan C.D., Oliver T.L., *Misinformation and disinformation in food science and nutrition: impact on practice*, "The Journal of Nutrition" 2023, t. 153, nr 1.

Dornan C., *Dezinformatsiya: The past, present and future of 'fake news'*, A Reflection Paper for the Canadian Commission for UNESCO, marzec 2017 r., https://www.researchgate.net/profile/Christopher-Dornan/publication/335881115_Dezinformatsiya_The_past_present_and_future_of_'fake_news'_A_Reflection_Paper_for_the_Canadian_Commission_for_UNESCO/links/5d81a738a6fdcc12cb989feb/Dezinformatsiya-The-past-present-and-future-of-fake-news-A-Reflection-Paper-for-the-Canadian-Commission-for-UNESCO.pdf (dostęp: 29 marca 2024 r.).

Fetzer J.H., *Disinformation: The use of false information*, "Minds and machines" 2004, nr 14.

How many people verified online information in 2021?, Eurostat, 16 grudnia 2021 r., https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211216-3 (dostęp: 3 kwietnia 2024 r.).

Kaczmarek K., *Appealing to compassion as an element of Russia's hybrid warfare against the West*, "Cybersecurity and Law" 2022, t. 7, nr 1.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, t. 51, nr 2.

Kanekar A.S., Thombre A., *Fake medical news: avoiding pitfalls and perils*, "Family Medicine and Community Health" 2019, t. 7.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, "Cybersecurity and Law" 2021, t. 5, nr 1.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, "International Journal of Legal Studies" 2023, t. 14, nr 2.

Komunikat ws. dezinformacji ws. sytuacji na Ukrainie w internecie, „Instytut Badań Internetu i Mediów Społecznościowych", https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ (dostęp: 2 kwietnia 2024 r.).

Kuo R., Marwick A., *Critical disinformation studies: History, power, and politics*, "Harvard Kennedy School Misinformation Review" 2021, t. 2, nr 4.

Makuch A., *„Psychological judo" Seftona Delmera – brytyjskie techniki dezinformacji w okresie II wojny światowej*, "Cybersecurity and Law" 2021, t. 5, nr 1.

Mandić J., Klarić D., *Case study of the Russian disinformation campaign during the war in Ukraine – propaganda narratives, goals, and impacts*, "National security and the future" 2023, t. 24, nr 2.

Meister S., *„Sprawa Lisy": Niemcy na celowniku rosyjskiej dezinformacji*, „NATO review", 25 lipca 2016 r., https://www.nato.int/docu/review/pl/articles/2016/07/25/sprawa-lisy-niemcy-na-celowniku-rosyjskiej-dezinformacji/index.html (dostęp: 29 marca 2024 r.).

Neylan J.H., Patel S.S., Erickson T.B., *Strategies to counter disinformation for healthcare practitioners and policymakers*, "World medical & health policy" 2022, t. 14, nr 2.

Nieć M., *Kampania wyborcza – uwagi politologa o genezie idei*, „Roczniki Nauk Społecznych" 2012, t. 4, nr 3.

Ó Fathaigh R., Helberger N., Appelman N., *The perils of legally defining disinformation*, "Internet policy review" 2021, t. 10, nr 4.

Persily N., Tucker J.A., *Introduction*, w: Persily N., Tucker J.A. (red.), *Social media and democracy: The State of the Field and Prospects for Reform*, Cambridge University Press, Cambridge 2020.

Polacy są świadomi dezinformacji, lecz i tak ulegają fake newsom, Demagog, 23 lutego 2022 r., https://demagog.org.pl/analizy_i_raporty/polacy-sa-swiadomi-dezinformacji-lecz-i-tak-ulegaja-fake-newsom/ (dostęp: 29 marca 2024 r.).

Shultz H.R., Godson R., *Dezinformatsia: Active Measures in Soviet Strategy*, Pergamon-Brassey's, Washington 1984.

Tworek H., *Disinformation: It's History*, Centre for International Governance Innovation, 14 lipca 2021 r., https://www.cigionline.org/articles/disinformation-its-history/ (dostęp: 29 marca 2024 r.).

Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, t. 266–267, nr 1–2.

Walka z algorytmami. UE wzywa Google i Facebook, aby promowały niezależne media, Belsat.eu, 8 stycznia 2024 r., https://belsat.eu/pl/news/08-01-2024-walka-z-algorytmami-ue-wzywa-google-i-facebook-aby-promowaly-niezalezne-media (dostęp: 2 kwietnia 2024 r.).

Wasilewski K., *Fake News and the Europeanization of Cyberspace*, "Polish Political Science Yearbook" 2021, t. 50, nr 4.

Więcej prorosyjskich, mniej proukraińskich treści. Tak Rosjanie oszukują Facebooka, PolskieRadio.pl, 18 grudnia 2022 r., https://www.polskieradio.pl/399/7977/Artykul/3089097,Wiecej-prorosyjskich-mniej-proukrainskich-tresci-Tak-Rosjanie-oszukuja-Facebooka (dostęp: 2 kwietnia 2024 r.).

Włodyka E.M., *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce*, w: Karpiuk M. (red.),

Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, "Cybersecurity and Law" 2022, t. 7, nr 1.

Wolny M., *Nauka Hippokratesa i rzymska propaganda. Zaraza na Sycylii w relacji Liwiusza (Liv. 25.26. 7–15)*, „Echa Przeszłości" 2016, t. 17.

Wolska A., *Fejk tygodnia: UE jest na krawędzi bankructwa, więc będą zajmowane oszczędności obywateli*, EURACTIV.pl, 15 marca 2024 r., https://www.euractiv.pl/section/demokracja/news/fejk-tygodnia-ue-jest-na-krawedzi-bankructwa-wiec-beda-zajmowane-oszczednosci-obywateli/ (dostęp: 2 kwietnia 2024 r.).

DOI:10.59800/bn/196690

dr Łukasz Dryblak[1]
Instytut Historii im. Tadeusza Manteuffla PAN, Warszawa, Polska

ROLA I ZNACZENIE ROSYJSKICH DOKUMENTÓW DOKTRYNALNYCH ZE SZCZEGÓLNYM UWZGLĘDNIENIEM DOKTRYN BEZPIECZEŃSTWA INFORMACYJNEGO Z 2000 I 2016 ROKU[1]

THE ROLE AND SIGNIFICANCE OF RUSSIAN DOCTRINAL DOCUMENTS WITH PARTICULAR FOCUS ON INFORMATION SECURITY DOCTRINES FROM 2000 AND 2016[2]

Abstrakt: Autor artykułu stawia sobie za zadnie przeanalizowanie roli rosyjskich dokumentów doktrynalnych oraz ich wartości w kontekście polityki rosyjskiej. Podkreśla ciągłość sowieckiej i rosyjskiej myśli wojskowej, która znajduje odzwierciedlenie m.in. w sposobie formułowania i używania przez Rosję dokumentów doktrynalnych. Na przykładzie wspomnianych dokumentów podkreśla on ofensywny charakter działań Kremla, który pod pretekstem obrony rosyjskiej tożsamości realizuje starą politykę imperialną.

Słowa kluczowe: ZSRR, doktryna wojenna Federacji Rosyjskiej, doktryna informacyjna, dezinformacja, strategia informacyjna, rosyjska narracja polityczna, *Russkij mir*, sowietologia

[1] https://orcid.org/0000-0002-7459-5700, ldryblak@bbn.gov.pl

[2] Niniejszy artykuł stanowi rozszerzoną i zaktualizowaną wersję tekstu opublikowanego wyłącznie w wersji anglojęzycznej w „Studiach z Dziejów Rosji i Europy Środkowo-Wschodniej". Por. Ł. Dryblak, *The role and significance of Russian doctrinal documents, with particular focus on information security doctrines from 2000 and 2016*, SDR, LII, 2017, s. 209-229.

Abstract: The author underlines the continuity of the Soviet and Russian military thought, reflected also in the way Russia formulates and uses doctrinal documents. Using the example of these documents, he emphasises the offensive character of Kremlin's actions, which under the pretext of defending Russian identity implements the old imperial policy.

Keywords: USSR, disinformation, Russkiy Mir, Russian Federation military doctrine, information doctrine, information strategy, Russian political narration, Sovietology

Wprowadzenie

Od lat 30. XX w. sowietolodzy podkreślali, że kierownictwo Związku Socjalistycznych Republik Sowieckich prowadząc politykę zagraniczną, kierowało się klasyczną zasadą Carla von Clausewitza – „Wojna jest tylko dalszym ciągiem polityki prowadzonej innymi środkami"[3]. Zwolennikiem tej definicji wojny był Władimir Lenin[4]. Płynna granica pomiędzy stanem wojny a pokoju u Clausewitza znalazła również odzwierciedlenie w sowieckiej myśli wojskowej, którą cechowało łączenie strategii politycznej z militarną oraz podporządkowanie ekspansywnej ideologii komunistycznej, zakładającej ciągłą konfrontację „świata kapitalistycznego" z blokiem komunistycznym[5]. Ten schemat pojmowania rzeczywistości nadal stanowi podstawę rosyjskiej myśli wojskowej i politycznej.

[3] C. Clausevitz, *O wojnie*, Wydawnictwo Mireki, Warszawa 2010, s. 29.

[4] Jednymi z pierwszych, którzy podkreślali ten fakt, byli polscy sowietolodzy Jerzy Niezbrzycki ps. Ryszard Wraga oraz Włodzimierz Bączkowski. Por.: R. Wraga, *Gwarancje Pana Otmara*, „Bunt Młodych" 1935, nr 10, s. 4–5; *idem*, *Geopolityka, strategia i granice*, Tel Awiw 1943, s. 21; W. Bączkowski, *Uwagi o istocie siły rosyjskiej*, „Wschód-Orient" 1938, nr 4, http://www.omp.org.pl/artykul.php?artykul=115 (dostęp: 13 kwietnia 2017 r.); i*dem*, *Rosja wczoraj i dziś*, Jerozolima 1946, s. 17. Z czasem ten pogląd wszedł również do kanonu światowej sowietologii: R.L. Garthoff, *Soviet military doctrine [Radziecka doktryna wojskowa]*, RAND Corporation, Illinois 1953, s. 10. Ostatnio o znaczeniu notatek Lenina na marginesie Clausewitza pisał także: A. Nowak, *Powrót „Imperium Zła". Ideologie współczesnej Rosji, ich twórcy i krytycy (1913–2023)*, Kraków 2023, s. 26–27.

[5] Za Leninem do Clausewitza odwoływali się najważniejsi sowieccy wojskowi teoretycy: Michaił Frunze, Aleksandr Swieczin, Michaił Tuchaczewski, Wasilij Sokołowski i inni. Zob.: R.L. Garthoff, *op. cit.*, s. 12.

W latach 80. XX w. w wyniku dużego zapóźnienia technologicznego i gospodarczego w stosunku do Zachodu w ZSRS dokonano transformacji systemowej. Komunizm przestał być ideologią spajającą wielonarodowe państwo. W 1986 r. Alain Besançon zwrócił uwagę, że „jeśli zniszczy się ideologię, naród wielkorosyjski nie będzie miał czym jej zastąpić”[6]. Elity sowieckie również zdawały sobie z tego sprawę i równolegle z procesem *pierestrojki* podjęły działania mające na celu utrzymanie dominacji nad narodami bloku wschodniego – koniec ZSRS nie oznaczał końca rosyjskich aspiracji imperialnych[7]. W sformułowaniu nowej ideologii imperialnej pomogli emigranci rosyjscy, którzy w swych koncepcjach naukowych i politycznych często poszukiwali innej formy konsolidacji imperium aniżeli poprzez ideologię komunistyczną[8]. Jedność i niepodzielność ziem Rosji, często sakralizowana, była wartością, co do której zarówno wśród emigracji rosyjskiej, jak i mieszkańców ZSRS, poza pewnymi wyjątkami, nie było wątpliwości[9]. Rządy Władimira

[6] A. Besançon, *Imperium rosyjskie i panowanie sowieckie*, w: J. Karpiński, I. Lasota (red.), *Sowietskij Sojuz. Wybór*, Wrocław 1989, s. 18.

[7] Słusznie zauważył Robert A. Jones, że powrót do doktryny Breżniewa (ograniczonej suwerenności) nie był niemożliwy. Por.: R.A. Jones, *The Soviet Concept of „Limited Sovereignty” from Lenin to Gorbachev: The Brezhnev Doctrine [Radziecka koncepcja „ograniczonej suwerenności” od Lenina do Gorbaczowa: Doktryna Breżniewa]*, Londyn 1990, s. 260–261.

[8] Popularność zdobyła koncepcja eurazjatycka, sformułowana w latach 20. przez Piotra Sawickiego na emigracji. Nośność tej idei szybko docenili bolszewicy, używając jej do pozyskiwania emigrantów na rzecz ZSRS, przedstawianego jako imperium eurazjatyckie. Najsłynniejszym badaczem tej koncepcji był Lew Gumilow (miał okazję spotkać w łagrze Sawickiego). Obecnie najbardziej znanym propagatorem tej koncepcji w Rosji jest powołujący się na Gumilowa Aleksandr Dugin, sam eurazjatyzm stał się zaś nośnikiem rosyjskich ambicji imperialnych. Imperializm rosyjski ma jednak wiele postaci i posługuje się różnymi konstrukcjami ideologicznymi, dobieranymi taktycznie, w zależności od adresata i okoliczności wewnętrznych i międzynarodowych.

[9] Przywiązanie do tego, co dzisiaj rosyjska propaganda nazywa *Russkim mirem*, prezentował w swojej publicystyce emigracyjnej jeden z najbardziej znanych emigrantów – Aleksander Sołżenicyn. W 2000 r. odbył on rozmowę z nowo wybranym na prezydenta Władimirem Putinem, który wykorzystał jego autorytet i poglądy jako komponent nowej państwowej ideologii. Zakładała ona nie tylko odbudowę imperium, lecz także przejęcie od Zachodu, zgodnie z myślą Sołżenicyna, funkcji przewodniej dla innych narodów. Por.: P. Głuszkowski, *Antyrosja. Historyczne wizje świata Aleksandra Sołżenicyna. Próba polskiego odczytania*, Warszawa 2008, s. 37–39. W wyniku przeprowadzonego wszechzwiązkowego referendum 71,3 proc. głosujących opowiedziało się za utrzymaniem ZSRS. Informacje za: B. Gołąbek, *Lew Gumilow i Aleksander Dugin. O dwóch obliczach euroazjatyzmu w Rosji po 1991 roku*, Kraków 2012, s. 9.

Putina są syntezą spuścizny sowieckiej oraz przedrewolucyjnej Rosji, lecz podłoże do tego typu miksu ideologicznego od dziesięcioleci było szykowane przez przedstawicieli emigracji rosyjskiej, a także sowieckie służby, które umiejętnie wykorzystywały przywiązanie „białych" Rosjan do tradycji imperialnej[10]. Bezpośrednie działania mające na celu przygotowanie tej syntezy ideologicznej na gruncie wewnątrzrosyjskim były prowadzone w okresie, kiedy urząd sekretarza generalnego Komunistycznej Partii Związku Sowieckiego pełnił Michaił Gorbaczow[11].

Lata 90. były postrzegane przez Rosjan jako okres upokorzenia, biedy, korupcji, „ekspansji" NATO, słabej władzy oraz obaw przed zamachami terrorystycznymi. Te czynniki posłużyły elitom rządzącym do pogłębiania w społeczeństwie przeświadczenia o ciągłej konfrontacji Rosji z zagrażającym jej Zachodem. Przeżywając okres słabości, Rosja nie była w stanie zapobiec wejściu państw dawnego bloku wschodniego w struktury NATO i UE. Nie znaczy to, że pogodziła się z tym faktem, wręcz przeciwnie – zaczęła poszukiwać metod, dzięki którym skutecznie mogłaby odwrócić ten proces. Metody, jakie zamierzały zastosować władze rosyjskie, mają odzwierciedlenie w pozornie defensywnych dokumentach doktrynalnych (zwłaszcza

[10] U niektórych przedstawicieli rosyjskiej diaspory ten trend nasilił się wraz z oszałamiającymi sukcesami Armii Czerwonej, która nie tylko przywróciła Rosji granice sprzed I wojny światowej, lecz także znacząco poszerzyła terytorium rosyjskie i obszar wpływów. Zob.: Ł. Dryblak, *Szermierze wolności i zakładnicy imperium. Emigracyjny dialog polsko-rosyjski w latach 1939–1956. Konfrontacje idei, koncepcji oraz analiz politycznych*, Warszawa 2023, s. 175–176.

[11] Lew Gumilow stworzył wszystkie swoje koncepcje w ZSRS. Jednak dla szerszego audytorium niż akademickie stał się znany dopiero w 1989 r. (dzięki programom w leningradzkiej telewizji). Por.: B. Gołąbek, *op. cit.*, s. 10. W tym samym okresie budowanie zagranicznej sieci wpływów zaczynał Dugin, powołujący się na spuściznę Gumilowa, bardzo aktywny, w szczególności jeśli chodzi o dywersję ideologiczną wśród elit zachodnich. Więcej patrz: M. Wojnowski, *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 25–26. Ważnym emigrantem, którego działalność została wykorzystana do budowy nowej ideologii, był Nikita Struwe, syn słynnego naukowca i polityka Piotra Struwe. W 1990 r. zaangażował się on w akcję powrotów emigrantów do Rosji, od 1991 r. w ramach inicjatywy «Русский путь» założył sieć czytelni na terenie Wspólnoty Niepodległych Państw oraz państw bałtyckich, a także w 1995 r. Библиотеку-фонд «Русское Зарубежье», która stała się jednym z narzędzi konsolidacji diaspory rosyjskiej oraz promowania nowej ideologii. Zob.: http://www.rp-net.ru/book/OurAutors/struve/index.php (dostęp: 17 maja 2017 r.).

doktrynach informacyjnych, najlepiej odzwierciedlających specyfikę rosyjskiego myślenia). Ich rola i znaczenie zostaną omówione w poniższym artykule.

Narracja w oficjalnych doktrynach wojennych Federacji Rosyjskiej

Pierwszym dokumentem doktrynalnym, jaki spisano w Federacji Rosyjskiej, były „Główne Założenia Doktryny Wojennej FR z 2 listopada 1993 r."[12]. Do najważniejszych komunikatów, skierowanych ku Zachodowi, należało zastrzeżenie sobie przez FR prawa do interwencji w krajach, w których rosyjska mniejszość byłaby represjonowana, oraz brak zgody na stacjonowanie wojsk NATO w państwach uznawanych przez Rosję za jej strefę bezpieczeństwa. W dokumencie podkreślano gotowość do współpracy w budowaniu bezpieczeństwa międzynarodowego oraz do dalszej redukcji zasobów nuklearnych (zastrzegając sobie prawo do odpowiedzi nuklearnej na atak konwencjonalny). Ta doktryna oficjalnie miała charakter obronny, lecz w rzeczywistości pokazywała, że Rosja będzie się starała stosować wobec państw dawnego bloku wschodniego zasadę ograniczonej suwerenności. Do najpoważniejszych zagrożeń zaliczono groźbę represjonowania mniejszości rosyjskiej oraz ruchy separatystyczne, wskazując pośrednio elementy, na których w późniejszych latach oparła swoją agresywną politykę wobec krajów byłego ZSRS[13]. Warto zaznaczyć, że wraz z doktryną wydano numer „Rosyjskiego Wojennego Sbornika" na temat dyskusji wokół rosyjskiej doktryny wojennej w latach 1911–1939[14]. W trzech rozdziałach dotyczących Rosji,

[12] *Основные* положения военной доктрины российской федерации *[Główne postanowienia doktryny wojskowej Federacji Rosyjskiej]*, 2 listopada 1993 r., http://studydoc.ru/doc/360885/osnovnye-polozheniya-voennoj-doktriny-rossijskoj-federacii (dostęp: 13 kwietnia 2017 r.).

[13] Używanie mniejszości rosyjskiej i przedstawicieli narodów utożsamiających się z *Russkim mirem*, ruchów separatystycznych oraz opozycyjnych (zgodnie ze starymi metodami carskiej ochrany) jest stałym narzędziem rosyjskiej polityki zagranicznej (napięta sytuacja w państwach bałtyckich, zacieśnianie związków z Białorusią i Naddniestrzem, działania militarne w Gruzji i Ukrainie, wspieranie przychylnych Rosji polityków).

[14] A.E. Sawinkin, *Русская* Военная Доктрина. Материалы дискуссий 1911–1939 годов *[Rosyjska doktryna wojskowa. Materiały z lat 1911-1939]*, Moskwa 1994. Praca

carskiej, sowieckiej i zagranicznej („białej" emigracji), pokazano syntetyczność rosyjskiej tożsamości i ciągłość myśli wojskowej.

W „Doktrynie wojennej FR" zatwierdzonej 21 kwietnia 2000 r. po raz kolejny podkreślono jej przejściowy (związany z „budową demokracji") i obronny charakter. We wstępie zaznaczono, że doktryna ma na celu centralizację państwowego i wojennego zarządzania w sferze politycznej, dyplomatycznej, ekonomicznej, społecznej, informacyjnej, prawnej, wojskowej i innych. Oceniono, że istnieje niskie prawdopodobieństwo wybuchu globalnego konfliktu, w tym jądrowego[15]. Spodziewano się wzmożenia różnych ekstremizmów i separatyzmów, lokalnych wojen, wyścigu zbrojeń, rozprzestrzeniania broni jądrowej i innych broni masowego rażenia, a także „zaostrzenia konfrontacji informacyjnej". Elementami destabilizującymi sytuację międzynarodową miały być marginalizacja roli ONZ i OBWE, niezgodne z umowami międzynarodowymi zbrojenia, używanie informacyjnych technologii w celu ekspansji, działalność grup ekstremistycznych (nacjonalistycznych, religijnych, separatystycznych, terrorystycznych). W zagrożeniach zewnętrznych skupiono się na wymienieniu działań mogących mieć miejsce bez wystąpienia oficjalnego stanu wojny lub w ramach wojny lokalnej (m.in. działania informacyjno-techniczne lub informacyjno-psychologiczne), w tym „próby ignorowania (umniejszania) interesu Federacji Rosyjskiej w decydowaniu o kwestiach bezpieczeństwa międzynarodowego, przeciwdziałanie jej wzmocnieniu jako jednego z wpływowych centrów wielopolarnego świata"[16]. W ostatnim akapicie doktryny podkreślono, że celami FR są zapobieganie konfliktom i wspieranie międzynarodowego bezpieczeństwa i pokoju.

---

zarejestrowana 29 października 1993 r. w moskiewskiej rejonowej inspekcji wolności prasy i masowej informacji. Tom wydano w serii wydawnictwa *Russkij Put'*, którego założycielem był m.in. Nikita Struwe.

[15] *Военная доктрина Российской Федерации [Doktryna wojskowa Federacji Rosyjskiej],* 21 kwietnia 2000 r., http://www.ng.ru/politics/2000-04-22/5_doktrina.html (dostęp: 13 kwietnia 2017 r.).

[16] *ibidem*.

W „Doktrynie wojennej FR" z 2010 r. powtórzono tezę o narastaniu regionalnych konfliktów[17]. Pojawiło się także stwierdzenie, że obecna architektura bezpieczeństwa nie zapewnia go w sposób jednakowy wszystkim państwom; zauważono, że zagrożenie wojenne dla Rosji wzrasta m.in. ze względu na łamanie prawa międzynarodowego przez NATO i próby rozszerzenia sojuszu o państwa graniczące z FR, próby destabilizacji w państwach i regionach oraz podważanie strategicznej stabilności, lokowanie obcych wojsk w państwach sąsiadujących z Rosją, rozmieszczanie systemów obrony przeciwrakietowej, pretensje terytorialne wobec Rosji i jej sojuszników, nieprzestrzeganie umów międzynarodowych, eskalację konfliktów w rejonach graniczących z Rosją, rozprzestrzenienie terroryzmu międzynarodowego oraz separatyzmy. Specyfiką konfliktów miała być nieprzewidywalność ich wybuchu, szeroka gama użytych środków walki, w tym konfrontacji informacyjnej dla osiągnięcia celów politycznych bez wojny. W kontekście informacji w doktrynie znalazł się zapis o konieczności rozwoju sił i środków konfrontacji informacyjnej w oparciu o nowoczesne technologie.

W „Doktrynie wojennej FR" z 2014 r.[18], w punkcie dotyczącym zagrożeń po raz kolejny wymienia się globalną konkurencję oraz regionalne konflikty. Duży konflikt militarny z udziałem Rosji został określony jako mało prawdopodobny – co w kontekście inwazji rosyjskiej na Ukrainę w 2022 r. dobitnie pokazuje, że Moskwa maskowała swoje rzeczywiste zamiary. Jednocześnie podkreślono wzrost zagrożeń w sferze informacyjnej. Jako główne zagrożenie znów wskazano NATO, następnie kolejno: destabilizację wewnętrzną w poszczególnych krajach, zwiększanie obcych kontyngentów wojskowych na terenie państw graniczących z Rosją, rozwijanie strategicznych systemów obrony przeciwrakietowej oraz na końcu wykorzystywanie technologii informacyjnych w celach wojskowo-politycznych oraz narzucanie w państwach graniczących z Rosją wrogich jej reżimów.

[17] Военная доктрина Российской Федерации *[Doktryna wojskowa Federacji Rosyjskiej]*, 5 lutego 2010 r., http://kremlin.ru/supplement/461 (dostęp: 24 marca 2017 r.).

[18] Военная доктрина Российской Федерации *[Doktryna wojskowa Federacji Rosyjskiej]*, 26 grudnia 2014 r., s. 4-7, http://kremlin.ru/events/president/news/47334 (dostęp: 13 kwietnia 2017 r.).

Wśród głównych wewnętrznych niebezpieczeństw wojennych wymieniono na pierwszym miejscu działania prowadzące do obalenia ustroju konstytucyjnego, destabilizację sytuacji wewnątrzpolitycznej, społecznej oraz dezorganizację funkcjonowania organów władzy państwowej i infrastruktury, w tym infrastruktury informacyjnej. Następnie wskazano na: działalność organizacji terrorystycznych; oddziaływanie informacyjne na społeczeństwo (przede wszystkim na młodzież), mające na celu przerwanie historycznych, duchowych i patriotycznych tradycji w zakresie obrony ojczyzny; prowokowanie napięć o charakterze narodowościowym, etnicznym, społecznym i religijnym. Do zagrożeń wojennych zaliczono: gwałtowne zaostrzenie sytuacji militarno-politycznej oraz stworzenie warunków do stosowania siły militarnej; zakłócanie pracy systemów państwowego i wojskowego zarządzania FR; tworzenie i szkolenie nielegalnych formacji zbrojnych w celu wykorzystania ich przeciwko Rosji lub jej sojusznikom; demonstracje militarne w czasie manewrów na terytorium państw graniczących z FR i jej sojusznikami; aktywizację działalności sił zbrojnych poszczególnych państw (częściowa lub powszechna mobilizacja, funkcjonowanie państwa na stopie wojennej).

Powyższy skrótowy przegląd zagrożeń zawartych w rosyjskich doktrynach wojennych stanowi dowód na odmienność funkcji, jaką pełnią doktryny w Rosji. Stanowią one narzędzie oddziaływania informacyjnego używane zgodnie z dalekosiężną strategią, której nie formułuje się *explicite*. Mimo to po zastosowaniu odpowiedniego aparatu krytycznego dzięki ich lekturze można dostrzec, jak bardzo konsekwentne i długofalowe są działania rosyjskie oraz jakie elementy cechują rosyjskie myślenie.

Podstawowe założenia doktryny z 1993 r. zostały niezmienne i były jedynie aktualizowane, rozwijane lub inaczej ujmowane w kolejnych dokumentach w zależności od potrzeb polityki zagranicznej. Na ich podstawie można zobaczyć, jak Rosja używa doktryn do wywierania wpływu informacyjnego zarówno na użytek wewnętrzny, jak zewnętrzny[19]. W każdej kolejnej doktrynie coraz bardziej stanowczo

[19] Jolanta Darczewska wyróżnia cztery funkcje rosyjskich dokumentów strategicznych: światopoglądową, metodologiczną, edukacyjną/dydaktyczną i mobilizacyjną (funkcja

podkreślano rosyjskie prawa do posiadania stref wpływów, starając się przekonać obce państwa, że jest to działanie defensywne i w pełni uzasadnione. W oddziaływaniu wewnętrznym dążono natomiast do maksymalnej konsolidacji społeczeństwa i wytworzenia obrazu dwóch światów: Rosji z sojusznikami (w tym celu promowane są różnego typu koncepcje ideologiczne, np. *Russkij mir,* Unia Eurazjatycka czy czwarta teoria polityczna)[20] oraz obozu euroatlantyckiego, który jest przedstawiany jako agresor zagrażający porządkowi światowemu[21]. Obronno-odstraszająca retoryka oraz budowanie obrazu NATO jako organizacji przyczyniającej się do destabilizacji sytuacji na świecie to zabiegi mające na celu odebranie moralnej supremacji obozowi euroatlantyckiemu. Ma to również budować wrażenie, że działania rosyjskie są podejmowane reaktywnie w stosunku do działań – w myśl forsowanego przekazu – „agresywnego" sojuszu północnoatlantyckiego. Poprzez doktryny, których przekaz jest synergicznie połączony z przekazem decydentów, polityków, mediów oraz innych podmiotów służących kreowaniu polityki informacyjnej, Rosja wprowadza dysonans poznawczy u swoich przeciwników i stara się zyskać przewagę informacyjną (narzucanie własnej

prognostyczna stanowi margines). Zdaniem badaczki te dokumenty są elementem strategii informacyjnej i pełnią inne funkcje od dokumentów zachodnich. Por.: J. Darczewska, *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, „Prace OSW" 2016, nr 57, s. 22. Specyfika obecnych rosyjskich doktryn nie odbiega od standardów stosowanych w ZSRS, według Laurenca Martina sowieckie doktryny służyły „manipulowaniu wrogiem, a nie tylko podporządkowaniu go sobie" *[To manipulate the enemy rather than merely to subdue him* – tłum. własne*]*. Zob.:, L. Martin, *The Influence of Soviet Military Doctrine on Western Strategy [Wpływ radzieckiej doktryny wojskowej na zachodnią strategię]*, w: G. Flynn (red.), *Soviet Military Doctrine and Western Policy*, Londyn 1989, s. 406.

[20] Podobne zadanie pełnił program zbierania ziem ruskich, a następnie panslawizm i komunizm, które kolejno były porzucane ze względu na swoją anachroniczność lub nieefektywność. Dzisiaj pełnią one jedynie funkcje pomocnicze. Wybitny polski sowietolog Ryszard Wraga, zauważył, że XIX w. był dla Rosji okresem poszukiwania idei, która pozwoliłaby jej w sposób pełniejszy realizować budowę imperium – to stwierdzenie można odnieść również do XX w. Zob.: R. Wraga, *Geopolityka, strategia i granice*, Rzym 1945, s. 11.

[21] Schemat konfrontacji dwóch cywilizacji został rozwinięty w doktrynie *Russkiego mira*, sporządzonej przez członków założonego w 2012 r. Klubu Izborskiego: Доктрина Русского мира *[Doktryna rosyjskiego pokoju]*, 26 września 2016 r., https://izborsk-club.ru/10269 (dostep: 17 maja 2017 r.). Sam pomysł napisania takiej doktryny ujawnił już w 2005 r. Witalij Awierianow działający w ramach wspieranego przez Cerkiew *Sergijewskiego Projektu.* Por. stronę internetową: http://www.rusdoctrina.ru/page95504.html (dostep: 17 maja 2017 r.).

narracji społeczeństwom zachodnim). Zamęt dotyczący rozpoznania rosyjskich intencji, wprowadzany poprzez oficjalne dokumenty doktrynalne, może być zagrożeniem dla polityków, analityków czy naukowców, którzy w swych pracach nie uwzględnią dualistycznego charakteru oficjalnych dokumentów rosyjskich[22]. Chociaż Rosja nie jest w stanie zdominować przekazów zachodnich, to jednak punktowo i krótkookresowo może na nie wpływać. Długofalowe oddziaływanie pozwala także z czasem wytworzyć w danym kraju podatny grunt na swoje narracje w konkretnych kwestiach (dotyczy to również Polski).

Jak bardzo fałszywy jest „awers", prezentowany w rosyjskich dokumentach doktrynalnych, można wykazać poprzez lekturę specjalistycznych pozycji z zakresu rosyjskich czy sowieckich nauk wojskowych. W tym kontekście warto przytoczyć artykuł kpt. Dymitra Czuwatkina, pracownika Permskiego Wojennego Instytutu Wojsk Wewnętrznych MSW Rosji, pt.*:* „Wojenna doktryna jako sposób wpływu informacyjnego (ujęcie semiotyczne)"[23]. Artykuł został wygłoszony na specjalistycznej konferencji w Barnaulu. Wybór zarówno miejsca (audytorium), jak i samego referenta (zaledwie kapitan) pozwala stwierdzić, że referat był emanacją poglądów wspólnych, przynajmniej dla środowiska wywodzącego się ze służb mających decydujący wpływ na procesy zachodzące w Rosji. Na podstawie lektury artykułu widać, że myślenie autora jest osadzone o tezy Clausewitza – przyswojone przez bolszewików i nadal popularne w rosyjskiej nauce – „(…) po analizie podstawowych wojenno-politycznych

[22] Problem polega m.in. na różnym rozumieniu tych samych terminów. FR chętnie używa zachodnich terminów, by wprowadzać inne kraje w błąd, co jest standardową praktyką stosowaną od czasów ZSRS – „Trzeba wiedzieć, że sowieckiej (komunistycznej) propagandzie zależy niezwykle na wprowadzaniu chaosu do pojęć przyjętych przez ludzkość. Oficjalna doktryna komunistyczna posiłkuje się w tym celu dużą ilością nazw, które nie tylko w praktyce, lecz i w teorii komunistycznej oznaczają zupełnie co innego, aniżeli w słownictwie humanistycznym świata wolnego". Cytat za: R. Wraga, *O tak zw. „Komuniźmie narodowym"*, „Syrena" 1956, nr 48.

[23] D.N. Czubatkin, Военная доктрина как способ информационного воздействия (семиотический подход) *[Doktryna wojskowa jako sposób oddziaływania informacyjnego (podejście semiotyczne)]*, w: J.G. Czernyszow (red.), Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях) *[Współczesna Rosja i świat: alternatywy rozwoju (wojny informacyjne w stosunkach międzynarodowych)]*, Barnauł 2012, s. 136–140.

orientacji i kierunków okazuje się jasnym, że wojenne doktryny mają nie tylko obronny charakter, lecz są ukierunkowane na szerokie użycie wojskowej siły jako rozstrzygającego instrumentu polityki zagranicznej”[24]. Inaczej mówiąc, każda doktryna wojenna jest z góry ofensywna, gdyż użycie siły stanowi jedynie kolejny etap prowadzonej polityki zagranicznej. Nie ma tutaj wyraźnego rozgraniczenia na etap pokoju i wojny, gdyż liczą się jedynie cele, które chce się osiągnąć, dobór środków ma zaś znaczenie techniczne. Takie postrzeganie doktryny pozwala stwierdzić, że Rosjanie nie ograniczają się jedynie do teorii, lecz faktycznie ich doktryny mają charakter ofensywny. Czemu zatem służy oficjalna doktryna? Odpowiedź sformułowana przez Czuwatkina jest jednoznaczna: „Wojenna doktryna [jest] systemem idei, zestawionych w ramach semiotycznego paradygmatu. (…) Czyni to wojenną doktrynę współczesnego państwa bronią w wojnie informacyjnej (…). Idea informacyjnego wpływu polega na zaszczepieniu potencjalnemu przeciwnikowi zaprogramowanego (kontrolowanego) informacyjnego obrazu świata, sposobu myślenia. Stało się oczywistym, że wpływ informacyjny jest w stanie zmienić główny wojenno-polityczny zasób państwa – mentalność narodową, kulturę, moralność i wolę ludzi. Tym samym pytanie o rolę symbolicznego kapitału kultury w przestrzeni informacyjnej przestaje być abstrakcyjno-teoretycznym i przybiera strategiczne znaczenie polityczne”[25]. Takie myślenie wynika zarówno ze wschodnich tradycji funkcjonowania tego państwa, głęboko zakorzenionych w historii, jak i z bardzo rozwiniętych badań nad ludzką psychiką. Te obserwacje doprowadziły do wypracowania metodologii zarządzania refleksyjnego, stosowanego na wszystkich poziomach funkcjonowania człowieka i państwa w Rosji[26]. Mając na uwadze specyfikę podejścia

[24] *ibidem*, s. 137 [tłum. własne].
[25] *ibidem*, s. 138 [tłum. własne].
[26] Szerzej na temat teorii zarządzania refleksyjnego w rosyjskich naukach wojskowych patrz: M. Wojnowski, *„Zarządzanie refleksyjne” jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 12 s. 11–36; C. Reid, *Reflexive Control in Soviet Military Planning [Kontrola refleksyjna w radzieckim planowaniu wojskowym]*, w: B.D. Dailey, P.J. Parker (red.), *Soviet Strategic Deception [Radzieckie oszustwo strategiczne]*, Toronto 1987, s. 295–311.

rosyjskiego, można przejść do analizy doktryn bezpieczeństwa informacyjnego FR.

Doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej z 2000 i 2016 r.[27]

Podczas porównania obu doktryn można dostrzec, że ta z 2000 r. posiada bardziej rozbudowaną strukturę w porównaniu z o wiele krótszą, bardziej ogólną i oskarżycielską w swym tonie doktryną z 2016 r. W obu dokumentach interes narodowy został zdefiniowany jako: obrona suwerenności informacyjnej FR; zabezpieczenie konstytucyjnych praw i wolności człowieka i obywatela w obszarze pozyskiwania oraz używania informacji, korzystania z technologii informacyjnych, wsparcia informacyjnego dla instytutów demokratycznych, mechanizmów wzajemnego oddziaływania państwa i społeczeństwa obywatelskiego, przyswojenia technologii informacyjnych w celu ochrony kultury, historycznych i duchowych wartości wielonarodowego narodu FR (ten termin wiąże się z ideologią *Ruskiego miru*), zabezpieczenia infrastruktury informacyjnej, rozwinięcia w FR branży technologii informacyjnych i przemysłu elektronicznego; dostarczenie do wewnętrznego i zewnętrznego odbiorcy wiarygodnych informacji; wsparcie w budowaniu międzynarodowego systemu bezpieczeństwa informacyjnego[28].

[27] W obu dokumentach infosfera jest połączeniem informacji, narzędzi informatyzacji, systemów informacyjnych, stron internetowych, sieci połączeń, technologii informacyjnych, narzędzi, które służą do konstruowania i obróbki informacji, rozwoju i wykorzystania technologii, zapewnienia bezpieczeństwa informacyjnego oraz kompleksowości mechanizmów regulowania wzajemnych stosunków społecznych (podkreślono globalny i transgraniczny charakter zagrożeń w infosferze). Zob.: Доктрина информационной безопасности Российской Федерации *[Doktryna bezpieczeństwa informacji Federacji Rosyjskiej]*, 9 września 2000 r., http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/doki-po-ib (dostep: 9 stycznia 2017 r.); Доктрина информационной безопасности Российской Федерации *[Doktryna bezpieczeństwa informacji Federacji Rosyjskiej]*, 5 grudnia 2016 r., s. 1, 3, 5, http://www.scrf.gov.ru/documents/6/5.html (dostęp: 9 stycznia 2017 r.).

[28] Доктрина информационной..., 9 września 2000 r., *op. cit.*; Доктрина информационной..., 5 grudnia 2016 r., *op. cit.*

W doktrynie z 2000 r. zagrożenia dla bezpieczeństwa FR podzielono w podrozdziale „Typy zagrożeń bezpieczeństwa informacyjnego FR" na cztery grupy zagrożeń: „dla konstytucyjnych praw i wolności człowieka i obywatela w sferze życia duchowego i działań informacyjnych dla indywidualnej, grupowej i społecznej świadomości oraz duchowego odrodzenia Rosji", „dla bezpieczeństwa informacyjnego państwowej polityki FR", „dla rozwoju rodzimego przemysłu informacyjnego" oraz „dla bezpieczeństwa informacyjnych i telekomunikacyjnych środków i systemów". Takiego podziału nie dokonano w 2016 r., wówczas ujęto wszystkie zagrożenia w ramach trzeciego rozdziału: „Główne zagrożenia informacyjne i stan bezpieczeństwa informacyjnego". W obu doktrynach podkreślono jednak: zagrożenie dla życia duchowego i funkcjonowania w przestrzeni informacyjnej w sferze indywidualnej, grupowej i społecznej; związek rozwoju technologii informatycznych z możliwością manipulacji świadomością (chociaż w 2016 r. dodano, że coraz częściej służy to państwom w „wojenno-politycznych" celach, a także do podważenia suwerenności i integralności terytorialnej państw); niebezpieczeństwo uzależnienia rosyjskiego przemysłu informacyjnego od zachodnich technologii (w nowej doktrynie stwierdzono, że ten stan uzależnia społeczno-ekonomiczny rozwój FR od geopolitycznych interesów innych krajów); niedostateczną kadrę naukową w dziedzinie technologii informacyjnych i użycie narzędzi elektronicznych do pozyskiwania informacji. Wśród najważniejszych zagrożeń, których nie powtórzono, znalazł się punkt o groźbie monopolizacji, zwłaszcza przez zagraniczne struktury informacyjne rosyjskiego rynku informacyjnego[29]. Zmniejszono oraz bardziej uogólniono również listę zagrożeń dotyczących kwestii technicznych (ochrony danych, sieci połączeń itp.), zabrakło także punktów związanych z brakiem dostępu obywateli do informacji pochodzących ze struktur państwa. Zagrożenia w nowej doktrynie zostały sformułowane tak, by podkreślić

[29] Zachodni specjaliści bardzo przyczynili się nie tylko do udostępnienia Rosji rozmaitych technologii, lecz także podzielili się swoim doświadczeniem, czego przykładem jest zespół zachodnich konsultantów, którzy tworzyli nowoczesną telewizję rosyjską (oficjalnie z myślą o demokratyzacji Rosji). Takim konsultantem był Angus Roxburgh, autor książki „Strongman u szczytu władzy. Władimir Putin i walka o Rosję" z 2012 r.

nasilające się niebezpieczeństwo ze strony innych państw w sferze informacyjnej. Podkreślono „wykorzystywanie technologicznego pierwszeństwa dla dominowania w sferze informacyjnej", dodano także punkty dotyczące międzynarodowego aspektu bezpieczeństwa informacyjnego. Autorzy zwrócili uwagę na niesprawiedliwy podział zasobów dla funkcjonowania Internetu oraz duże trudności w wytworzeniu „strategicznej stabilności i równoprawnego strategicznego partnerstwa". Część zagrożeń została sformułowana tak, by można było odnieść wrażenie, że Rosja jest zapóźniona technologicznie w stosunku do Zachodu. Mimo że przykładowo w dziedzinie wykorzystania nowoczesnych technologii oraz sieci do kontroli i wpływu na społeczeństwo (również za granicą) Rosja może już dysponować zaawansowanymi narzędziami. Wymienione zagrożenia odzwierciedlają w rzeczywistości agresywne działania rosyjskie, ukierunkowane zarówno na zwiększenie kontroli nad własnym społeczeństwem, jak i aktywne oddziaływanie na sferę informacyjną w obcych krajach.

Oficjalnie doktryna z 2016 r. posiada zatem charakter obronny[30] i służy przerzucaniu winy za wzrost zagrożeń w sferze informacyjnej na Zachód, czego dowodem ma być jego technologiczne górowanie nad Rosją. Tłumaczy ona rosyjską ekspansję obroną jej bezpieczeństwa informacyjnego, podnosi również jego rangę i dowodzi, że użycie technologii informacyjnych może prowadzić do wojny (FR rości sobie prawo do strategicznego powstrzymywania i zapobiegania w przypadku wystąpienia takiego zagrożenia). Wśród innych działań w obszarze obrony wymieniono: „doskonalenie systemu bezpieczeństwa informacyjnego Sił Zbrojnych FR, innych wojsk, formacji wojskowych i organów, włączając w to siły i środki obrony informacyjnej; prognozowanie, wykrywanie i ocenę niebezpieczeństw

[30] „Strategicznym celem zapewnienia bezpieczeństwa informacyjnego w obszarze obrony kraju jest: obrona żywotnych interesów jednostki, społeczeństwa i państwa przed wewnętrznymi i zewnętrznymi zagrożeniami, związanymi z użyciem technologii informacyjnych w celach wojenno-politycznych, sprzecznych z prawem międzynarodowym, w tym, w celu realizacji wrogich działań i aktów agresji, ukierunkowanych na podważenie suwerenności, naruszenie całości terytorialnej państw oraz zagrażającym międzynarodowemu pokojowi, jego bezpieczeństwu i strategicznej stabilności". Cytat za: Доктрина информационной…, 5 grudnia 2016 r., *op. cit*., s. 8–9 [tłum. własne].

informacyjnych, włącznie z zagrożeniami dla SZ FR w sferze informacyjnej; pomoc w obronie interesów sojuszników FR w sferze informacyjnej; neutralizacja wpływu operacji informacyjno-psychologicznych ukierunkowanych na naruszenie historycznych podstaw i tradycji patriotycznych związanych z obroną Ojczyzny”[31]. Ten tok myślenia został rozwinięty w kolejnych podpunktach, m.in. w tym dotyczącym zapewnienia bezpieczeństwa informacyjnego w obszarze państwowego i społecznego bezpieczeństwa: „Przeciwdziałanie używaniu technologii informacyjnych do szerzenia propagandy, ekstremistycznych ideologii, ksenofobii, dyskryminacji narodowej w celu podważenia suwerenności, politycznej i społecznej stabilności, siłowej zmiany ustroju konstytucyjnego, naruszeniu suwerenności terytorialnej FR; przeciwdziałanie używaniu (…) technologii informacyjnych przez służby specjalne, organizacje innych państw oraz pojedyncze osoby; wzmocnienie ochrony informacyjnej infrastruktury krytycznej oraz ciągłości jej działania, rozwinięcie mechanizmów walki, wyprzedzania niebezpieczeństw informacyjnych i likwidacji ich symptomów (…); zwiększenie bezpieczeństwa funkcjonowania obiektów infrastruktury informacyjnej, w celu zapewnienia nieustannej łączności między organami państwa, niedopuszczenia do sprawowania z zagranicy kontroli nad tymi łączami, zabezpieczenia stałego funkcjonowania i bezpieczeństwa scalonej sieci teleinformatycznej RF oraz bezpieczeństwa informacji, przekazywanej nią i obrabianej (…); zabezpieczenie ochrony informacji, zawierającej dane, składające się tajemnicę państwową (…); zwiększenie efektywności informacyjnego zabezpieczenia polityki zagranicznej FR; neutralizacja działań ukierunkowanych na rozmycie tradycyjnych duchowo-moralnych wartości”[32].

Różnice w doktrynach wynikają m.in. ze zmiany międzynarodowej sytuacji politycznej (częściowo wynika to też z dezaktualizacji

[31] *ibidem*, s. 8–9.

[32] *ibidem*, s. 9–10. Podpunkty dotyczące strategicznych celów i głównych kierunków zapewnienia bezpieczeństwa informacyjnego zostały zdefiniowane także dla obszarów: gospodarczego, nauki, technologii i wychowania oraz zachowania strategicznej stabilności i równoprawnego międzynarodowego partnerstwa.

niektórych zagrożeń)[33]. Nowa doktryna posługuje się o wiele bardziej agresywną retoryką (w domyśle antynatowską) i rozwija jedynie wybrane zagrożenia z poprzedniego dokumentu, by podkreślić wzrastające niebezpieczeństwo dla Rosji, usprawiedliwić swoje agresywne działania oraz zastraszyć potencjalnych przeciwników. Rosja metodycznie szykowała się do poważnej konfrontacji. Przez lata prowadziła działania informacyjne, zaostrzając z roku na rok antyukraińską oraz antypolską propagandę. Były to symptomy świadczące o prowadzonych przygotowaniach do wojny.

Komentarz do doktryn

Rosyjskie doktryny bezpieczeństwa informacyjnego nie mają swoich NATO-wskich odpowiedników[34]. W państwach NATO zagadnienie informacji pojawia się w ramach zagrożeń omawianych w doktrynach cyberbezpieczeństwa, w rosyjskich dokumentach Internet jest natomiast tylko elementem szerszego środowiska informacyjnego. Nie oznacza to, że nowe technologie związane z rozwojem Internetu zostały w Rosji zlekceważone, wręcz przeciwnie – szybko zorientowano się, że użycie ich w paradygmacie zarządzania refleksyjnego może być bardzo groźne dla przeciwnika[35]. Myślenie w tych kategoriach jest domeną elity FR, wywodzącej się głównie ze służb byłego ZSRS.

[33] Cele, które nie znalazły się w nowej doktrynie (zostały już osiągnięte): zapewnienie monopolu informacyjnego państwa, likwidacja zagranicznych struktur informacyjnych, rozwój państwowych stowarzyszeń i agencji informacyjnych, wykorzystywanie certyfikowanych środków łączności, przeanalizowanie obcych metod wojny informacyjnej oraz zapowiedzi opracowania odpowiednich przepisów prawa. Ostatnia niezależna stacja telewizyjna (NTW) została zlikwidowana niemalże równolegle z wejściem doktryny, wyrokiem sądu w 2001 r. Zob.: D. Carman, *op. cit.*, s. 364.

[34] Jedynym państwem europejskim, które posiada taką doktrynę, jest Ukraina: Доктрина інформаційної безпеки України *[Doktryna bezpieczeństwa informacji Ukrainy]*, 29 grudnia 2016 r., http://www.president.gov.ua/documents/472017-21374 (dostęp: 13 kwietnia 2017 r.).

[35] Myślenie rosyjskie dobrze odzwierciedla artykuł Aleksandra Sołowiewa, kierownika katedry analiz politycznych Moskiewskiego Uniwersytetu Państwowego: А. Сołowiew, Информационно-коммуникативные процессы в современном мире: социокультурные иллюстрации *[Procesy informacyjne i komunikacyjne we współczesnym świecie: ilustracje społeczno-kulturowe]*, w: Современная российская политология *[Współczesna rosyjska politologia]*, Moskwa 2003, s. 327, 335–336.

Lata 90. były okresem słabości państwa rosyjskiego oraz pozornego otwarcia na Zachód. Objęcie obowiązków prezydenta w 1999 r. przez młodego pułkownika KGB/FSB Władimira Putina zapoczątkowało zmianę rosyjskiej narracji, którą w skrócie można by określić jako neoimperialną. W wyniku wyborów w 2000 r. został on prezydentem i w ciągu zaledwie kilku miesięcy podpisał dwie nowe doktryny: wojenną i bezpieczeństwa informacyjnego[36]. Projekt tej drugiej był już przygotowany w 1994 r.[37], lecz musiał dojrzeć do odpowiedniego momentu, by zostać ogłoszonym oficjalnie[38]. Jak ważną rolę w strategii politycznej Rosji odgrywało bezpieczeństwo informacyjne, świadczy nie tylko opublikowana doktryna, lecz także pierwsze InfoForum, zainicjowane w 2001 r. przez Aparat Rady Bezpieczeństwa FR i Komitet Dumy Państwowej FR[39]. Niewypowiedziane w doktrynie cele, którymi były konsolidacja byłego ZSRS i odbudowa jego stref wpływów, wymagały uzyskania dominacji informacyjnej w obrębie Rosji i innych obszarów jej zainteresowania. Uważna lektura zagrożeń z doktryny z 2000 r. prowadzi do dwóch głównych wniosków:

1. Kreml już w 2000 r. był w trakcie zwiększenia kontroli politycznej społeczeństwa, narzucania nowej ideologii, ustanawiania

[36] Доктрина информационной..., 9 września 2000 r., *op. cit.*

[37] D. Carman, *Translation And Analysis Of The Doctrine Of Information Security Of The Russian Federation: Mass Media And The Politics Of Identity [Tłumaczenie i analiza doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej: Media masowe i polityka tożsamości]*, "Pacific Rim Law & Policy Journal" 2002, t. 11, nr 2, s. 343.

[38] Ogłoszenie tego dokumentu spotkało się z obawami w samej Rosji, przykładowo wśród środowisk dziennikarskich i historyków, którzy bali się ograniczenia wolności słowa i wprowadzenia kar za niezgodne z państwową interpretacje historii. Por.: *Кремль не увидел угроз историкам в доктрине информационной безопасности [Kreml nie widzi zagrożenia dla historyków w doktrynie bezpieczeństwa informacji]*, 6 grudnia 2016 r., http://www.rbc.ru/politics/06/12/2016/5846872e9a794718be9693c3 (dostęp: 17 maja 2017 r.); D. Carman, *Translation and analysis...*, *op. cit*., s. 345.

[39] InfoForum (Narodowe Forum Bezpieczeństwa Informacyjnego) oficjalnie służy wymianie myśli, lecz w praktyce jest atrapą zachodnich mechanizmów. Sprzyja budowaniu poczucia zaangażowania społeczeństwa w proces kreowania polityki informacyjnej, wspomaga jego wdrażanie („programowanie") oraz zachęca obywateli do angażowania się w działania informacyjne przeciwko wrogom Rosji. Odbywa się cyklicznie od 2001 r., w ostatnich latach uczestniczyło w nim jednorazowo około tysiąca osób – zarówno przedstawicieli administracji centralnej (m.in. minister obrony narodowej i spraw zagranicznych), terytorialnej, wojska, członków Dumy, jak i specjalistów (informatyków, dziennikarzy, naukowców, biznesmenów, członków NGO i GONGO).

monopolu informacyjnego państwa, rozwijania działalności państwowych stowarzyszeń i agencji informacyjnych, analizy przydatności nowych technologii w celach wojennych, wprowadzania nowych przepisów prawa.

2. Sposób, w jaki postrzegano zagrożenia w doktrynie, odzwierciedlał słabości systemów demokratycznych. W zestawieniu z bieżącymi działaniami Rosji stanowi to dobry wskaźnik działań, na jakie jest narażony Zachód, i pokazuje specyfikę rosyjskiego myślenia.

Nowa „Doktryna bezpieczeństwa informacyjnego" została zatwierdzona w dniu 5 grudnia 2016 r., pięć dni po opublikowaniu „Koncepcji polityki zagranicznej FR". Tym samym dokumenty zastąpiły obowiązującą od 9 września 2000 r. i znowelizowaną w 2013 r. „Doktrynę bezpieczeństwa informacyjnego FR" oraz wprowadzoną 12 lutego 2013 r. „Koncepcję polityki zagranicznej FR". Zakończenie prac nad nową doktryną zapowiedziano już na początku 2016 r., w czasie trwającego w dniach 4–5 lutego InfoForum[40]. 24 czerwca 2016 r. na stronie Rady Bezpieczeństwa FR pojawił się jej projekt ze skierowanym do obywateli apelem o zgłaszanie swoich uwag[41]. To przykład zachowywania ze względów propagandowych pozorów demokratycznych mechanizmów w czasie prac nad dokumentem. Rosyjska doktryna została opublikowana 12 dni po przyjęciu przez Parlament Europejski rezolucji nt. dezinformacji i propagandy uprawianej przez Daesh i Rosję. Możliwe, że Kreml czekał do przegłosowania rezolucji przez Parlament Europejski, żeby podkreślić obronny charakter własnej doktryny, w której znalazły się elementy tożsame z wypowiedzią Putina na jej temat[42] oraz innymi głosami

[40] *Результаты Инфофорума-2016 «Информационная безопасность России в условиях глобального информационного общества» [Wyniki Infoforum-2016 „Bezpieczeństwo informacyjne Rosji w globalnym społeczeństwie informacyjnym"],* SecurityLab, 12 lutego 2016 r., http://www.securitylab.ru/news/479412.php (dostęp: 30 września 2016 r.).

[41] Доктрина информационной безопасности Российской Федерации (проект*) [Doktryna bezpieczeństwa informacji Federacji Rosyjskiej (projekt)],* http://www.scrf.gov.ru/news/1098.html (dostęp: 30 grudnia 2016 r.).

[42] Putin stwierdził, że rezolucja łamie demokratyczne standardy i wyraził nadzieję, że w związku z tym Zachód nie zdecyduje się na podjęcie działań przeciwko rosyjskim dziennikarzom. Por.: *Путин назвал негативную резолюцию Европарламента по российским СМИ деградацией демократии [Putin nazwał negatywną rezolucję*

oskarżającymi Zachód o wprowadzanie cenzury, ograniczanie wolności słowa i dyskryminację rosyjskich dziennikarzy[43].

Cechą charakterystyczną dla obu doktryn jest prymat informacji nad techniką oraz ochrona informacji, a nie sposobu jej przekazywania, stąd w Rosji stosuje się głównie przymiotnik informacyjny, nie zaś informatyczny. Problemy ze zrozumieniem tego podejścia i wypracowaniem na nie odpowiedniego remedium posiada wiele państw demokratycznych, których działania ogniskują się głównie wokół zagadnień technicznych, związanych z ochroną infrastruktury informacyjnej. Spektakularnym przykładem była kampania wyborcza w USA w 2016 r. oraz tarcia polityczne, które są pokłosiem wprowadzenia do dyskursu publicznego pytania, czy Donald Trump oraz jego środowisko mają agenturalne powiązania z Rosją. Rosyjski atak na skrzynkę mailową Hilary Clinton z jednej strony doprowadził do ujawnienia informacji dość mało istotnych, lecz skandalicznych dla opinii publicznej, a z drugiej potwierdził popularną u przeciwników Trumpa tezę, że sprzyja mu Rosja. W tej operacji zdolności technologiczne odegrały jedynie rolę techniczną, jej celem było osiągniecie efektu psychologicznego. Zasiane wówczas ziarno wydało plon w postaci niebywałego zaostrzenia się konfliktu politycznego w USA (warto chociażby wspomnieć późniejszy szturm na Kapitol czy dwa zamachy na życie Trumpa). Ten przykład ilustruje, jak Rosja próbuje wytworzyć obraz swojej omnipotencji i chociaż oficjalnie zaprzecza wszelkim oskarżeniom, samo zasianie podejrzeń oraz ich eskalowanie mogą zaowocować sukcesem. Władze rosyjskie mają świadomość, że z powodu używania zagranicznych technologii nie będą mogły w pełni kontrolować swojej przestrzeni informacyjnej

Parlamentu Europejskiego w sprawie rosyjskich mediów degradacją demokracji], 23 stycznia 2016 r., http://tass.ru/politika/3807411 (dostęp: 9 stycznia 2017 r.). Rzeczniczka MSZ FR Maria Zacharowa poinformowała, że odpowiedź rosyjska będzie symetryczna.

[43] Patrz: wystąpienie W. Putina z października 2016 r. na dorocznym zjeździe Klubu Wałdajskiego oraz przed Zebraniem Federalnym z 1 grudnia 2016 r.; *Заседание Международного дискуссионного клуба «Валдай» [Spotkanie Międzynarodowego Klubu Dyskusyjnego Wałdaj]*, 27 października 2016 r., http://kremlin.ru/events/president/news/53151; *Послание Президента Федеральному Собранию [Przemówienie Prezydenta do Zgromadzenia Federalnego]*, 1 grudnia 2016 r., http://kremlin.ru/events/president/news/53379 (dostęp: 16 stycznia 2017 r.).

(i społeczeństwa), będą więc dążyły do wzrostu konkurencyjności rosyjskich produktów z branży IT oraz zapewnienia sobie samowystarczalności w dziedzinie wysokich technologii, elektroniki, urządzeń komputerowych i oprogramowania. Z drugiej strony rozumieją, że nie są w stanie pokonać Zachodu w wyścigu technologicznym, dlatego stosują środki asymetryczne i starają się zaskakiwać swoich przeciwników[44].

W dokumentach świadomie posłużono się zachodnią terminologią związaną z obroną praw człowieka i obywatela, aby wprowadzić zamęt pojęciowy i ukryć swe prawdziwe zamiary. Rosyjskie doktryny tylko oficjalnie mają charakter defensywny[45], a ich zadaniem jest dezinformowanie zewnętrznego i wewnętrznego odbiorcy (Kreml dąży do ekspansji mentalnej, gospodarczej i terytorialnej). Treść doktryny świadczyła o coraz bardziej konfrontacyjnym kierunku polityki FR, wynikającym nie z obawy przed nowymi zagrożeniami, lecz z dawno przyjętej strategii i sytuacji wewnętrznej w Rosji, której konsolidacja dokonuje się poprzez utrzymywanie społeczeństwa w przeświadczeniu o nieustannym zagrożeniu ze strony USA, UE, terrorystów czy obcych nacjonalistów. Dokument z 2016 r. był naturalną kontynuacją kursu oficjalnie zaprezentowanego w 2000 r. Obecnie można zaobserwować zaostrzenie się politycznej retoryki wewnątrz poszczególnych państw oraz na forum międzynarodowym, co niewątpliwie w jakimś stopniu jest zasługą rosyjskiej polityki narzucania światu swojej zmilitaryzowanej matrycy pojęciowej[46]. Dotyczy to nie tylko używania rosyjskiej terminologii do opisu

[44] Fakt, że środki aktywne są skutecznym narzędziem niwelowania militarnej i technologicznej przewagi NATO nad Federacją Rosyjską, potwierdza przykładowo artykuł wicedyrektora Moskiewskiego Centrum Carnegie Dmitrija Trenina: D. Trenin, *Выборы в США и российско-американские отношения* [*Wybory w USA i stosunki amerykańsko-rosyjskie]*, Russia in Global Affairs, 30 stycznia 2020 r., https://globalaffairs.ru/articles/vybory-v-ssha-i-rossijsko-amerikanskie-otnosheniya/ (dostęp: 3 czerwca 2024 r.).

[45] Trafnie rosyjską narrację zdefiniował Pomerantsev: „Zachód ściera małe narody na proch, a w Rosji one rozkwitają". Por.: P. Pomerantsev, *Jądro dziwności. Nowa Rosja*, Wołowiec 2015, s. 229.

[46] „Grono teoretyków stosujących taki aparat pojęciowy powiększa się, symulując obraz rozbudowanego kolektywnego wsparcia władz FR. Pojawiły się określenia: wojna informacyjna, atak informacyjny, broń historyczna, informacyjny specnaz, broń cywilizacyjna, broń informacyjna". Cytat za: J. Darczewska, *Wojna informacyjna Rosji*

działań Zachodu oraz zachodniej do opisu działań Rosji, lecz także bezkrytycznej recepcji rosyjskiej myśli politycznej i nauki, co sprzyja w rzeczywistości promowanej przez FR wizji świata, uzasadniającej rosyjskie agresywne działania i zbrojenia[47]. Rosyjski paradygmat należy badać, by sformułować adekwatną odpowiedź, lecz nie można mu ulec.

Rosja intensyfikowała działania w sferze informacyjnej i jednocześnie tłumaczyła je na forum międzynarodowym koniecznością obrony. Mimo że częściowo ujawniła swój plan działania w doktrynie z 2000 r., Zachód zaczął bardziej zwracać uwagę na działania rosyjskie dopiero od 2014 r., nadal jednak nie potrafiąc poprawnie odczytać strategii Moskwy.

Obronna retoryka usprawiedliwia centralizację polityki informacyjnej oraz sprawowanie pełnej kontroli nad infrastrukturą informacyjną w Rosji. Owa centralizacja polega na podporządkowaniu wszystkich aspektów polityki informacyjnej FR ścisłemu kierownictwu państwa – Radzie Bezpieczeństwa FR[48], w ramach której funkcjonuje komisja ds. polityki informacyjnej FR[49] (najważniejsze decyzje

z Zachodem. Nowe wyzwanie?, w: *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa. Wydanie specjalne*, Warszawa 2015, s. 71.

[47] Elementem tych działań jest wykorzystywanie zachodnich terminów do opisywania działań rosyjskich w celu przerzucenia winy na świat zachodni lub usprawiedliwienia działań rosyjskich. Do takich przykładów należy wykorzystanie przez Rosję terminu *hybrid warfare*. Termin został ukuty przez amerykańskich naukowców, a w narracji rosyjskiej został użyty do oskarżania Zachodu o prowadzenie działań, które *de facto* są tożsame głównie z rosyjskim/sowieckim paradygmatem wojny informacyjnej. Tym samym wojna wywołana przez Rosję w Ukrainie została określona mianem wojny hybrydowej, co dało asumpt do przerzucenia winy na Zachód.

[48] Przewodniczący: prezydent; stali członkowie: szef FSB, szef administracji prezydenta, przewodniczący Dumy, przedstawiciel prezydenta do spraw ekologii i transportu, minister spraw wewnętrznych, minister spraw zagranicznych, przewodnicząca Rady Federacji Federalnego Zebrania, premier, dyrektor Służby Wywiadu Zagranicznego, sekretarz Rady Bezpieczeństwa, minister obrony oraz 18 zwykłych członków.

[49] Skład międzyresortowej komisji Rady Bezpieczeństwa FR ds. bezpieczeństwa informacyjnego (aktualizowany w maju 2015 r.): z-ca Sekretarza Rady Bezpieczeństwa FR (przewodniczący komisji), specjalny przedstawiciel prezydenta FR w kwestiach międzynarodowej współpracy w obszarze bezpieczeństwa informacyjnego, I z-ca przewodniczącego Komitetu Dumy Państwowej ds. bezpieczeństwa i przeciwdziałaniu korupcji, I z-ca szefa Banku Rosji, I z-ca Ministra kultury FR, I z-ca ministra wychowania i szkolnictwa FR, sekretarz stanu – z-ca ministra rozwoju gospodarki FR, sekretarz stanu – z-ca ministra energetyki FR, z-ca ministra spraw wewnętrznych FR, z-ca ministra przemysłu i handlu FR, z-ca ministra połączeń i masowej komunikacji FR (z-ca przewodniczącego komisji),

dotyczące kierunków tejże polityki podejmowane są w najbliższym otoczeniu Putina). Centralizacji tej polityki sprzyja fakt, że wiele stanowisk kierowniczych w administracji, kluczowych placówkach naukowych[50], stowarzyszeniach i finansujących je koncernach pełnią osoby, które wywodzą się ze służb specjalnych oraz wojska. Wspólnota doświadczeń, znajomość tych samych modeli działania, jeden kod myślowy i osobiste kontakty determinują sposób prowadzenia rosyjskich działań, sprzyjają uzyskaniu efektu synergii oraz umożliwiają prowadzenie długoletnich operacji informacyjnych (potwierdzają to rodzaje zagrożeń wymienione w obu doktrynach informacyjnych,

z-ca ministra transportu FR, z-ca ministra sprawiedliwości FR, Główny inspektor państwowy FR ds. nadzoru pożarniczego, z-ca dyrektora Rosfinmonitoringu, z-ca dyrektora Służby Wywiadu Zagranicznego, z-ca dyrektora Federalnej Służby Ochrony, z-ca dyr. Federalnej Służby Technicznej i Eksportowej Kontroli, pierwszy z-ca dyrektora Federalnej Służby Celnej, sekretarz stanu – z-ca kierownika Federalnej Służby Nadzoru Ekologicznego, Technologicznego i Atomowego, z-ca kierownika Federalnej Służby Migracyjnej, z-ca kierownika Roskomnadzora (federalnej służby nadzoru w sferze połączeń, technologii informacyjnych i komunikacji masowej), z-ca kierownika Rospatenta (federalnej służby własności intelektualnej), z-ca kierownika Rospieczati (federalna agencja ds. prasy i komunikacji masowej), z-ca kierownika Rosswjazi (federalna agencja połączeń), z-ca kierownika Rosstata (federalnej służby państwowej statystyki), z-ca kierownika Federalnej Służby Podatkowej, szef FSB (z-ca przewodniczącego Komisji), szef administracji prezydenta FR ds. wdrażania technologii informacyjnych i rozwoju demokracji elektronicznej, szef Głównego zarządu operacyjnego Sztabu Generalnego SZ FR – z-ca szefa SG SZ FR, z-ca szefa Głównego Zarządu Specjalnych Programów prezydenta FR, z-ca szefa Zarządu służby prasowej i informacji prezydenta FR, referent aparatu Rady Bezpieczeństwa FR, referent Zarządu informacyjnego i dokumentacyjnego zabezpieczenia prezydenta FR, kierownik departamentu aparatu Rady Bezpieczeństwa FR (sekretarz Komisji), dyrektor departamentu Aparatu Rządu FR, wiceprezes – kierownik służby bezpieczeństwa Koncernu „Rosnieft", z-ca przewodniczącego zarządu Gazpromu. Informacje za: *Состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям [Skład Międzyresortowej Komisji Rady Bezpieczeństwa Federacji Rosyjskiej ds. Bezpieczeństwa Informacji według stanowisk],* http://www.scrf.gov.ru/about/commission/MVK_info_members/ (dostęp: 13 maja 2017 r.).

[50] W Rosji bardzo rozwinięte zostały studia nie tylko nad geopolityką, lecz także bezpieczeństwem informacyjnym.: Rosyjski Instytut Studiów Strategicznych (do stycznia 2017 r. dyrektorem był kandydat nauk historycznych, gen. por. SWR Leonid Rieszetnikow, a obecnie b. szef SWR Michaił Fradkow); Instytut Kryptografii i Informatyki Akademii FSB FR, Instytut Problemów Bezpieczeństwa Informacyjnego Uniwersytetu im. M.W. Łomonosowa (dyrektor gen. płk KGB Władisław Szerstiuk). Por. strony internetowe Instytutu Problemów Bezpieczeństwa Informacji [Институт Проблем Информационной Безопасности] oraz Rosyjskiego Instytutu Studiów Strategicznych [Российский институт стратегических исследований]: http://www.iisi.msu.ru; https://riss.ru (dostęp: 12 stycznia 2017 r.).

takie jak rozmywanie tradycyjnych rosyjskich wartości duchowo-moralnych, wymagających długookresowego wpływu). Polityce informacyjnej podporządkowane są: media państwowe i prywatne (wypracowano specyficzny model funkcjonowania mediów, łączący zachodnią technikę z rosyjskimi sposobami manipulowania świadomością społeczną)[51], media internetowe (wielojęzyczna sieć złożona z oficjalnych serwisów informacyjnych, autorytetów prowadzących aktywną działalność w sieci, stron internetowych, blogów, kanałów udostępniania memów, zdjęć i filmów, grup dyskusyjnych na portalach społecznościowych czy komentujących trolli), ustawodawstwo (godzące w wolność słowa)[52], edukacja (na wszystkich szczeblach)[53], agencje badania opinii publicznej, kultura[54], rozrywka (w tym gry komputerowe)[55], nauka[56], wydawnictwa[57], Cerkiew prawosławna[58],

[51] P. Pomerantsev, *op. cit.*, s. 288.

[52] Wprowadzenie odpowiednich przepisów poprzedziła seria obrazoburczych incydentów z udziałem Pussy Riot, przedstawianych jako forpoczta „zgniłego Zachodu" (możliwe, że była to prowokacja służb w celu zwiększenia przyzwolenia Rosjan na zaostrzenie niektórych przepisów).

[53] Szczególnemu oddziaływaniu poddawani są uczniowie w szkołach wojskowych, w tym m.in. w Korpusach Kadetów. Zob.: P. Jastrzębski, *Wschodni model wychowania państwowego na przykładzie rosyjskiego korpusu kadetów. Zarys problemu*, „Wschodni Rocznik Humanistyczny" 2012, nr 8, s. 145–152.

[54] Przykładowo atak na Ukrainę był poprzedzony kampanią propagandową w popkulturze (dobrym przykładem jest serial „Biała Gwardia", w którym pozytywnymi bohaterami byli zarówno biali, jak i czerwoni – w przeciwieństwie do Ukraińców, którzy negowali jedności ziem Imperium). Dużą rolę w mobilizowaniu społeczeństwa rosyjskiego odgrywa również przypominanie upokorzeń, których Rosja miała doznać za sprawą Polaków, podkreślanie polskiej rusofobii oraz roli Watykanu, a zwłaszcza jezuitów w walce z prawosławiem. Patrz: „Sofia Paleolog" (nowy serial dofinansowany przez Cerkiew i Ministerstwo Obrony FR).

[55] Rozpowszechnianie rosyjskiej propagandy poprzez komunikatory gier online oraz ich fabuła propagująca mit zwycięskiej wojny ojczyźnianej.

[56] Spektakularnymi przykładami podporządkowania nauki celom doktryny informacyjnej jest objęcie przewodnictwa nad Rosyjskim Towarzystwem Historycznym przez szefa SWR Siergieja Naryszkina nad Rosyjskim Towarzystwem Geograficznym przez ministra obrony narodowej gen. Siergieja Szojgu (przewodniczącym rady wspomagającej towarzystwo jest Władimir Putin) czy nad Akademią Problemów Geopolitycznych przez gen. płk Leonida Iwaszowa. Na wszystkich uczelniach wyższych wykłada się geopolitykę, w sieci zaś dostępna jest szeroka paleta podręczników.

[57] Przykładowo związane z FSB wydawnictwo „Wiecze", wydające głównie książki z dziedziny historii, politologii i literatury pięknej.

[58] Imperatorskie Prawosławne Towarzystwo Palestyńskie połączone z Centrum ds. Rozwoju Chrześcijaństwa na Wschodzie (prezes gen. Siergiej Stiepaszyn, b. szef FSB). Por.: http://www.ippo.ru (dostęp: 12 stycznia 2017 r.).

organizacje „pozarządowe" (również międzynarodowe, finansowane przez koncerny państwowe, np. Gazprom czy Rosnieft)[59], młodzieżowe organizacje paramilitarne[60], grupy paramilitarne[61], ośrodki kultury i nauki języka rosyjskiego poza granicami FR[62].

Wnioski

Działania Rosji od 1991 r. do dziś przeszły ewolucję od konsolidacji społeczeństwa oraz odstraszania i prób utrzymania dawnej strefy wpływów do działań ofensywnych, które rozpoczęto atakiem na Gruzję w 2008 r. Intensyfikacji działań postępujących od 2014 r. nie można postrzegać przez pryzmat rosyjskiej propagandy, która posunięcia Moskwy przedstawia jako reakcję na działania NATO i UE, świadomie określając je mianem ekspansji, by podkreślić ich rzekomy ofensywny charakter[63]. Agresywna postawa Rosji wynika z przyjętej doktryny. Odbudowa potencjału Rosji oraz sprzyjająca konfliktom sytuacja międzynarodowa pozwalają jej na coraz bardziej zdecydowane działania dywersyjne i dezintegracyjne wobec NATO i UE, których celem jest zmiana układu geopolitycznego.

[59] Przykładowo CIS-EMO, organizacja zajmująca się „monitoringiem" standardów demokratycznych. Por.: A. Shekhovtsov, *Far-right Election Observation Monitors in the Service of the Kremlins Foreign Policy [Skrajnie prawicowi obserwatorzy wyborów w służbie polityki zagranicznej Kremla]*, w: M. Laruelle (red.), *Eurasianism and the European Far Right: Reshaping the Europe–Russia Relationship*, Lexington Books, 2015, s. 224–226.

[60] We wrześniu 2016 r. powołano Junarmię, organizację skupiającą dzieci w wieku od 11 do 18 roku życia.

[61] Przykładowo: „Nocne Wilki", organizacje kozackie, nacjonalistyczne, grupy hakerskie (Fancy Bears, Cozy Bear, pod którym prawdopodobnie kryją się regularne jednostki rosyjskich służb specjalnych lub wojska).

[62] Organizacja „Russkij Mir" policzyła rosyjską diasporę, osoby posługujące się na świecie językiem rosyjskim oraz placówki nauczające języka rosyjskiego (stwierdzono, że województwa podlaskie, mazowieckie, lubelskie i podkarpackie ciążą ku wschodowi, tam też język rosyjski jest popularniejszy w nauczeniu szkolnym).

[63] Takie oskarżenia wychodziły spod pióra światowej sławy naukowców, dziennikarzy czy polityków. Najlepszym przykładem na to, jak głęboko udało się Moskwie zaszczepić swój pogląd na stosunki międzynarodowe w państwach Zachodu, był wrześniowo-październikowy numer „Foreign Affairs" z 2014 r. pt. "How The West Provoked Putin", a w nim artykuł: John J. Mearsheimer, *Why the Ukraine Crisis Is the West's Fault [Dlaczego kryzys na Ukrainie jest winą Zachodu]*, „Foreign Affairs" 2014, nr 5, s. 77–97.

„Doktryna bezpieczeństwa informacyjnego FR" z 2016 r. jest kontynuacją polityki zaprezentowanej w doktrynie z 2000 r., zaostrzeniu uległa jedynie retoryka. W 2023 r. zapisy tych doktryn zostały uzupełnione o nowy dokument poświęcony tylko i wyłącznie bezpieczeństwu informacyjnemu dzieci[64]. Zintensyfikowane od 2014 r. działania rosyjskie w sferze informacyjnej są wypadkową ciągłości myślenia, o której świadczą zaprezentowane doktryny. Poza oficjalną aktualizacją wyzwań i zagrożeń służą one przede wszystkim celom rosyjskiej strategii informacyjnej (są elementem strategicznej dezinformacji), w ramach której pełnią funkcje:

1. Propagandową – konsolidacja społeczeństwa, oskarżanie innych krajów o agresywne działania, wytyczanie oficjalnej linii narracyjnej oraz budowanie dobrego wizerunku prezydenta;
2. Dezinformacyjną – ukrywanie rzeczywistych zamiarów władz, wspieranie tezy o obronnym charakterze działań rosyjskich.

Lektura „Doktryny bezpieczeństwa informacyjnego" w kontekście innych dokumentów i działań podejmowanych przez władze FR świadczy o tym, że:

1. Treść doktryn ujawnia rosyjski sposób myślenia i pozwala zdefiniować, jakich działań można się spodziewać ze strony rosyjskiej: oddziaływanie na indywidualną i grupową świadomość, ze szczególnym uwzględnieniem młodzieży[65], w celu podsycania międzynarodowych, religijnych, etnicznych, kulturowych i socjalnych napięć.
2. Rosyjskie działania w infosferze charakteryzuje łączenie narzędzi z zakresu nauk humanistycznych i ścisłych. W myśleniu dominuje prymat psychologiczny, co powoduje, że szczególnie rozwijane są metody mające na celu wpływ na ludzką percepcję, poglądy, mentalność i emocje.

[64] *Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р [Rezolucja rządu rosyjskiego N 1105-r z dnia 28 kwietnia 2023 r.]*; https://normativ.kontur.ru/document?documentId=448153&moduleId=1 (dostęp: 21 września 2024 r.).

[65] W przypadku Polski dobry grunt pod rosyjskie operacje stwarza coraz słabsza pamięć o czasach II wojny światowej i PRL, niedostateczna liczba godzin nauczania historii w szkołach oraz nowe, często niewiarygodne źródła informacji dostępne w Internecie.

3. Opublikowanie doktryny i inne działania mające na celu podniesienie rosyjskich zdolności w sferze informacyjnej świadczą o dużej wadze, jaką Kreml przykłada do operacji psychologiczno-informacyjnych zarówno na gruncie wewnętrznym, jak i zewnętrznym[66].
4. Władze Rosji starały się narzucić światu swój paradygmat wojen informacyjnych oraz rosyjskocentryczną wizję geopolityczną, aby wytworzyć sprzyjającą atmosferę do stosowania rozwiązań siłowych (obecna międzynarodowa sytuacja bezpieczeństwa, również ze względu na konflikty na Bliskim Wschodzie, sprzyja siłowej wizji stosunków międzynarodowych, w której nie ma miejsca na prawo międzynarodowe).
5. W celu odstraszania i ukrywania swoich prawdziwych zdolności Rosja próbuje wytworzyć obraz omnipotencji (chociaż oficjalnie temu zaprzecza). Z tego powodu podkreśla m.in. znaczenie nowej doktryny czy powołanie nowego rodzaju wojsk „do operacji informacyjnych"[67] (zastrzega sobie też możliwość odpowiedzi kinetycznej na zagrożenia informacyjne).
6. Plan odbudowy imperium wymaga kontynuacji ideologicznego oddziaływania w obrębie takich koncepcji jak: *Russkij mir* (idea, w ramach której wykorzystywane są również akcenty panslawistyczne, głoszona głównie na potrzeby samych Rosjan oraz powiązanych z nimi narodów dawnego imperium, w tym zwłaszcza Słowian)[68], Unia Eurazjatycka (koncept polityczny

[66] Działania destabilizacyjne mogą ulegać intensyfikacji w czasie kampanii wyborczych, nasilenia konfliktów politycznych oraz sporów międzynarodowych. Polska specyfika powoduje, że kwestią newralgiczną nadal będą miejsca pamięci, związane zarówno z Armią Czerwoną, jak i UPA oraz incydenty, które mogą wyniknąć m.in. na linii Polska–Ukraina (niewykluczone, że w przyszłości na skutek zewnętrznych działań będą prowokowane konflikty z innymi państwami oraz narodowościami lub grupami etnicznymi zamieszkującymi Polskę).

[67] *Rosja: Szojgu o istnieniu oddziału żołnierzy wojny informacyjnej,* 22 lutego 2017 r., https://forsal.pl/artykuly/1021878,rosja-szojgu-o-istnieniu-oddzialu-zolnierzy-wojny-informacyjnej.html (dostęp: 26 maja 2017 r.).

[68] Patrz m.in. portal *Западная Русь* [Ruś Zachodnia], na którym można znaleźć również zakładkę poświęconą tematyce polskiej. Na stronie publikują m.in. analitycy związanego z SWR Rosyjskiego Instytutu Badań Strategicznych. Stałym publicystą strony jest m.in. Oleg Niemienskij. Por. stronę: https://zapadrus.su/bibli/geobib/2011-08-03-16-33-54.html (dostęp: 17 maja 2017 r.).

obecny na giełdzie idei od ponad pół wieku, obliczony na pozyskiwanie elit południowo – i zachodnioeuropejskich dla współpracy gospodarczo-politycznej z Rosją kosztem USA)[69] oraz czwarta teoria polityczna (adresowana do wszystkich mieszkańców Zachodu rozczarowanych rządami partii liberalno-demokratycznych, określanymi w tej koncepcji mianem totalitarnych). Te koncepcje posiadają zarówno elementy wspólne, jak i wykluczające. Dzięki temu udaje się znaleźć większe grono odbiorców idei, prowadzących *de facto* do jednego celu – zmiany układu geopolitycznego na taki, w którym Rosja uzyska lepszą pozycję wobec podzielonego i skłóconego świata zachodniego.

Rosyjskie służby w sposób naturalny szybko dostrzegły korzyści, które mogą płynąć z zastosowania nowych technologii w ramach starych metod operacji wpływu. Takie spostrzeżenia poczyniono już w latach 90., w 2000. rozwijano w tym kierunku zdolności, a co najmniej od kilkunastu lat za pomocą Internetu prowadzi się intensywne działania. Na podstawie doktryn bezpieczeństwa informacyjnego można zauważyć, że Rosjanie dokładnie zlokalizowali luki w systemach demokratycznych i będą je konsekwentnie wykorzystywać, co stanowi zagrożenie także dla stabilności państwa polskiego. Ostatnio opublikowana doktryna poświęcona ochronie informacyjnej dzieci może podpowiadać, że rosyjskie operacje dezinformacyjno-psychologiczne w sposób szczególny będą wymierzone właśnie w dzieci i młodzież. Kwestia oddziaływania rosyjskiego w tych grupach powinna być zatem przedmiotem głębokiej analizy.

[69] Na początku wojny rosyjsko-ukraińskiej nawiązał do niej Dmitrij Miedwiediew: „Президент России Владимир Путин твёрдо поставил цель демилитаризации и денацификации Украины. Эти сложные задачи не исполняются одномоментно. И они будут решаться не только на полях сражений. Изменить кровавое и полное лживых мифов сознание части нынешних украинцев – важнейшая цель. Цель во имя спокойствия будущих поколений самих украинцев и возможности наконец построить открытую Евразию – от Лиссабона до Владивостока", Telegram, 5 kwietnia 2022 r., https://t.me/medvedev_telegram/34 (dostęp: 21 września 2024 r.).

Bibliografia
References list

Piśmiennictwo
Literature

Bączkowski W., *Rosja wczoraj i dziś*, Jerozolima 1946.

Bączkowski W., *Uwagi o istocie siły rosyjskiej*, „Wschód-Orient" 1938, nr 4, http://www.omp.org.pl/artykul.php?artykul=115 (dostęp: 13 kwietnia 2017 r.).

Besançon A., *Imperium rosyjskie i panowanie sowieckie*, w: Karpiński J., Lasota I. (red.), *Sowietskij Sojuz. Wybór*, Wrocław 1989.

Carman D., *Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity [Tłumaczenie i analiza doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej: Media masowe i polityka tożsamości]*, „Pacific Rim Law & Policy Journal" 2002, t. 11, nr 2.

Clausevitz C., *O wojnie*, Wydawnictwo Mireki, Warszawa 2010.

Czubatkin D.N., *Военная доктрина как способ информационного воздействия (семиотический подход)* [*Doktryna wojskowa jako sposób oddziaływania informacyjnego (podejście semiotyczne)]*, w: Czernyszow J.G. (red.), *Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях) [Współczesna Rosja i świat: alternatywy rozwoju (wojny informacyjne w stosunkach międzynarodowych)]*.

Darczewska J., *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, „Prace OSW" 2016, nr 57.

Darczewska J., *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?*, w: *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa. Wydanie specjalne*, Warszawa 2015.

Garthoff R.L., *Soviet military doctrine [Radziecka doktryna wojskowa]*, RAND Corporation, Illinois 1953.

Głuszkowski P., *Antyrosja. Historyczne wizje świata Aleksandra Sołżenicyna. Próba polskiego odczytania*, Warszawa 2008.

Gołąbek B., *Lew Gumilow i Aleksander Dugin. O dwóch obliczach euroazjatyzmu w Rosji po 1991 roku*, Kraków 2012.

Jastrzębski P., *Wschodni model wychowania państwowego na przykładzie rosyjskiego korpusu kadetów. Zarys problemu*, „Wschodni Rocznik Humanistyczny" 2012, nr 8.

Jones R.A., *The Soviet Concept of „Limited Sovereignty" from Lenin to Gorbachev: The Brezhnev Doctrine [Radziecka koncepcja „ograniczonej suwerenności" od Lenina do Gorbaczowa: Doktryna Breżniewa]*, Londyn 1990.

Martin L., *The Influence of Soviet Military Doctrine on Western Strategy [Wpływ radzieckiej doktryny wojskowej na zachodnią strategię]*, w: Flynn G. (red.), *Soviet Military Doctrine and Western Policy*, Londyn 1989.

Nowak A., *Powrót „Imperium Zła". Ideologie współczesnej Rosji, ich twórcy i krytycy (1913–2023)*, Kraków 2023.

Pomerantsev P., *Jądro dziwności. Nowa Rosja*, Wołowiec 2015.

Послание Президента Федеральному Собранию [Przemówienie Prezydenta do Zgromadzenia Federalnego], 1 grudnia 2016 r., http://kremlin.ru/events/president/news/53379 (dostęp: 16 stycznia 2017 r.).

Путин назвал негативную резолюцию Европарламента по российским СМИ деградацией демократии [Putin nazwał negatywną rezolucję Parlamentu Europejskiego w sprawie rosyjskich mediów degradacją demokracji], 23 stycznia 2016 r., http://tass.ru/politika/3807411 (dostęp: 9 stycznia 2017 r.).

Reid C., *Reflexive Control in Soviet Military Planning [Kontrola refleksyjna w radzieckim planowaniu wojskowym]*, w: B.D. Dailey, P.J. Parker (red.), *Soviet Strategic Deception [Radzieckie oszustwo strategiczne]*, Toronto 1987.

Результаты Инфофорума-2016 «Информационная безопасность России в условиях глобального информационного общества» [Wyniki Infoforum-2016 „Bezpieczeństwo informacyjne Rosji w globalnym społeczeństwie informacyjnym"], SecurityLab, 12 lutego 2016 r., http://www.securitylab.ru/news/479412.php (dostęp: 30 września 2016 r.).

Rosja: Szojgu o istnieniu oddziału żołnierzy wojny informacyjnej, 22 lutego 2017 r., https://forsal.pl/artykuly/1021878,rosja-szojgu-o-istnieniu-oddzialu-zolnierzy-wojny-informacyjnej.html (dostęp: 26 maja 2017 r.).

Roxburgh A., *Strongman u szczytu władzy. Władimir Putin i walka o Rosję*, Warszawa 2012.

Shekhovtsov A., *Far-right Election Observation Monitors in the Service of the Kremlin's Foreign Policy [Skrajnie prawicowi obserwatorzy wyborów w służbie polityki zagranicznej Kremla]*, w: Laruelle M. (red.), *Eurasianism and the European Far Right: Reshaping the Europe–Russia Relationship*, Lexington Books, 2015.

Sołowiew A., *Информационно-коммуникативные процессы в современном мире: соци-окультурные иллюстрации [Procesy informacyjne i komunikacyjne we współczesnym świecie: ilustracje społeczno-kulturowe]*, w: *Современная российская политология [Współczesna rosyjska politologia]*, Moskwa 2003.

Состав Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям [Skład Międzyresortowej Komisji Rady Bezpieczeństwa Federacji Rosyjskiej ds. Bezpieczeństwa Informacji według stanowisk], http://www.scrf.gov.ru/about/commission/MVK_info_members/ (dostęp: 13 maja 2017 r.).

Trenin D., *Выборы в США и российско-американские отношения [Wybory w USA i stosunki amerykańsko-rosyjskie]*, Russia in Global Affairs, 30 stycznia 2020 r., https://globalaffairs.ru/articles/vybory-v-ssha-i-rossijsko-amerikanskie-otnosheniya/ (dostęp: 3 czerwca 2024 r.).

Wojnowski M., *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

Wraga R., *Gwarancje Pana Otmara*, „Bunt Młodych" 1935, nr 10.

Wraga R., *Geopolityka, strategia i granice*, Tel Awiw 1943.

Wraga R., *O tak zw. „Komuniźmie narodowym"*, „Syrena" 1956.

Заседание Международного дискуссионного клуба «Валдай» [Spotkanie Międzynarodowego Klubu Dyskusyjnego Władadaj], 27 października 2016 r., http://kremlin.ru/events/president/news/53151 (dostęp: 16 stycznia 2017 r.).

Źródła
Sources

Военная доктрина Российской Федерации [Doktryna wojskowa Federacji Rosyjskiej], 21 kwietnia 2000 r., http://www.ng.ru/politics/2000-04-22/5_doktrina.html (dostęp: 13 kwietnia 2017 r.).

Военная доктрина Российской Федерации [Doktryna wojskowa Federacji Rosyjskiej], 5 lutego 2010 r., http://kremlin.ru/supplement/461 (dostęp: 24 marca 2017 r.).

Военная доктрина Российской Федерации [Doktryna wojskowa Federacji Rosyjskiej], 26 grudnia 2014 r., http://kremlin.ru/events/president/news/47334 (dostęp: 13 kwietnia 2017 r.).

Доктрина информационной безопасности Российской Федерации [Doktryna bezpieczeństwa informacji Federacji Rosyjskiej], 9 września 2000 r., http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/dokipo-ib (dostęp: 9 stycznia 2017 r.).

Доктрина информационной безопасности Российской Федерации, [Doktryna bezpieczeństwa informacji Federacji Rosyjskiej], 5 grudnia 2016 r., http://www.scrf.gov.ru/documents/6/5.html (dostęp: 9 stycznia 2017 r.).

Доктрина Русского мира [Doktryna rosyjskiego pokoju], 26 września 2016 r., https://izborsk-club.ru/10269 (dostęp: 17 maja 2017 r.).

Доктрина інформаційної безпеки України [Doktryna bezpieczeństwa informacji Ukrainy], 29 grudnia 2016 r., http://www.president.gov.ua/documents/472017-21374 (dostęp: 13 kwietnia 2017 r.).

Основные положения военной доктрины российской федерации [Główne postanowienia doktryny wojskowej Federacji Rosyjskiej], 2 listopada 1993 r., http://studydoc.ru/doc/360885/osnovnye-polozheniya-voennoj-doktriny-rossijskoj-federacii (dostęp: 13 kwietnia 2017 r.).

Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р [Rezolucja rządu rosyjskiego N 1105-r z dnia 28 kwietnia 2023 r.]; https://normativ.kontur.ru/document?documentId=448153&moduleId=1 (dostęp: 21 września 2024 r.).

Sawinkin A.E., *Русская Военная Доктрина. Материалы дискуссий 1911–1939 годов [Rosyjska doktryna wojskowa. Materiały z lat 1911-1939]*, Moskwa 1994.

Strony internetowe[70]
Websites

http://www.rp-net.ru
http://www.rusdoctrina.ru
http://tass.ru
http://kremlin.ru
http://russkiymir.ru
https://zapadrus.su
http://www.ippo.ru
http://www.iisi.msu.ru
https://riss.ru
http://www.securitylab.ru
http://rushistory.org
https://www.rgo.ru
http://akademiagp.ru

[70] Spis stron internetowych, które rozwijają tematykę poniższego artykułu. Dostęp do wszystkich źródeł pochodzi z 17 maja 2017 r.

DOI:10.59800/bn/195839

prof. Marek Wrzosek[1]
Wydział Wojskowy, Akademia Sztuki Wojennej, Warszawa, Polska

ROSYJSKA DEZINFORMACJA W KONFLIKCIE ZBROJNYM W UKRAINIE

RUSSIAN DISINFORMATION IN THE ARMED CONFLICT IN UKRAINE

Abstrakt: Celem przedstawionego materiału jest zaprezentowanie czynników wpływających na sposób kreowania dezinformacji podczas rosyjskiej „wojskowej operacji specjalnej". Niestety, badane zjawisko nie doczekało się jeszcze zwartych opracowań monograficznych. Należy zwrócić uwagę na fakt, że z powodu nadal trwającego konfliktu wyniki badań będą uzupełniane przez kolejne informacje oraz pozyskiwaną na ich podstawie wiedzę naukową. Zasadniczy problem, czyli jakie są zasadnicze treści narracji wykorzystywane w procesie dezinformacji podczas wojny rosyjsko-ukraińskiej, przedstawiono w trzech aspektach: (1) podstawowe treści rosyjskiej dezinformacji w okresie destabilizacji sytuacji w Ukrainie, (2) treści informacyjne stanowiące elementy składowe rosyjskiej dezinformacji po rozpoczęciu agresji na Ukrainę, (3) osie narracji dominujące w procesie rosyjskiej dezinformacji w Polsce. Proces badawczy umożliwił wskazanie cech charakterystycznych dla doboru rosyjskich narracji podczas trwającej wojny. W zaprezentowanym materiale wykorzystano metody analizy krytycznej, a ponadto indukcji, dedukcji i syntezy. Do pozyskania materiału empirycznego użyto także wnioski i doświadczenia, które przekazali oficerowie armii ukraińskiej w czasie seminariów i konferencji organizowanych w Akademii Sztuki Wojennej.

Słowa kluczowe: dezinformacja, konflikt w Ukrainie, walka informacyjna, dominacja informacyjna

[1] 0000-0002-1369-9434, wrzosek.m.a@gmail.com.

Abstract: The aim of this article is to present the factors influencing the use of disinformation during the Russian military special operations in Ukraine. Unfortunately, the current nature of the studied phenomenon has not yet been published in comprehensive monographic studies. It should be noted that due to the ongoing conflict, the research results will be supplemented by subsequently obtained information and scientific knowledge. The fundamental problem – what are the basic contents of the narrative used in the disinformation process during the Russian-Ukrainian war – is presented in three aspects: (1) the basic content of Russian disinformation during the period of destabilization of the situation in Ukraine, (2) the information content constituting the components of Russian disinformation after the start of aggression against Ukraine, (3) the narrative axes dominant in the process of Russian disinformation in Poland. Selected examples present the methods of Russian disinformation used during the aggression against Ukraine. The research process made it possible to identify features characteristic of Russian narratives during the ongoing war. During the research, the method of critical analysis, as well as the methods of induction, deduction and synthesis was used. In obtaining empirical material, conclusions and experiences provided by Ukrainian army officers during seminars and conferences organized at the Academy of War Arts were also used.

Keywords: disinformation, conflict in Ukraine, information warfare, information domination

Wprowadzenie

W naukowym postrzeganiu rzeczywistości przyjmuje się, że społeczeństwo jest obecnie w trakcie czwartej rewolucji przemysłowej, a współczesna technologia rozwija się z większą niż kiedykolwiek dynamiką[2]. Rynek technologii informacyjnych rośnie w równie szybkim tempie i przenika coraz więcej obszarów i dziedzin funkcjonowania społecznego, gospodarczego, ale także militarnego i politycznego. Nie dziwi więc fakt, że z roku na rok liczba poszukiwanych

[2] Zob. szerzej: M. Gorynia (red.), *Świat w obliczu pandemii*, CeDeWu, Warszawa 2021.

specjalistów IT na rynku pracy stale rośnie[3]. Obserwacja efektów zachodzących przemian już na przełomie wieków wskazywała na to, że nowe technologie zmienią świat techniki, a także oblicze demokracji jako systemu politycznego.

Wkrótce okazało się, że informacja stała się nową bronią w sensie ekonomicznym i społecznym, została też wliczona do arsenału narzędzi walki dla sił zbrojnych[4]. Informacja, dostęp do niej lub jej brak stały się czynnikami, które gruntownie zmieniły obraz nowej wojny[5]. Dowodem jest metamorfoza w sposobie prowadzenia działań militarnych w Iraku i Afganistanie. W nowych operacjach militarnych technologie informatyczne pozwalały wojsku kontrolować przeciwnika dzięki znajomości jego zamiarów i środków, którymi dysponuje (poprzez zbieranie i analizę informacji). Informację wykorzystywano także w celu wprowadzenia przeciwnika w błąd (wojna psychologiczna, dezinformacja) lub do zniszczenia i unieruchomienia systemów informatycznych (np. poprzez środki walki elektronicznej).

Siły zbrojne – podobnie jak agencje informacyjne – weszły w erę „bitwy elektronicznej". Można ją postrzegać jako zbiór wszystkich technik wykorzystujących informację (będącą w tym przypadku narzędziem do wprowadzania zamieszania w przestrzeni informacyjnej przeciwnika, odstraszania go od aktywności informacyjnej, a także środkiem do wywalczenia i utrzymania przewagi informacyjnej). Już w końcu minionego wieku armia amerykańska przekonała się, że informacja może obrócić się przeciwko siłom zbrojnym podejmującym militarną interwencję[6].

[3] Na zatrudnienie mogą liczyć w pierwszej kolejności eksperci do spraw cyberbezpieczeństwa, *big data, cloud computing* oraz osoby doświadczone w obszarze sztucznej inteligencji. Według danych GUS (stan na 2021 r.) w Polsce brakuje obecnie około 50 tys. pracowników IT. Jak wynika z raportu „IT Globalne Trendy HR", przygotowanego przez Gi Group Holding, w Polsce 37,6 proc. firm zgłasza trudności w ich rekrutacji. Zob.: M. Marszycki, *Na rynku pracy nadal brakuje specjalistów IT*, ITwiz, 12 lutego 2024 r., https://itwiz.pl/na-rynku-pracy-nadal-brakuje-specjalistow-it/ (dostęp: 12 lutego 2024 r.).

[4] Por.: L. Ciborowski, *Walka informacyjna*, Toruń 1999; T. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016; P. Dela, *Założenia działań w cyberprzestrzeni*, PWN, Warszawa 2022.

[5] J. Joniak, A. Polak, *Wojny w Zatoce Perskiej: aspekty operacyjne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2011.

[6] Przykładowo pod wpływem zdjęć zabitych żołnierzy amerykańskich opinia publiczna zmusiła prezydenta Clintona do wycofania oddziałów wojskowych USA z Somalii,

W kanonach dotychczasowej sztuki wojennej powstał nowy rodzaj przewagi – „przewaga informacyjna”[7]. Mianowicie armia, która lepiej niż przeciwnik zapanuje nad zdobyczami rewolucji informacyjnej, uzyska nie tylko przewagę informacyjną, lecz także zapewni sobie zwycięstwo. Stąd tak dynamiczny rozwój walki informacyjnej w siłach zbrojnych[8], doskonalenie koncepcji działań sieciocentrycznych czy budowy zautomatyzowanych systemów dowodzenia i kierowania środkami walki.

Przez ostatnie dwa dziesięciolecia nowego wieku sieć przekazu informacji (telekomunikacja, satelity, Internet, telewizja) stała się silnym atutem w grze o zdobycie przewagi na poziomie zarówno organizacji, państwa, jak i międzynarodowych korporacji. Wyniki badań dowodzą, że większość miejsc pracy jest lub będzie związana z technologiami informatycznymi[9]. W związku z priorytetowym postrzeganiem znaczenia informacji wzrosła także rola dezinformacji jako antagonistycznego działania w kooperacji negatywnej podmiotów. Wprowadzanie treści sprzecznych z ogólną oceną lub manipulowanie zakresem przekazywanych komunikatów, a także generowanie wiadomości ukierunkowanych na odbiorcę jest realizowane

w której prowadzono operację „Przywrócić nadzieję” (*Operation Restore Hope*). Była to operacja humanitarna, prowadzona od 9 grudnia 1992 r. do maja 1993 r. w Mogadiszu. Jej głównym celem było zabezpieczenie dostaw humanitarnych i ich dystrybucja wśród mieszkańców Somalii. Podczas operacji 3 października 1993 r. amerykańskie siły specjalne przeprowadziły w stolicy Somalii, Mogadiszu, akcję mającą na celu aresztowanie dowódców klanu Habr Gidr, kierowanego przez Farraha Mohameda Aidida. W założeniu godzinna operacja przekształciła się w ponad 15-godzinną krwawą bitwę. W stolicy Somalii zginęło kilkunastu amerykańskich żołnierzy, a telewizyjne zdjęcia pokazywały, jak somalijscy bojownicy ciągnęli samochodami po ulicach miasta zwłoki. Ten incydent sprawił, że prezydent USA wycofał amerykańskie jednostki do kraju.

[7] Por.: M. Wrzosek, S. Markiewicz, Z. Modrzejewski (red.), *Informacyjny wymiar wojny hybrydowej*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2019; M. Fryc, *Sztuka zwyciężania. Strategia tworzenia i wykorzystania asymetrycznej przewagi*, Zona Zero, Warszawa 2020.

[8] Jednostki walki informacyjnej, w różnym układzie strukturalnym i zadaniowym, posiada obecnie wiele państw, m.in. Chiny, Rosja, USA, ale także Niemcy czy Polska.

[9] W marcu 2024 r. stwierdzono przecięcie kabli komunikacyjnych na dnie Morza Czerwonego. Według ocen ekspertów wpłynęło to na 25 proc. ograniczenie ruchu internetowego między Azją a Europą i zaburzyło funkcjonowanie tysięcy miejsc pracy. Zob.: *Podmorskie kable uszkodzone. Zagrożenie dla świata finansów*, 9 marca 2024 r., https://www.money.pl/gospodarka/podmorskie-kable-uszkodzone-zagrozenie-dla-swiata-finansow-7004055834422048a.html (dostęp: 11 marca 2024 r.).

w trakcie trwającego rosyjsko-ukraińskiego konfliktu zbrojnego. Dezinformację stosują obie strony konfliktu zarówno w celu zakłócenia procesów informacyjnych przeciwnika, jak i ochrony własnych zasobów informacyjnych.

Metodologia badań własnych

Celem badań, których rezultaty przedstawiono w niniejszym artykule, były zagadnienia dotyczące sposobu prowadzenia dezinformacji przez Federację Rosyjską w konflikcie rosyjsko-ukraińskim. Formalnie rosyjska agresja zbrojna na Ukrainę rozpoczęła się 24 lutego 2022 r., niemniej jednak szereg działań o charakterze informacyjno-propagandowym[10] z wykorzystaniem dezinformacji był podejmowany już wcześniej, zarówno podczas aneksji Krymu, jak i w okresie formowania się separatystycznych republik na wschodzie Ukrainy. Dlatego istotnym elementem składowym badań stało się określenie charakteru wykorzystania rosyjskich możliwości kreowania środowiska informacyjnego w procesie dezinformacji. W związku z tym główny problem badawczy sformułowano w postaci pytania, jakie były zasadnicze treści narracji wykorzystywane w procesie dezinformacji podczas wojny rosyjsko-ukraińskiej.

Odpowiedź na tak postawione pytanie jest złożona, ale z merytorycznego punktu widzenia zależy też od kontekstu rozpatrywanego zjawiska. W celu rozwiązania głównego problemu badawczego zadano następujące pytania szczegółowe:

1. Jakie były zasadnicze treści rosyjskiej dezinformacji w okresie destabilizacji sytuacji w Ukrainie?
2. Jakie treści informacyjne stanowiły elementy składowe rosyjskiej dezinformacji po rozpoczęciu agresji na Ukrainę?
3. Jakie osie narracji dominowały w procesie rosyjskiej dezinformacji w Polsce?

[10] Federacja Rosyjska stosuje określenie „działania informacyjno-propagandowe" w odniesieniu do całego spektrum aktywności w ramach walki informacyjnej, w tym także do operacji informacyjnych.

W efekcie ustalono, że armia rosyjska przygotowywała się informacyjnie do konfliktu zbrojnego z Ukrainą już od 2013 r., a zatem od czasu, gdy rozpoczęła rozwijanie swojego potencjału bojowego i reorganizację sił zbrojnych. W rosyjskiej optyce postrzegania rzeczywistości na wewnętrzny proces informacyjny te przedsięwzięcia były realizowane jako adekwatna odpowiedź Federacji Rosyjskiej na rosnące zagrożenie ze strony NATO.

W zaprezentowanym materiale przedstawiono wyniki poznawcze uzyskane metodą analizy krytycznej, której poddano materiał źródłowy (artykuły[11], raporty[12], monografie[13]). Umożliwiły one przeprowadzenie interpretacji zakresu prowadzenia dezinformacji w warunkach wojny nowej generacji[14]. Ponadto w procesie badawczym wykorzystano metody indukcji, dedukcji i syntezy, które w odniesieniu do podnoszonej problematyki pozwoliły na sformułowanie wniosków końcowych. Istotną trudnością w procesie badawczym okazała się kwestia wykorzystania obiektywnych źródeł rosyjskich – szczególnie w sytuacji, gdy szereg artykułów ma wyraźny aspekt propagandowy, przez co ich wartość merytoryczna jest niewielka. W pozyskiwaniu materiału empirycznego wykorzystano także wnioski i doświadczenia, którymi podzielili się oficerowie armii ukraińskiej w czasie seminariów i konferencji organizowanych w Akademii Sztuki Wojennej.

W procesie cyklu badawczego powstało już wiele publikacji, zróżnicowanych co do zawartości merytorycznej, obejmujących problematykę przebiegu konfliktu hybrydowego oraz rosyjskiej agresji na Ukrainę[15]. Te zagadnienia były także podejmowane na łamach pe-

[11] Zob. np.: M. Wrzosek, *Rosyjska wojskowa operacja specjalna – polityczno-militarne przyczyny porażki*, „Przegląd Sił Zbrojnych" 2023, nr 2, s. 82-92.

[12] *Endgame scenarios for Russia's war in Ukraine, International Centre For Ukrainian Victory,* czerwiec 2023 r., https://ukrainianvictory.org/wp-content/uploads/Endgame-scenarios-web.pdf (dostęp: 29 lipca 2024 r.).

[13] Por.: M. Wrzosek, *Militarne (nie)bezpieczeństwo Polski po rosyjskiej agresji na Ukrainę (2022),* Akademia Sztuki Wojennej, Warszawa 2023.

[14] Zob.: M. Wrzosek, *Przyszła wojna wielodomenowa w rosyjskiej myśli wojskowej,* w: S. Markiewicz, W. Materak (red.), *Organizacja systemu rozpoznania zagrożeń państwa – zagrożenia militarne w wielodomenowych operacjach w przyszłych konfliktach zbrojnych*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

[15] Zob.: M. Banasik, *Zagrożenia Federacji Rosyjskiej i euroatlantycka perspektywa bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2019; M. Wrzosek (red.), *Rosyjska dominacja informacyjna. W teorii i praktyce*, Akademia Sztuki Wojennej, Warszawa 2022.

riodyków o różnym zasięgu i zróżnicowanym gronie odbiorców[16]. Wiele aspektów z całego spektrum problemów rosyjskiej wojny nowego typu znalazło swoje odzwierciedlenie na łamach wydawnictw ośrodków akademickich[17]. W odniesieniu do rozpatrywanych kwestii szczególnie interesujące są publikacje bezpośrednio związane z problematyką wojny rosyjsko-ukraińskiej[18]. W Wydziale Wojskowym Akademii Sztuki Wojennej w ramach zespołu badawczego były i nadal są realizowane zamierzenia naukowe prowadzące do rozwiązywania militarnych problemów we współczesnych konfliktach zbrojnych[19].

Reasumując poczynione ustalenia w obszarze krytycznej analizy literatury, można stwierdzić, że wiedza dotycząca rosyjskiej dezinformacji jest rozproszona w wielu źródłach, czasami fragmentaryczna i pozbawiona cech naukowego opracowania przedmiotowej tematyki, stąd konieczność kontunuowania badań i kompleksowego opracowania wskazanej problematyki.

---

[16] Por.: M. Wrzosek, *Rosyjska wojskowa..., op. cit.;* P. Paprocki, *Charakterystyczne cechy działań hybrydowych – analiza porównawcza*, „Przegląd Sił Zbrojnych" 2023, nr 2; A. Szczygielska, *Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku*, „Roczniki Nauk Społecznych 2023", nr 2.

[17] Zob.: M. Banasik, *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euroatlantyckiego*, Wydawnictwo Difin, Warszawa 2018; D. Jarnicki, *Rosyjska wizja współczesnej globalnej architektury bezpieczeństwa*, Uniwersytet w Siedlcach, Siedlce 2023; B. Pacek, *Wojna hybrydowa na Ukrainie*, Oficyna Wydawnicza RYTM, Warszawa 2018. Interesujące rozważania są także zawarte w: M. Marek, *Operacja Ukraina. Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013-2019*, Wydawnictwo Difin, Warszawa 2020.

[18] Zob.: Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wyd. spec.; A. Krzak, *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015; M. Fryc, *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, „Bezpieczeństwo Narodowe" 2015, nr 33; M. Banasik, *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej,* „Kwartalnik Bellona" 2016, nr 2. Bardzo inspirujące treści z zakresu rozpatrywanej problematyki znajdują się w publikacji: W. Baluk, M. Doroszko, *Wojna hybrydowa Rosji przeciwko Ukrainie w latach 2014–2016*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2017.

[19] Por.: M. Wrzosek, *Militarne (nie)bezpieczeństwo..., op. cit.;* S. Markiewicz (red.), *Rosyjska wizja prowadzenia operacji militarnych*, Akademia Sztuki Wojennej, Warszawa 2018; S. Markiewicz (red.), *Scenariusz przebiegu konfliktu hybrydowego*, Akademia Sztuki Wojennej, Warszawa 2019.

Dezinformacja w okresie destabilizacji sytuacji w Ukrainie – rosyjskie narracje

Zgromadzone fakty prowadzą do tezy, iż wydarzenia obserwowane obecnie w Ukrainie są częścią zakrojonego na szeroką skalę planu obalenia rządu w Kijowie i podporządkowania Ukrainy Rosji. Pierwszy etap rosyjskiej dezinformacji został zapoczątkowany, gdy ukraiński parlament odsunął Janukowycza od władzy 22 lutego 2014 r. Wówczas rosyjska propaganda z wykorzystaniem dezinformacji przedstawiała nowo wybrane, prodemokratyczne władze w Kijowie jako „faszystowską kijowską juntę", a do obywateli w Rosji i w Ukrainie Wschodniej dodawano jeszcze: „na usługach Zachodu". Zarówno Polaków, jak i Rosjan czy Ukraińców przestrzegano, iż nowe władze to „nacjonalistyczni, banderowscy faszyści, mający na celu wpierw eksterminacje ludności rosyjskojęzycznej"[20], a później marsz przeciwko Polsce i zajęcie jej wschodnich obszarów. Nową polityczną sytuację w Ukrainie wykorzystano do szeroko zakrojonych działań dezinformacyjnych. Zmierzały one do wykazania na forum międzynarodowym, że Ukraina jest zdestabilizowana i pozbawiona prawowitych władz.

Kolejny etap aktywności rosyjskiej dezinformacji nastąpił w 2015 r. Po przejęciu przez Rosję Krymu podpisano porozumienia mińskie, gwarantujące zawieszenie działań zbrojnych i przewidujące scenariusz uregulowania statusu nowych pseudopaństwowych bytów. Wówczas już rosyjskie działania dezinformacyjne były ukierunkowane na izolowanie Ukrainy na arenie międzynarodowej. Rosja za pomocą różnych narracji próbowała wymóc na Kijowie realizację porozumień zgodnie z własną interpretacją podpisanych porozumień. W praktyce oznaczałoby to utratę suwerenności przez Ukrainę oraz akceptację zajęcia Krymu i prorosyjskiego Donbasu. Władze w Kijowie skutecznie się temu przeciwstawiały, a Rosja prowadziła działania dyplomatyczne mające wykazać, że Ukraina to nie narodowe państwo, lecz jedynie twór organizacyjny postrzegany

[20] Zob. szerzej: M. Marek, *op. cit.*

jako państwo, a w rzeczywistości jest niestabilna i zagraża bezpieczeństwu Europy.

Na wiele tygodni przed agresją rosyjską propaganda prowadziła wielokierunkowe działania informacyjne, które miały maskować decyzje Kremla i zwiększyć napięcia na wschodzie Ukrainy. Z tego powodu rosyjska działalność informacyjna od początku kwietnia 2021 r. koncentrowała się na publikacji tekstów mających przekonywać rosyjskie społeczeństwo, że Ukraina i NATO przygotowują się do wojny z Rosją. W rosyjskiej ocenie sytuacji bezpieczeństwa międzynarodowego okazją do rozpoczęcia działań przeciwko Rosji miały być m.in. ćwiczenia „Defender Europe 2021". Teksty publikowane w rosyjskiej prasie prezentowały Ukrainę jako stronę agresywną, która zagraża pokojowi w Europie[21]. Należy zwrócić uwagę na fakt, że ówcześnie sytuacja na wschodzie Ukrainy stawała się coraz bardziej napięta. Obserwatorzy OBWE odnotowywali coraz więcej przypadków łamania porozumienia o zawieszeniu broni. W związku z zagrożeniem separatyści ukraińscy – wspierani przez rosyjskie media – w ramach szeroko zakrojonej operacji dezinformacyjnej oskarżali Ukrainę o prowokacje i nieuzasadnione otwieranie ognia. W kryzysowej sytuacji polityczno-militarnej, sztucznie wygenerowanej przez separatystów, przedstawiciele Donieckiej i Ługańskiej Republiki Ludowej, Denis Puszylin i Leonid Pasiecznik, zwrócili się do prezydenta Rosji Władimira Putina o uznanie przez Rosję samozwańczych republik jako terytorium Federacji Rosyjskiej[22].

Kreml dążył do uzyskania gwarancji nieprzyjmowania Ukrainy do NATO oraz zamierzał doprowadzić do rewizji powojennego ładu w Europie[23]. Po niepowodzeniu tej zmasowanej ofensywy dyploma-

[21] *ibidem*.

[22] Prezydent Rosji Władimir Putin 21 lutego 2022 r. wystąpił z orędziem, w którym zapowiedział pozytywne rozpatrzenie wniosku dotyczącego niepodległości Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej. Następnie podpisał z przedstawicielami zbuntowanych ukraińskich republik międzypaństwowe układy o przyjaźni oraz porozumienie o pomocy wojskowej. W przypadku zagrożenia Rosja zobowiązała się do udzielenia obu republikom zbrojnego wsparcia. Putin formalnie ogłosił, że uznał obie republiki wraz z ich konstytucjami, w których zapisano, że terytorium tych republik rozciąga się do granic administracyjnych ukraińskich obwodów.

[23] 10 grudnia 2021 r. rosyjskie Ministerstwo Spraw Zagranicznych wydało oświadczenie o „warunkach przyszłego dialogu Federacji Rosyjskiej (FR) z USA i innymi państwami

tycznej Rosja przystąpiła do agresji zbrojnej – najpierw informacyjnie, a potem militarnie. Jej celem było podważenie państwowości Ukrainy i oderwanie od niej separatystycznych terytoriów.

W procesie dezinformacji opinii międzynarodowej prezydent Rosji wielokrotnie przedstawiał własny pogląd na Ukrainę, dostosowany do swoich potrzeb politycznych. W wystąpieniach wskazywał, że jest to obszar bez tradycji państwowości, wymyślony przez Lenina, a obecnie rządzony przez nielegalne władze pod przemożnym wpływem Zachodu, bez prawa do samodzielnego istnienia. Twierdził, że jedynie powrót do stanu sprzed rozpadu Związku Radzieckiego może przywrócić spokój w całej Ukrainie. Proces rosyjskiej dezinformacji został przygotowany na podstawie celowo dobranych faktów historycznych, których wybiórcze wykorzystanie miało uwiarygodnić przekaz informacyjny. W tym czasie oparto ją na dwóch zasadniczych narracjach, promowanych zarówno w środkach masowego przekazu, jak i w działaniach dyplomatycznych. Po pierwsze – informowano, a właściwie dezinformowano, że Ukraina destabilizuje sytuację w Donbasie, gdyż jej działalność dywersyjna zakłóca proces życia społecznego cywilnej ludności oraz funkcjonowanie lokalnej administracji państwowej. Ponadto twierdzono, że wojska ukraińskie ostrzeliwują przygraniczne miejscowości i posterunki straży granicznej, dokonują rajdów i wypadów na obszar obu republik, prowadzą działania dywersyjne i rozpoznawcze, przez co zastraszają miejscową ludność. Po drugie, donoszono, iż ukraińskie wojska koncentrują swoje siły na kierunku Doniecka i Ługańska, aby zerwać rozejm ustalony w ramach porozumień mińskich i zbrojnie podporządkować sobie obie republiki. Dla uwiarygodnienia powyższej narracji w rosyjskich środkach masowego przekazu oraz w sieciach społecznościowych pojawiały się artykuły i komentarze, które eksponowały doniesienia, czasem bardzo emocjonalne, wskazujące na

zachodnimi" na temat bezpieczeństwa europejskiego. Do najważniejszych żądań Rosji wobec USA i innych państw zachodnich wskazanych w oświadczeniu należało przyjęcie porozumienia w formie umowy prawnomiędzynarodowej (traktatu), która dawałaby Rosji długoterminowe gwarancje bezpieczeństwa poprzez wykluczenie opcji dalszego rozszerzania Sojuszu Północnoatlantyckiego na wschód. Ponadto rosyjskie żądania sprowadzały się do wycofania się Sojuszu z postanowień szczytu w Bukareszcie z 2008 r., kiedy stwierdzono, że Ukraina i Gruzja staną się członkami NATO.

pilną konieczność ochrony zagrożonej rosyjskiej ludności cywilnej w Donbasie, szczególnie w obliczu zbliżającej się ukraińskiej interwencji militarnej. W tej sytuacji Federacja Rosyjska została zmuszona, by podjąć działania mające zapewnić pomoc obywatelom rosyjskim w obwodach Ługańskim i Donieckim[24].

Strona rosyjska w działaniach dyplomatycznych podejmowała próby kreowania i narzucania zgodnej z linią Kremla interpretacji wydarzeń wokół Ukrainy (wskazywano, że w Ukrainie panuje rząd banderowców, państwo jest upadłe i skorumpowane, bez własnej historii i tradycji narodowych), szczególnie wśród zwolenników Rosji. Wszystko w celu podtrzymania poparcia rosyjskojęzycznej społeczności na świecie i promowania akceptacji dla podejmowanych działań[25]. Działania dezinformacyjne były prowadzone tak, by odsunąć od Federacji Rosyjskiej oskarżenia o eskalację napięcia w Europie. Takie głosy pojawiały się w związku z koncentracją rosyjskich wojsk wokół Ukrainy. Wówczas minister spraw zagranicznych Siergiej Ławrow zaprezentował w imieniu Federacji Rosyjskiej oficjalne stanowisko, z którego wynikało, że nikt nie ma prawa narzucać Rosji, gdzie może, a gdzie nie może prowadzić manewrów wojskowych na swoim własnym terytorium[26]. Mimo jasnych oznak zbliżającego się konfliktu zbrojnego Rosja w ramach dezinformacji kwestionowała wiarygodność danych wywiadowczych przekazywanych przez Stany Zjednoczone i Wielką Brytanię. Na dowód nierzetelności ich ocen rosyjska dyplomacja przywoływała sytuację z 2003 r., gdy Amerykanie wskazywali na Irak jako państwo rozwijające systemy broni masowego rażenia[27]. W tym aspekcie Rosja głosiła także prawdopodobieństwo

[24] P. Kirby, *Why Russia is trying to capture eastern Ukraine*, BBC News, 26 maja 2022 r., https://www.bbc.com/news/world-europe-60938544 (dostęp: 11 stycznia 2024 r.).

[25] *Examples of Russian disinformation and the facts*, Bundesministerium des Innern und für Heimat, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/examples-of-russian-disinformation-and-the-facts.html (dostęp: 23 lutego 2023 r.).

[26] *Ławrow: wojskowe manewry rosyjsko-białoruskie zakończą się zgodnie z planem*, „Rzeczpospolita", 17 lutego 2022 r., https://www.rp.pl/dyplomacja/art35700521-lawrow-wojskowe-manewry-rosyjsko-bialoruskie-zakoncza-sie-zgodnie-z-planem (dostęp: 23 lutego 2024 r.).

[27] J. Raubo, *Rosjanie rzucają do boju w wojnie informacyjnej wszystkie narracje*, Defence24, 20 lutego 2022 r., https://defence24.pl/geopolityka/rosjanie-rzucaja-do-boju-wszystkie-mozliwe-narracje-komentarz (dostęp; 22 lutego 2022 r.).

wyprodukowania przez Ukrainę broni jądrowej. Argumentowano, że Ukraina posiadała broń jądrową i w związku z tym nadal dysponuje specjalistami oraz technologią do jej produkcji. Dodatkowo wskazywano na możliwość przygotowania przez Ukrainę „brudnej bomby", powstałej z odpadów radioaktywnych zgromadzonych w czterech funkcjonujących elektrowniach jądrowych[28].

Kolejny wątek dezinformacyjnej narracji stanowiła rosyjska pomoc humanitarna, będąca reakcją na trudną sytuację na wschodzie Ukrainy. W tym celu rosyjskie ministerstwo obrony powołało dowództwo humanitarnej odpowiedzi, które organizowało wparcie dla mieszkańców obwodów ogarniętych klęską humanitarną. Sytuacja dotyczyła szczególnie tych miejscowości, w których – zgodnie z rosyjską narracją – wojska ukraińskie uniemożliwiały wyjście ludności cywilnej z obszaru walk. W rosyjskich transportach zaopatrzenia, które formalnie były określane jako dostawy pomocy humanitarnej dla mieszkańców okupowanych terenów Ukrainy, armia rosyjska przewoziła setki ton amunicji i innego wyposażenia dla swoich wojsk. Wbrew deklaracjom w rejon konfliktu dostarczano w rzeczywistości zimowe umundurowanie, przeznaczone dla jednostek prorosyjskich operujących w Donbasie. Zaopatrzenie (żywność czy materiały higieniczne) nie było natomiast przeznaczone dla lokalnej ludności, lecz dla wojsk prorosyjskiego kontyngentu, wspierającego separatystyczne władze w obwodach Ługańskim i Donieckim[29].

[28] Władimir Putin w przemówieniu wskazał, że Rosja nie może pozwolić Ukrainie na ponowne pozyskanie nawet taktycznej broni jądrowej, a Kijów jest dosłownie o krok od jej stworzenia. Zob.: *Rosja oskarża Ukrainę o sprowadzanie materiałów do „brudnej bomby". Jest mowa o Polsce*, „Rzeczpospolita", 25 czerwca 2024 r., https://www.rp.pl/konflikty-zbrojne/art40701931-rosja-oskarza-ukraine-o-sprowadzanie-materialow-do-brudnej-bomby-jest-mowa-o-polsce (dostęp: 25 czerwca 2024 r.).

[29] *Russia Crisis Military Assessment: The race to resupply Ukraine*, Atlantic Council, 27 kwietnia 2022 r., https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-crisis-military-assessment-the-race-to-resupply-ukraine/ (dostęp: 12 lutego 2024 r.).

Rosyjska dezinformacja po rozpoczęciu agresji na Ukrainę

Prezydent Federacji Rosyjskiej wielokrotnie wskazywał, że w jego przekonaniu Ukraina to „państwo sztuczne". W rosyjskim ujęciu było ono rozumiane jako obszar, którego granice polityczne nie są zgodne z podziałem narodowościowym, funkcjonującym wśród ludności zamieszkującej geograficzną przestrzeń. W przekonaniu Putina o sztuczności granic miałyby decydować zatem dwa czynniki: po pierwsze, w jaki sposób granice dzielą różne grupy etniczne między dwa różne państwa, a po drugie, założenie, że wytyczone granice są najprawdopodobniej nienaturalne, a więc sztuczne. Rozwijając ten sposób rozumowania na praktykę dezinformacji rosyjskiej, można zauważyć, że w takim ujęciu sztuczne państwa to byty stworzone przez dotychczasowe państwa kolonialne lub mocarstwa w traktatach powojennych, na mocy których różne grupy etniczne, językowe czy religijne zostały złączone lub odseparowane bez poszanowania aspiracji tych grup[30]. Taka teoria stała się zasadniczą treścią narracji rosyjskiej w aspekcie podważania zasadności funkcjonowania państwa ukraińskiego. Rozpad różnych federacji, w tym Jugosławii czy ZSRR, to następstwo dążenia narodów do samostanowienia. W każdym ze wskazanych przypadków nie było jednak możliwe wytyczenie granicy zgodnie z aspiracjami poszczególnych grup etnicznych, religijnych czy językowych oraz bez rozdzielenia jednych nacji i łączenia innych. W tym kontekście tezy prezydenta są pozbawione argumentów merytorycznych i służą jedynie za przesłankę polityczną do deprecjonowania Ukrainy jako państwa i jej obywateli rozumianych jako odrębny naród.

W nocy z 21 na 22 lutego 2022 r. rosyjskie wojska na prośbę obu zbuntowanych ukraińskich republik weszły na terytorium Donbasu. Prezydent Putin powierzył im rolę misji pokojowej, gdyż – według

[30] Większość granic w Europie nabierała nowego kształtu i zmieniała się w wyniku prowadzonych wojen. Faktem jest także, iż powodem wojen były spory i pretensje terytorialne argumentowane w większości historyczną tradycją oraz etniczną tożsamością miejscowej ludności. W wielu przypadkach jednak tereny pogranicza były etnicznie, językowo i religijnie wymieszane, co skutkowało sprzecznymi aspiracjami miejscowej ludności.

stanowiska Moskwy – ludność tych obszarów była narażona na atak ukraińskich sił zbrojnych, rzekomo ostrzeliwujących tereny w pobliżu linii rozgraniczenia. W tym czasie rosyjskie środki masowego przekazu wzmacniały poziom dezinformacji i informowały opinię publiczną o wielu ukraińskich prowokacjach. W rzeczywistości wszystkie doniesienia były tylko propagandowym wymysłem rosyjskich autorów dezinformacji[31]. Sama nazwa „wojskowej operacji specjalnej" miała wskazywać na ograniczony charakter działań militarnych, których zasadniczym celem była demilitaryzacja i denazyfikacja Ukrainy. Zgodnie z narracją rosyjskiej propagandy nie chodziło zatem o opanowanie obszaru Ukrainy, a jedynie osiągnięcie politycznych celów, które miały zagwarantować bezpieczeństwo i wewnętrzny ład publiczny. Dla podtrzymania toku narracji administracja rosyjska zakazała stosowania w sferze informacyjnej terminów „wojna", „konflikt" czy „ofensywa militarna". Od początku napaści na Ukrainę jedynym dopuszczalnym sformułowaniem była „specjalna operacja wojskowa". Zgodnie z linią kremlowskiej narracji Rosyjski Trybunał Konstytucyjny odrzucił wnioski organizacji praw człowieka o uchylenie ustawy, która zabraniała wypowiadania się przeciwko rosyjskiej inwazji na Ukrainę.

Pomimo wzrostu intensywności działań militarnych w Ukrainie rosyjskie media utrzymywały, że celem „wojskowej operacji specjalnej" jest – zgodnie z oświadczeniem prezydenta Rosji – obrona prorosyjskich republik przed ukraińską armią. Rosyjskie władze zablokowały media, które używały określenia „wojna". Niezależne radio „Echo Moskwy" zostało wyłączone, a telewizja „Dożdż" zamknięta na wniosek prokuratury generalnej z powodu publikacji „kłamliwych informacji na temat działań wojsk rosyjskich" w Ukrainie. Rosyjski parlament ustanowił, że za przygotowanie „fake newsów" grozi kara do trzech lat więzienia, a za ich szerzenie od 5 do 10 lat, jeśli rozpowszechniane są przez Internet bądź przez grupę ludzi[32]. Obecnie

[31] P. Christopher, M. Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, 11 lipca 2016 r., https://www.rand.org/pubs/perspectives/PE198.html (dostęp: 18 marca 2024 r.).

[32] Rosja testowała już odłączenie się od globalnego Internetu w 2019 r. Taką operację przeprowadzano wtedy podczas 30-dniowego testu. Rosja przyjęła też ustawę

w Rosji najwyższa kara – 15 lat więzienia – grozi „osobom rozpowszechniającym informacje, których skutki są społecznie niebezpieczne". Pomimo blokady informacyjnej do rosyjskiej społeczności coraz częściej dociera prawda o skutkach wojny w Ukrainie. Oficjalnie władze rosyjskie twierdzą, że tylko profesjonalni żołnierze wykonują zadania w ramach operacji specjalnej[33]. Tymczasem rosyjscy poborowi, którzy trafili do ukraińskiej niewoli, za pomocą udostępnionych im telefonów informują swoje rodziny o faktycznej sytuacji. Przekazują prawdziwy obraz wojny, a nie „misji pokojowej", dementują kłamstwa rosyjskiej dezinformacji i stanowią świadectwo rozwoju imperialnej polityki Rosji.

W miarę jak w czasie walki zbrojnej wzrastały straty, w armii rosyjskiej zmieniła się narracja dotycząca sposobu relacjonowania „specjalnej operacji wojskowej". Rosjanie coraz częściej informowali, że działania zbrojne w Ukrainie są podtrzymywane przez państwa zachodnie. Jako argument wskazywano, że 27 państw europejskich, w tym Wielka Brytania oraz USA, zgodziły się przekazać Ukrainie broń, środki medyczne i dodatkową pomoc wojskową. Rosyjskie władze twierdziły, że w ten sposób kraje niemal całego świata zależnego od USA wspierają Ukrainę w walce z rosyjską armią[34].

W rosyjskiej prasie ukraiński prezydent nazywany jest zbrodniarzem wojennym, gdyż odpowiada za niewinne ofiary wojny, zniszczenia oraz brak pomocy humanitarnej dla obywateli Donbasu[35]. Inna oś rosyjskiej narracji wskazuje, że Zełenski „nie dba o Ukrainę", kolaboruje bowiem ze światem zachodnim i wciąga państwo w sieć

o „suwerennym Internecie", która zakładała przebudowę struktury sieci tak, by rosyjska komunikacja internetowa przebiegała przez węzłowe punkty wewnątrz kraju.

[33] Zob.: *Putin: Poborowi nie biorą i nie będą brać udziału w operacji specjalnej na Ukrainie*, „Rzeczpospolita", 7 marca 2022 r., https://www.rp.pl/polityka/art35823001-putin-poborowi-nie-biora-i-nie-beda-brac-udzialu-w-operacji-specjalnej-na-ukrainie (dostęp: 11 marca 2024 r.).

[34] W. Kazanecki, *Porozumienie niemal 30 państw. Przekażą broń Ukrainie*, Interia.pl, 26 lutego 2022 r., https://wydarzenia.interia.pl/raporty/raport-ukraina-rosja/aktualnosci/news-porozumienie-niemal-30-panstw-przekaza-bron-ukrainie,nId,5857148#utm_source=paste&utm_medium=paste&utm_campaign=firefox (dostęp: 23 lutego 2024 r.).

[35] A. Wrona, *Kłamstwa w nagłówkach. Jak Rosja przedstawia inwazję na Ukrainę?*, Onet.pl, 3 marca 2022 r., https://www.onet.pl/informacje/pravdaorgpl/klamstwa-w-naglowkach-jak-rosja-przedstawia-inwazje-na-ukraine/eblnb6g,30bc1058 (dostęp: 11 stycznia 2024 r.).

ekonomiczno-finansowych zależności od zachodnich koncernów. Co więcej, w przekazach informacyjnych generowano wiadomości, że w Ukrainie „szaleją nacjonaliści", którzy wprowadzają własne rozwiązania prawne i szykanują rosyjskojęzyczną ludność. W opinii rosyjskiej propagandy nacjonalistyczna i militarystyczna histeria, wywoływana przez kijowski reżim, przybrała rasistowski wymiar, a cudzoziemcy, którym nie udało się opuścić na czas Ukrainy, są prześladowani, zatrzymywani i kierowani do obozów internowania lub osadzani w więzieniach[36].

W oficjalnym przekazie informacyjnym rosyjskie służby niezmiennie akcentowały fakt, że zasadniczym celem użycia rosyjskich sił zbrojnych była „ochrona ludności Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej". Wskazywały, że prezydent Putin chce przywrócić międzynarodowy porządek prawny i doprowadzić do stabilizacji sytuacji w Ukrainie oraz wybrania nowych władz zgodnie z ukraińską konstytucją. W opinii rosyjskich komentatorów sprzyjających władzy Ukraińcy zaczynają rozumieć, że nie ma sensu oddawać życia za skorumpowany naród (autorskie wskazanie) i już niedługo prawdopodobnie z radością powitają wojska rosyjskie jako gwaranta normalizacji życia społecznego i politycznego. Według informacji rosyjskiej telewizji wyrazem poparcia dla operacji specjalnej była dobrowolna kapitulacja dwóch ukraińskich garnizonów: Tokmoku i Wasylówki[37].

W odpowiedzi na liczne komentarze i filmy krążące po ukraińskich portalach społecznościowych, w których pokazywano akty okrucieństwa agresora, rosyjska propaganda dowodziła, że fabuły rozsyłane jako materiał filmowy nie mają nic wspólnego z tym, co się dzieje w Ukrainie. W opinii rosyjskiej dezinformacji prezentowane zdjęcia i filmy to obrazy pochodzące z nieznanych miejsc czy z minionych konfliktów prowadzonych w różnych częściach świata.

[36] *Russia's use of disinformation and information manipulation,* Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng (dostęp: 23 stycznia 2024 r.).

[37] Zob. szerzej: A. Karnaukh, *Świadomość narodowa w zmieniającym się społeczeństwie ukraińskim na przykładzie Ukraińców, Rosjan i Bułgarów na Zaporożu,* „Kultura i społeczeństwo" 2015, nr 2.

Czasem na potrzeby dezinformacji wskazywano również, że są to fragmenty wycięte z kadrów z serbskiego kina lub kroniki chińskich incydentów. Te osie narracji rosyjskiej dezinformacji są nadal rozwijane i uzupełniane przez kolejne propagandowe artykuły, które brzmią niemal surrealistycznie w obliczu wojny panującej w Ukrainie. Niestety, wyniki badań przeprowadzonych przez ukraiński ośrodek wskazują, że przekazywane treści odnoszą założony skutek w rosyjskiej przestrzeni informacyjnej, gdyż w wielu zachodnich agencjach pojawiają się doniesienia o trudnościach komunikacyjnych w kontaktach z rodzinami przebywającymi w Rosji[38]. Ukraińcy od swoich rodzin zamieszkujących w Rosji słyszą propagandowe wiadomości o nazistach zasiedlających ich kraj, szerzącej się korupcji, rozkradaniu zachodnich pożyczek czy luksusowych wyjazdach żony prezydenta Ukrainy[39]. Tymczasem Ukraina stara się podważać poparcie dla wojny wśród rosyjskich obywateli, stąd na przykład decyzja o umożliwieniu rosyjskim matkom odebrania ciał zmarłych na polu bitwy synów i mężów[40]. Wobec takiego nagromadzenia kłamliwych informacji o Ukrainie przekazanie prawdziwego obrazu wojny w rosyjskim społeczeństwie jest nadal niezwykle trudne[41].

[38] K. Kasianenko, *Learning from Russian Propaganda and Disinformation in Ukraine,* Australian Institute of International Affairs, 6 marca 2024 r., https://www.internationalaffairs.org.au/australianoutlook/learning-from-russian-propaganda-and-disinformation-in-ukraine/ (dostęp: 29 stycznia 2024 r.).

[39] Autor jednego z wpisów na portalu X twierdzi, że Ołena Zełenska wydała 1,1 mln dol. na biżuterię u Cartiera, a dowodem rzekomego zakupu ma być dołączone zdjęcie faktury z logo firmy. Widnieje na nim m.in. nazwisko Ołeny Zełenskiej i data wystawienia 22 września 2023 r. Wbrew temu, co głosi zamieszczony wpis, pierwsza dama Ukrainy nie nabyła biżuterii w nowojorskim Cartierze, a rzekomy paragon jej zakupów został sfałszowany. Ołena Zełenska nie mogła 22 września być w sklepie Cartiera w Nowym Jorku, ponieważ tego dnia nie przebywała w USA. Towarzyszyła wówczas swemu mężowi w Kanadzie. Trudno też sobie wyobrazić, że niepostrzeżenie opuściła oficjalną delegację, żeby wrócić do Nowego Jorku na zakupy, gdyż sklep Cartiera zamyka się o godz. 19:00.

[40] Na portalach Reddit i TikTok popularny stał się film, w którym zatrzymany żołnierz rosyjski kłóci się z własną matką, broniącą Władimira Putina.

[41] *Rosyjskie matki uwierzyły w propagandę Putina,* Spider's Web, https://spidersweb.pl/rozrywka/2022/03/09/rosyjska-propaganda-ukraina-wojna-wladimir-putin-telewizja-reddit-tiktok (dostęp: 13 lutego 2023 r.).

Rosyjska dezinformacja w Polsce

Od początku napaści Rosji na Ukrainę rosyjscy i prorosyjscy agitatorzy podejmują rożne formy aktywności informacyjnej skierowanej na podważanie relacji polsko-ukraińskich. Wyniki analiz wskazują, że dezinformacja prowadzona jest dwukierunkowo: do ludności ukraińskiej i do społeczeństwa polskiego. Relacje polsko-ukraińskie od dawna stanowią kluczowy element w rosyjskich działaniach informacyjno-propagandowych. Podstawą kreowania treści dezinformacyjnych w tym obszarze są resentymenty historyczne i „czarne karty" historii obu krajów. Dlatego celem prowadzonej dezinformacji jest wzbudzenie niechęci Polaków do udzielania pomocy i wsparcia zaatakowanej Ukrainie, a szczególnie do szukających schronienia Ukraińców. W rosyjskich mediach prezentowano anonimowe historie o rzekomym pierwszeństwie ukraińskich uczniów w wyborze szkoły. Rosyjska propaganda dyskredytowała także płynącą z Polski pomoc, wszelkie gesty solidarności i przede wszystkim spóźnione reakcje administracji państwowej, której obowiązki przejęła lokalna ludność pochodzenia ukraińskiego, a mieszkająca w Polsce.

Długoterminowe działania dezinformacyjne w przekonaniu strony rosyjskiej zakłócą relacje polsko-ukraińskie poprzez wrogie nastawienie ku sobie obu społeczeństw. Rosjanie zakładają, że w efekcie zwaśnienia obu stron dojdzie do aktów agresji, rozbojów, ataków chuligańskich, a nawet niepokojów społecznych, co doprowadzi do destabilizacji sytuacji wewnętrznej Polski.

Rosyjska dezinformacja koncertowała się także na odbudowie etnicznej wschodnich obszarów Polski i tłumaczyła Polakom, że zwiększona migracja Ukraińców to próba nowej „akcji przesiedleńczej", prowadzonej w celu zajęcia przedwojennych obszarów ukraińskich. W odpowiedzi na działania Ukraińców – według rosyjskiej dezinformacji – strona polska przygotowuje do walki nowo powstałą formację bojową, czyli 18. Dywizję Zmechanizowaną. Ponadto wkrótce do walki na obszarze zachodniej Ukrainy mają zostać przygotowane kolejne dwa związki taktyczne: 1. Dywizja Piechoty Legionów oraz 8. Dywizja Piechoty Armii Krajowej im. Romualda Traugutta.

W rosyjskim postrzeganiu akcentowany jest zatem agresywny charakter polskich działań militarnych, których efektem będzie zajęcie przez Polskę obszaru Ukrainy Zachodniej.

Rosjanie na potrzeby dezinformacji wykorzystują także fakt, że zarówno w Polsce, jak i w Ukrainie istnieje bardzo silne przywiązanie do własnego terytorium i wierność zasadzie nienaruszalności granic. Takie terminy jak „rozbiór" czy „podział" mają niezwykle silnie negatywne oddziaływanie i wzbudzają w obu społeczeństwach bardzo emocjonalne reakcje. Z tego względu rosyjska propaganda ustawicznie wykorzystuje motyw spornych obszarów obu krajów i cyklicznie publikuje doniesienia wskazujące, że Ukraińcy mają roszczenia terytorialne względem Polski i chcą przyłączenia naszych południowo-wschodnich ziem do swoich granic. Z drugiej strony wskazują, że polskie tereny sięgały daleko w głąb obszaru obecnej Ukrainy, a zatem Polacy nie porzucili koncepcji przyłączenia zachodniej Ukrainy do Polski. Bandera, Wołyń, OUN, UPA to bardzo dobrze dobrane tematy historyczne sprzyjające antagonizowaniu stosunków polsko-ukraińskich[42]. Wszystkie sporne kwestie historyczne stanowią dla Rosjan pożywkę do generowania dezinformacji. Przykładowo rosyjska propaganda kilka dni po wycofaniu się oddziałów rosyjskich z Buczy i ujawnieniu masowych zbrodni, których dopuścili się rosyjscy agresorzy, zasugerowała polskiej i ukraińskiej opinii publicznej, że wydarzenia w Buczy nie były prawdziwym ludobójstwem[43], ponieważ masakra na Wołyniu osiągnęła znacznie większą skalę[44].

Rosyjska dezinformacja objęła także zagadnienia kryzysu żywnościowego. W mediach społecznościowych odpowiedzialność zbiorową za zaistniałą sytuację, szczególnie widmo głodu na Bliskim

[42] Brak współpracy historycznej skutkuje tym, że zarówno postacie, jak i ukraińskie wydarzenia są inaczej odbierane w obu krajach – dla przykładu dla Ukraińców Bandera to przede wszystkim symbol walki z Sowietami, a dla Polaków to symbol ukraińskiego nacjonalizmu.

[43] Szacuje się, że w trakcie pobytu rosyjskich oddziałów w Buczy mogło zostać zamordowanych ponad 400 nieuzbrojonych ukraińskich cywilów. Ta liczba nie została jednak do tej pory potwierdzona przez ONZ, które nadal prowadzi w sprawie śledztwo.

[44] Ocenia się, że w sumie w latach 1943-1945 na Wołyniu i w Galicji Wschodniej zginęło ok. 100 tys. Polaków, zamordowanych przez oddziały Ukraińskiej Armii Powstańczej oraz miejscową ludność ukraińską.

Wschodzie i w Północnej Afryce, przypisywano Zachodowi. W opinii rosyjskich polityków to zachodnie sankcje uniemożliwiały Rosji, największemu na świecie eksporterowi pszenicy, zaopatrywanie innych krajów w zboże. Takie twierdzenia były wspierane oświadczeniami rosyjskiego MSZ, które jako przyczynę powstania sytuacji kryzysowej wskazywało „jednostronne antyrosyjskie restrykcje" i „wypowiedzianą przez UE totalną wojnę handlową". Te oskarżenia nie miały jednak pokrycia w faktach, ale stanowiły podstawę do wygenerowania negatywnego wizerunku Polski, która podczas transportu ukraińskiego zboża pobierała dodatkowe opłaty i handlowała zapasami po zaniżonych cenach.

Nowym elementem rosyjskiej narracji jest dezinformacja koncentrująca się na demonstrowaniu i opisywaniu zdolności uderzeniowych rosyjskich sił zbrojnych. W ramach tego rodzaju działalności w polskiej przestrzeni informacyjnej prezentowane są potencjalne możliwości wykonania uderzeń bronią nuklearną[45]. Ponadto poprzez eksponowanie drastycznych zdjęć i filmów z działań zaczepnych prowadzonych na pozycje ukraińskie Rosja zamierza wzbudzić lęk, a nawet strach przed swoimi siłami zbrojnymi. W materiałach telewizyjnych pokazuje transporty ciężkiego sprzętu bojowego i nowych jednostek wojskowych, aby wzbudzić przerażenie i przekonać zarówno swoje, jak i polskie oraz ukraińskie społeczeństwo do potencjału rosyjskiej potęgi militarnej.

Rosjanie powrócili też do działań informacyjnych opartych na micie „wojny ojczyźnianej" z okresu II wojny światowej. We własnym społeczeństwie próbują kształtować postrzeganie „specjalnej operacji wojskowej" jako konfliktu o dużej skali trudności, przełomowego i zagrażającego egzystencji Rosji, podobnie jak w okresie II wojny światowej, a więc zdarzenia wymagającego poświęcenia od każdego rosyjskiego obywatela. Tego rodzaju działania to kolejny element wysiłku dezinformacyjnego Kremla na rzecz przygotowania rosyjskiego społeczeństwa do perspektywy długotrwałej wojny w Ukrainie. Można także oceniać je w kategoriach psychologicznego przygotowania

[45] *Rosja straszy nuklearną triadą*, Wirtualny Nowy Przemysł, https://www.wnp.pl/przemysl-obronny/rosja-straszy-nuklearna-triada,807925.html (dostęp: 14 lutego 2024 r.).

ludności do kolejnych etapów mobilizacji oraz zwiększenia zaangażowania rosyjskich wojsk w działania militarne przeciwko Ukrainie.

Z przeprowadzonych obserwacji wynika, że każdy temat związany z polską armią stanowi dla Rosji obszar dezinformacji – na przykład powołania na ćwiczenia wojskowe Rosjanie przedstawiają jako tajną mobilizację wojska. W opinii rosyjskich informatorów mobilizacja budzi sprzeciw Polaków. W związku z tym plany polskiego resortu obrony narodowej dotyczące niemal każdych ćwiczeń wojskowych są wykorzystywane do uwiarygodnienia rosyjskich linii narracji o rzekomych agresywnych planach Polski.

W kwietniu 2023 r. w polskich mediach społecznościowych rozeszły się komunikaty, z których treści wynikało, że Ministerstwo Obrony Narodowej prowadzi rekrutację do korpusu litewsko-polsko-ukraińskiego. W treści rozpowszechnianej dezinformacji podkreślano, że dotychczas była to brygada licząca ok. 4500 żołnierzy, a obecnie polskie władze wojskowe przeformowały ją na korpus polsko-ukraińsko-litewski, który prawdopodobnie zostanie w niedalekiej przyszłości skierowany do walk w Ukrainie[46]. Fałszywą wiadomość upowszechniały przez kilka dni konta powiązane z rosyjską propagandą. Wszystko wskazuje na to, że dezinformacja została przygotowana przez rosyjski aparat propagandowy, aby uwiarygodnić przekaz o rzekomych planach militarnego zaangażowania się Polski i Litwy w konflikt w Ukrainie. MON w swoich komunikatach ostrzegało, że jest to operacja dezinformacyjna będąca częścią szerszej kampanii prowadzonej m.in. przez „białoruską grupę UNC1151".

Bardzo atrakcyjnym tematem dla rosyjskiej dezinformacji stał się program bezpłatnych szkoleń wojskowych realizowanych niemal w całej Polsce pod hasłem „Trenuj z wojskiem". To inicjatywa prospołeczna i proobronna, w ramach której można odbyć podstawowe,

[46] Adres mailowy, podany do kontaktu dla potencjalnych ochotników wstępujących do korpusu, jest prawdziwy, a międzynarodowa brygada rzeczywiście istnieje i ma siedzibę w Lublinie, ale wbrew rosyjskim informacjom nie jest wcale korpusem. Litewsko-Polsko-Ukraińska Brygada, do której rzekomo miała trwać rekrutacja, została utworzona w 2014 r. Liczy ona ponad 4 tys. żołnierzy z trzech krajów. Na co dzień stacjonują oni w swoich jednostkach macierzystych wchodzących w skład brygady. Jedynie dowództwo stacjonuje w Lublinie, a obowiązki osób funkcyjnych pełnią naprzemiennie oficerowie z Polski, Litwy i Ukrainy. Obecnie dowódcą jest Polak, gen. bryg. Jarosław Mokrzycki.

bezpłatne przeszkolenie wojskowe, prowadzone w jednostkach wojskowych przez wykwalifikowaną kadrę. Aby zgłosić się na takie 8-godzinne szkolenie, wystarczyły tylko imię, nazwisko, wiek i kontakt. Grupy do szkolenia wojskowego mogli zgłaszać także ich liderzy i opiekunowie. Czwarta edycja programu była realizowana pod hasłem „Trenuj z wojskiem – sam i w grupie". Trwała od września do końca października 2023 r. Do udziału zaproszono nie tylko ochotników indywidualnych, lecz także grupy środowiskowe, w tym organizacje, urzędy, stowarzyszenia, związki, zakłady pracy, firmy, kluby. Strona rosyjska oceniła akcję „Trenuj z wojskiem" jako ukrytą formę przygotowania wojskowego dla osób cywilnych, które w przypadku konfliktu zbrojnego zostaną w przyszłości wcielone do armii. W rosyjskim przekazie program funkcjonuje jako skryte mobilizacyjne przygotowywanie wybranych jednostek bojowych do przyjęcia przeszkolonych żołnierzy rezerwy.

Podsumowanie

Podstawą rosyjskiej dezinformacji i propagandy w trakcie wojny jest negowanie Ukrainy jako państwa. Po inwazji w 2022 r. rosyjskie władze i prokremlowskie media oraz portale społecznościowe (m.in. RT i Sputnik) stosowały przyjętą na potrzeby kryzysu nową retorykę. W tym celu w odniesieniu do władz ukraińskich stosowano takie określenia, jak „reżim kijowski", „marionetki Waszyngtonu", „faszyści", „naziści". Czyniono to przede wszystkim po to, aby dyskredytować Ukrainę, dehumanizować działania militarne ich sił zbrojnych i przekonać własną opinię publiczną o silnym amerykańskim wpływie na Ukrainę.

W kontekście wydarzeń w Ukrainie można postawić tezę, że wojna informacyjna prowadzona przez Federację Rosyjską przeciwko Zachodowi ma służyć wzmocnieniu jej pozycji międzynarodowej i skuteczniejszemu osiąganiu celów strategicznych w niezaangażowanych rejonach świata. Rosja poprzez działania dezinformacyjne dąży do uwzględnienia swoich żądań dotyczących bezpieczeństwa

w Europie, m.in. w kwestii rozszerzenia NATO na wschód, a także uzyskania zwycięstwa na froncie ukraińskim. Dlatego deprecjonując Ukrainę, Rosja stara się osłabić poziom poparcia dla walczącego państwa i próbuje wpłynąć na przebieg debaty w Europie i USA, wywołując i utrzymując antyukraińskie nastroje. Poprzez dezinformację zamierza także podważyć zasadność zachodnich sankcji i przedstawić je jako niesprawiedliwy nacisk gospodarczy na Rosję.

Na podstawie poczynionych analiz oraz wyników obserwacji można postawić tezę, że celem rosyjskiej propagandy jest nie tylko podsycanie napięć, izolowanie Ukrainy czy udaremnianie proaktywnej postawy wobec Kijowa. Dodatkowo należy wskazać, że działania dezinformacyjne skierowane są na budzenie niepokoju w polskim i ukraińskim społeczeństwie. Federacja Rosyjska za pośrednictwem fałszywych narracji będzie prawdopodobnie starała się wystawić na próbę solidarność międzynarodową, sprawdzić trwałość determinacji państw europejskich w procesie wsparcia walczącej Ukrainy, a także obniżyć poziom ciągłości w realizowanych działaniach pomocowych.

Z tego względu objęcie sankcjami wielu ośrodków propagandowych Federacji Rosyjskiej stanowi ważny instrument, który wskazuje na brak zgody na działania dezinformacyjne Rosji prowadzone w globalnej przestrzeni informacyjnej. Właściwym sposobem przeciwdziałania rosyjskiej dezinformacji jest także wykorzystywanie doświadczeń w procesie upowszechniania wiedzy o tym, w jaki sposób rosyjska propaganda celowo kształtuje emocje odbiorców: próbuje ona zawładnąć umysłami i systemami przekonań dominującymi w atakowanych społeczeństwach zachodnich.

Jednym z głównych celów rosyjskiej dezinformacji pozostaje przedstawianie inwazji na Ukrainę jako rezultatu gry zachodnich mocarstw. Rosja promuje narrację, zgodnie z którą to Stany Zjednoczone sprowokowały ją poprzez rozszerzanie NATO na wschód Europy do podjęcia działań asekurujących rosyjskie bezpieczeństwo w sferze militarnej. Przyjęta narracja pomaga przedstawić Rosję jako obiekt negatywnego oddziaływania państw Zachodu. W związku z zaistniałą sytuacją Rosja musiała podjąć działania obronne w wymiarze nie tylko dyplomatycznym, lecz także militarnym.

Dezinformacji, która jest specyficznym rodzajem broni w rosyjskiej wojnie informacyjnej, można skutecznie przeciwdziałać jedynie poprzez zweryfikowane i wiarygodne informacje, generowane przez zaufane źródła. Istotnym czynnikiem w walce z rosyjską dezinformacją okazuje się konsekwentne ujawnianie (demaskowanie) fałszywych narracji oraz ostrzeganie opinii międzynarodowej przed zjawiskiem ulegania złowrogiej rosyjskiej propagandzie. Z tego też względu należy zadbać o odporność społeczeństwa polskiego na dezinformację ze strony Rosji.

Bibliografia
References list

Aleksandrowicz T., *Podstawy walki informacyjnej*, Warszawa 2016.

Baluk W., Doroszko M. (red.), *Wojna hybrydowa Rosji przeciwko Ukrainie w latach 2014–2016*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2017.

Banasik M., *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euroatlantyckiego*, Wydawnictwo Difin, Warszawa 2018.

Banasik M., *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej*, „Kwartalnik Bellona" 2016, nr 2.

Banasik M., *Zagrożenia Federacji Rosyjskiej i euroatlantycka perspektywa bezpieczeństwa*, Wydawnictwo Difin, Warszawa 2019.

Christopher P., Matthews M., *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, 11 lipca 2016 r., https://www.rand.org/pubs/perspectives/PE198.html (dostęp: 18 marca 2024 r.).

Ciborowski L., *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 1999.

Dela P., *Założenia działań w cyberprzestrzeni*, PWN, Warszawa 2022.

Endgame scenarios for Russia's war in Ukraine, International Centre For Ukrainian Victory, czerwiec 2023 r., https://ukrainianvictory.org/wp-content/uploads/Endgame-scenarios-web.pdf (dostęp: 29 lipca 2024 r.).

Examples of Russian disinformation and the facts, Bundesministerium des Innern und für Heimat, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/examples-of-russian-disinformation-and-the-facts.html (dostęp: 23 lutego 2023 r.).

Fryc M., *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, „Bezpieczeństwo Narodowe" 2015, nr 33.

Fryc M., *Sztuka zwyciężania. Strategia tworzenia i wykorzystania asymetrycznej przewagi*, Zona Zero, Warszawa 2020.

Gorynia M. (red.), *Świat w obliczu pandemii*, CeDeWu, Warszawa 2021.

Jarnicki D., *Rosyjska wizja współczesnej globalnej architektury bezpieczeństwa*, Uniwersytet w Siedlcach, Siedlce 2023.

Joniak J., Polak A., *Wojny w Zatoce Perskiej: aspekty operacyjne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2011.

Karnaukh A., Świadomość narodowa w zmieniającym się społeczeństwie ukraińskim na przykładzie Ukraińców, Rosjan i Bułgarów na Zaporożu, „Kultura i społeczeństwo" 2015, nr 2.

Kasianenko K., *Learning from Russian Propaganda and Disinformation in Ukraine,* Australian Institute of International Affairs, 6 marca 2024 r., https://www.internationalaffairs.org.au/australianoutlook/learning-from-russian-propaganda-and-disinformation-in-ukraine/ (dostęp: 29 stycznia 2024 r.).

Kazanecki W., *Porozumienie niemal 30 państw. Przekażą broń Ukrainie*, Interia.pl, 26 lutego 2022 r., https://wydarzenia.interia.pl/raporty/raport-ukraina-rosja/aktualnosci/news-porozumienie-niemal-30-panstw-przekaza-bron-ukrainie,nId,5857148#utm_source=paste&utm_medium=paste&utm_campaign=firefox (dostęp: 23 lutego 2024 r.).

Kirby P., *Donbas: Why Russia is trying to capture eastern Ukraine*, BBC News, 26 maja 2022 r., https://www.bbc.com/news/world-europe-60938544 (dostęp: 11 stycznia 2024 r.).

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

Ławrow: wojskowe manewry rosyjsko-białoruskie zakończą się zgodnie z planem, „Rzeczpospolita", 17 lutego 2022 r., https://www.rp.pl/dyplo

macja/art35700521-lawrow-wojskowe-manewry-rosyjsko-bialoruskie--zakoncza-sie-zgodnie-z-planem (dostęp: 23 lutego 2024 r.).

Marek M., *Operacja Ukraina. Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013-2019*, Wydawnictwo Difin, Warszawa 2020.

Markiewicz S. (red.), *Rosyjska wizja prowadzenia operacji militarnych*, Akademia Sztuki Wojennej, Warszawa 2018.

Markiewicz S. (red.), *Scenariusz przebiegu konfliktu hybrydowego*, Akademia Sztuki Wojennej, Warszawa 2019.

Marszycki M., *Na rynku pracy nadal brakuje specjalistów IT*, ITwiz, 12 lutego 2024 r., https://itwiz.pl/na-rynku-pracy-nadal-brakuje-specjalistow-it/ (dostęp: 12 lutego 2024 r.).

Pacek B., *Wojna hybrydowa na Ukrainie*, Oficyna Wydawnicza RYTM, Warszawa 2018.

Paprocki P., *Charakterystyczne cechy działań hybrydowych – analiza porównawcza*, „Przegląd Sił Zbrojnych" 2023, nr 2.

Podmorskie kable uszkodzone. Zagrożenie dla świata finansów, 9 marca 2024 r., https://www.money.pl/gospodarka/podmorskie-kable-uszkodzone-zagrozenie-dla-swiata-finansow-7004055834422048a.html (dostęp: 11 marca 2024 r.).

Putin: Poborowi nie biorą i nie będą brać udziału w operacji specjalnej na Ukrainie, „Rzeczpospolita", 7 marca 2022 r., https://www.rp.pl/polityka/art-35823001-putin-poborowi-nie-biora-i-nie-beda-brac-udzialu-w-operacji-specjalnej-na-ukrainie (dostęp: 11 marca 2024 r.).

Raubo J., *Rosjanie rzucają do boju w wojnie informacyjnej wszystkie narracje*, Defence24, 20 lutego 2022 r., https://defence24.pl/geopolityka/rosjanie--rzucaja-do-boju-wszystkie-mozliwe-narracje-komentarz (dostęp: 22 lutego 2022 r.).

Rosja oskarża Ukrainę o sprowadzanie materiałów do „brudnej bomby". Jest mowa o Polsce, „Rzeczpospolita", 25 czerwca 2024 r., https://www.rp.pl/konflikty-zbrojne/art40701931-rosja-oskarza-ukraine-o-sprowadzanie-materialow-do-brudnej-bomby-jest-mowa-o-polsce (dostęp: 25 czerwca 2024 r.).

Rosja straszy nuklearną triadą, Wirtualny Nowy Przemysł, https://www.wnp.pl/przemysl-obronny/rosja-straszy-nuklearna-triada,807925.html (dostęp: 14 lutego 2024 r.).

Rosyjskie matki uwierzyły w propagandę Putina, Spider's Web, https://spidersweb.pl/rozrywka/2022/03/09/rosyjska-propaganda-ukraina-wojna-wladimir-putin-telewizja-reddit-tiktok (dostęp: 13 lutego 2024 r.).

Russia Crisis Military Assessment: The race to resupply Ukraine, Atlantic Council, 27 kwietnia 2022 r., https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-crisis-military-assessment-the-race-to-resupply-ukraine/ (dostęp: 12 lutego 2024 r.).

Russia's use of disinformation and information manipulation, Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng (dostęp: 23 stycznia 2024 r.).

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wyd. spec.

Szczygielska A., *Konflikt hybrydowy – analiza porównawcza źródeł wiedzy o zjawisku*, „Roczniki Nauk Społecznych" 2023, nr 2.

Wrona A., *Kłamstwa w nagłówkach. Jak Rosja przedstawia inwazję na Ukrainę?*, Onet.pl, 3 marca 2022 r., https://www.onet.pl/informacje/pravdaorgpl/klamstwa-w-naglowkach-jak-rosja-przedstawia-inwazje-na-ukraine/eblnb6g,30bc1058 (dostęp: 11 stycznia 2024 r.).

Wrzosek M. (red.), *Rosyjska dominacja informacyjna. W teorii i praktyce*, Akademia Sztuki Wojennej, Warszawa 2022.

Wrzosek M., *Militarne (nie)bezpieczeństwo Polski po rosyjskiej agresji na Ukrainę (2022)*, Akademia Sztuki Wojennej, Warszawa 2023.

Wrzosek M., *Przyszła wojna wielodomenowa w rosyjskiej myśli wojskowej,* w: Markiewicz S., Materak S. (red.), *Organizacja systemu rozpoznania zagrożeń państwa – zagrożenia militarne w wielodomenowych operacjach w przyszłych konfliktach zbrojnych*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

Wrzosek M., *Rosyjska wojskowa operacja specjalna – polityczno-militarne przyczyny porażki*, „Przegląd Sił Zbrojnych" 2023, nr 2.

Wrzosek M., Markiewicz S., Modrzejewski Z. (red.), *Informacyjny wymiar wojny hybrydowej*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2019.

DOI:10.59800/bn/196691

Paweł Pelc[1]
Akademickie Centrum Polityki Cyberbezpieczeństwa, Akademia Sztuki Wojennej, Polska

CYBERPRZESTRZEŃ JAKO ELEMENT WALKI INFORMACYJNEJ – DOŚWIADCZENIA Z KONFLIKTU W UKRAINIE

CYBERSPACE AS AN ELEMENT OF INFORMATION WARFARE – EXPERIENCE FROM THE CONFLICT IN UKRAINE

Abstrakt: Rosyjska agresja na Ukrainę od 2014 r. przechodziła różne fazy. Istotnym elementem działań Federacji Rosyjskiej zarówno w fazach konfliktu hybrydowego, jak i konfliktu kinetycznego była wojna informacyjna prowadzona w stosunku do ludności ukraińskiej oraz mieszkańców państw trzecich, niezaangażowanych bezpośrednio w konflikt. W tych działaniach wykorzystywane są nowe technologie, takie jak sztuczna inteligencja i deepfake czy sieci społecznościowe, ale też bardziej tradycyjne ataki przy użyciu narzędzi hakerskich, służących uzyskaniu dostępu do sieci i poszczególnych komputerów.

Słowa kluczowe: wojna informacyjna, cyberprzestrzeń, dezinformacja, media społecznościowe, deepfake

Abstract: Russian aggression against Ukraine has gone through various phases since 2014. However, in both the hybrid conflict and kinetic conflict phases, an important element of the Russian Federation's actions has been information warfare conducted against both the Ukrainian population and residents of third party countries not directly involved in the conflict. These operations use both new technologies, such as artificial intelligence and deepfake or social networks, but also more traditional

[1] 0000-0002-5007-568X, pawel.pelc@gmail.com

attacks using various types of hacking tools designed to gain access to networks and individual computers.

Keywords: information warfare, cyberspace, disinformation, social media, deepfake

Wstęp

Konflikt w Ukrainie rozpoczął się w 2014 r. od rosyjskiej aneksji Krymu, poprzedzonej zajęciem go przez jednostki pozbawione oznaczeń państwowych, a następnie od ataku w Donbasie, przypisywanego pierwotnie przez stronę rosyjską lokalnym separatystom. W wyniku tzw. porozumień mińskich doszło w znacznym stopniu do zamrożenia konfliktu i lokalizacji, jeśli chodzi o działania kinetyczne. Cały czas, nawet po zamrożeniu, strona rosyjska prowadziła jednak działania o charakterze wojny hybrydowej[2]. Ukraina stała się poligonem rosyjskich działań w cyberprzestrzeni[3], wymierzonych m.in. w jej infrastrukturę energetyczną, kolejową czy medialną[4]. Wirus NotPetya, rozprzestrzeniający się w 2017 r. za pomocą oprogramowania do

[2] E. Jakubiak wskazuje, że pojęcie wojny hybrydowej odnosi się do zaprzeczalnych i tajnych działań wspieranych przez groźbę użycia lub użycie sił konwencjonalnych lub nuklearnych, aby wpływać na politykę wewnętrzną krajów będących jej celem. Według niej wojna hybrydowa jest zbiorem działań wojskowych i niewojskowych o niestandardowej skomplikowanej naturze, a jej sprawca jest trudny do precyzyjnego ustalenia i zmienny w swej naturze. Autorka zwraca także uwagę na to, że działania hybrydowe wykorzystują kombinacje konwencjonalnych i niekonwencjonalnych metod. Por.: E. Jakubiak, *Hybrid warfare as a new type of armed conflict in the modern world*, „Studia Bezpieczeństwa Narodowego" 2022, zeszyt 24, s. 72, 79–80.

[3] Legalna definicja cyberprzestrzeni jest zawarta w art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz. U. z 2022 r. poz. 2091) i do tej definicji odwołuje się art. 2 pkt 1 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. Dz. U. z 2024 r., poz. 248). Por. także: K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, nr 2, s. 8–12; C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023, s. 27–31.

[4] K. Geers (red.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallin 2015.

rozliczeń podatkowych, przeniósł się z Ukrainy na inne kraje i wyrządził szkody licznym przedsiębiorcom[5]. Związane z tym atakiem spory prawne, dotyczące w szczególności dochodzenia odszkodowań od zakładów ubezpieczeń, toczyły się przez wiele lat[6]. Wraz z działaniami kinetycznymi i w cyberprzestrzeni Federacja Rosyjska podejmowała w tym czasie także aktywne akcje propagandowe w ramach toczonej przez siebie walki informacyjnej. W pełni odzwierciedla to koncepcję prowadzenia działań wojennych przez Federację Rosyjską – zgodnie z nią wojnę ma charakteryzować stosowanie środków informacyjnych i psychologicznych w celu wsparcia działań kinetycznych[7]. Istotnym jej elementem były argumenty historyczne, dotyczące dziedzictwa Rusi Kijowskiej, a także kwestionujące odrębność narodu ukraińskiego i związki Krymu z Ukrainą[8].

Działania informacyjne oraz w cyberprzestrzeni nasiliły się jeszcze na początku 2022 r. – hakerzy Federacji Rosyjskiej zaatakowali nie tylko serwery rządowe, lecz także banki. Elementem wojny informacyjnej stały się setki fałszywych powiadomień o zagrożeniach bombowych, a także fałszywe SMS-y ostrzegające przed rzekomymi awariami bankomatów. Towarzyszyło to koncentracji wojsk rosyjskich wokół granic Ukrainy. Według strony ukraińskiej te działania miały na celu wywołać panikę wśród ludności, doprowadzić do ewentualnego niezadowolenia i potencjalnie prowokowania protestów, co w rezultacie osłabiło ukraińską hrywnę. Aby osłabić nacisk

[5] Merck, FedEx (za pośrednictwem TNT Experss), Saint-Gobain, Maersk, Mondelez, Reckitt, a w Polsce m.in. także Raben i InterCars.

[6] Zob.: P. Słowiński, *NotPetya – analiza z perspektywy kryminalistyki i polskiego prawa karnego*, „Problemy Współczesnej Kryminalistyki" 2021, t. 25, s. 117–142, https://journals.indexcopernicus.com/api/file/viewByFileId/1584929 (dostęp: 20 lutego 2024 r.); A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, "Wired", 22 sierpnia 2018 r., https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp: 20 lutego 2024 r.).

[7] P. Krawczyk, J. Wiśnicki, *Mity i stereotypy narzędziem walki psychologiczno-informacyjnej Rosji w wojnie z Ukrainą*, "Cybersecurity and Law" 2023, nr 2, s. 346–347.

[8] L. Fijałkowska, *Elementy historycznoprawne w antyukraińskiej propagandzie Federacji Rosyjskiej w latach 2013–2022*, „Studia Prawno-Ekonomiczne" 2022, t. CXXIV, s. 9–20, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzo4bQn7qEAxXxQvEDHdMsAI0QFnoECA4QAQ&url=https%3A%2F%2Fbibliotekanauki.pl%2Farticles%2F2140612.pdf&usg=AOvVaw0qz0ouSHiplnM8CCZGsnnf&opi=89978449 (dostęp: 20 lutego 2024 r.).

rosyjskiej propagandy, strona ukraińska zakazała działalności trzech kanałów telewizyjnych kojarzonych z Rosją, oskarżając je o szerzenie rosyjskiej propagandy. Wcześniej – w 2014 r. – wyłączono dostęp do rosyjskiej telewizji państwowej na terenie Ukrainy[9].

Celem niniejszego artykułu jest analiza rosyjskich działań w cyberprzestrzeni i w sferze informacyjnej w trakcie kinetycznej fazy konfliktu. Przedmiotem zainteresowań będą także przeciwdziałania podejmowane przez stronę ukraińską, co doprowadzi do wysnucia wniosków płynących dla Polski z tych doświadczeń.

Kinetyczna faza konfliktu

Do obecnej fazy kinetycznej konfliktu doszło 24 lutego 2022 r., kiedy wojska Federacji Rosyjskiej zaatakowały Ukrainę z terytorium Rosji, Białorusi i okupowanego Krymu. Atak miał swoje uzasadnienie także na polu wojny informacyjnej[10]: „prezydent Rosji Władimir Putin wystąpił z orędziem do narodu, podczas którego ogłosił początek wojskowej operacji specjalnej mającej na celu obronę ludności Donbasu przed «ludobójstwem» oraz «demilitaryzację i denazyfikację Ukrainy»[11]". Jako podstawę dla wszczęcia agresji wskazał prośbę republik separatystycznych o pomoc i wolę obrony ludności, która „od ośmiu

[9] Por.: J. Marson, *Russians Have Already Started Hybrid War With Bomb Threats, Cyberattacks, Ukraine Says*, 13 lutego 2022 r., https://www.wsj.com/articles/russians-have-already-started-hybrid-war-with-bomb-threats-cyberattacks-ukraine-says11644748413?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.); J.K. Melchior, *The Cyberspace Front in the Attacks on Ukraine*, "The Wall Street Journal", 19 lutego 2022 r., s. A15.

[10] M. Pietras określa walkę informacyjną jako charakterystyczny przypadek procesu sterowania społecznego, którego celem jest niszczenie oponenta za pomocą informacji w trzech głównych obszarach: cyberprzestrzeni, infosferze (obejmującej także systemy informacyjne niewchodzące w skład sieci) oraz noosferze – obszarze mentalności nie tylko pojedynczego człowieka, lecz także narodów i grup społecznych. Por.: M. Pietras, *Wojna informacyjna jako współczesne narzędzie działań nieregularnych*, "Cybersecurity and Law" 2022, nr 1, s. 24.

[11] *Przemówienie Prezydenta Federacji Rosyjskiej Władimira Putina do współobywateli*, Ambasada Rosji w Polsce, 3 marca 2022 r., https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/przem_wienie_prezydenta_federacji_rosyjskiej_w_adimira_putina_do_wsp_obywateli_moskwa_24_lutego_2022/ (dostęp: 14 sierpnia 2024 r.).

lat jest ofiarą ludobójstwa ze strony kijowskiego reżimu”[12]. Zapowiedział oddanie pod sąd tych, którzy popełnili „krwawe zbrodnie”, również przeciwko obywatelom Rosji[13]. Rosyjskie działania zbrojne przeciwko Ukrainie konsekwentnie nazywane są przez stronę rosyjską „specjalną operacją wojskową” albo nawet „misją pokojową”[14], która ma na celu rozbrojenie Ukrainy oraz zaprowadzenie porządku w kraju[15].

Uderzenie wojsk Federacji Rosyjskiej zostało poprzedzone atakiem hakerskim na sieć satelitarną VIASAT, z której korzystały też wojska ukraińskie[16]. W późniejszym okresie, już po rosyjskim ataku kinetycznym na terytorium Ukrainy, rosyjscy hakerzy wybierali także na cel innych dostawców Internetu[17] (w tym satelitarną sieć Starlink[18], przy czym do części ataków na infrastrukturę dostawców Internetu wykorzystano najprawdopodobniej udoskonaloną wersję narzędzia użytego wcześniej do ataku na modemy w sieci VIASAT[19]) oraz elementy infrastruktury energetycznej[20] i inne elementy infrastruktury

[12] *ibidem.*

[13] A. Wilk, M. Domańska, *Rosyjski atak na Ukrainę (24 lutego, godz. 9.00)*, Ośrodek Studiów Wschodnich, 24 lutego 2022 r., https://www.osw.waw.pl/pl/publikacje/analizy/2022-02-24/rosyjski-atak-na-ukraine-24-lutego-godz-900 (dostęp: 20 lutego 2024 r.).

[14] M. Zadorożna, *The impact of wartime information strategy on defence capabilities. The case of the Russo-Ukrainian war*, ”Cybersecurity and Law” 2023, nr 2, s. 290–291.

[15] P. Krawczyk, J. Wiśnicki, *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, ”Cybersecurity and Law” 2023, nr 1, s. 199–200.

[16] Zob.: *Case Study. Viasat*, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.); Ch. Vasquez, E. Groll, *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault*, CyberScoop, 10 sierpnia 2023 r., https://cyberscoop.com/viasat-ka-sat-hack-black-hat/ (dostęp: 4 marca 2024 r.).

[17] A. Vicens, *Ukraine's largest mobile communications provider down after apparent cyber attack*, CyberScoop, 12 grudnia 2023 r., https://cyberscoop.com/ukraines-largest-mobile-communications-provider-down-after-apparent-cyber-attack/ (dostęp: 4 marca 2024 r.).

[18] S. Fitzgerald, *Report: Moscow's Starlink Takedown Efforts Advancing*, Newsmax, 19 kwietnia 2023 r., https://www.newsmax.com/newsfront/russia-ukraine-starlink/2023/04/19/id/1116709/?ns_mail_uid=0fcc12bc-c2de-46ff-bed0-afe9362fd63d&ns_mail_job=DM462397_04192023&s=acs&dkt_nbr=0105024swcvf (dostęp: 4 marca 2024 r.).

[19] A. Vincens, *Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs*, CyberScoop, 21 marca 2024 r., https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/ (dostęp: 21 marca 2024 r.).

[20] Por.: R. McMillan, D. Volz, *Internet Provider to Ukrainian Military Hit With Major Cyberattack*, “The Wall Street Journal”, 22 marca 2022 r., https://www.wsj.com/articles/

krytycznej[21]. Przynajmniej część z tych ataków była skorelowana z atakami kinetycznymi[22]. Operacje w cyberprzestrzeni – oprócz tych skierowanych przeciwko elementom infrastruktury krytycznej – służyły pozyskiwaniu informacji, w tym danych osobowych[23], a w szczególności dostępu do systemów wykorzystywanych przez armię ukraińską[24]. Kolejnym obszarem rosyjskich działań w cyberprzestrzeni było wprzęgnięcie ich w rosyjską kampanię dezinformacyjną[25], prowadzoną także przed rozpoczęciem w lutym 2022 r. kinetycznej fazy

internet-provider-to-ukrainian-military-hit-with-major-cyberattack-11648504218?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.); F. Bajak, *Ukraine says potent Russian hack against power grid thwarted*, Associated Press News, 13 kwietnia 2022 r., https://apnews.com/article/russia-ukraine-kyiv-technology-business-hacking-0147e33bc1846a3f8039f9c65a1b4b50?user_email=2f13c3ba3bc1824073117048cd530a2587844ce6575de478221117de2a1545ec (dostęp: 23 listopada 2023 r.).

[21] *The cyber war in Ukraine is as crucial as the battle in the trenches*, The Economist, 20 marca 2024 r., https://www.economist.com/europe/2024/03/20/the-cyber-war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches?utm_content=article-link-4&etear=nl_today_4&utm_campaign=r.the-economist-today&utm_medium=email.internal-newsletter.np&utm_source=salesforce-marketing-cloud&utm_term=3%2F20%2F2024&utm_id=1862034&slug=europe&slug=2024&slug=03&slug=20&slug=the-cyberwar-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches (dostęp: 21 marca 2024 r.).

[22] *Russia seems to be co-ordinating cyber-attacks with its military campaign*, The Economist, https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign?etear=nl_today_7 (dostęp: 4 marca 2024 r.). Do odmiennych wniosków dochodzą autorzy raportu "Center for Strategic and International Studies": G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias, *Cyber Operations during the Risso-Ukrainian War*, lipiec 2023 r., s. 7–8.

[23] Więcej o działaniach podejmowanych przez Federację Rosyjską przed obecną fazą kinetyczną konfliktu: A.E. Levite, *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict*, kwiecień 2023 r., Washington, DC., s. 3–4.

[24] D. Catteler, D. Black, *The Myth of the Missing Cyberwar*, "Foreign Affairs", 6 kwietnia 2022 r., https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar (dostęp: 4 marca 2024 r.).

[25] Zob. więcej na temat traktowania dezinformacji jako aktu agresji oraz prób zdefiniowania pojęcia dezinformacji: K. Chałubińska-Jentkiewicz, *Dezinformacja jako akt agresji w cyberprzestrzeni*, "Cybersecurity and Law" 2021, nr 1, s. 14–19. Por. także: K. Chałubińska-Jentkiewicz, *Disinformation – and what else?*, "Cybersecurity and Law" 2021, nr 2, s. 9–19. Różnice między dezinformacją a propagandą objaśnia M.J. Wachowicz. Por.: M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1–2, s. 239–243. Według jego propozycji dezinformacja to:

• „świadome, umyślne i podstępne wprowadzanie w błąd przeciwnika przez ukrywający rzeczywiste zamierzenia dowolny podmiot państwowy lub pozapaństwowy w przestrzeni fizycznej lub informacyjnej za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanego do podjęcia korzystnych dla dezinformatora decyzji (działań lub zaniechań), zmylenia dezinformowanego, odwrócenia jego uwagi, uzyskania efektu zaskoczenia,

konfliktu, w tym z wykorzystaniem mediów społecznościowych[26, 27]. Na terenach okupowanych przez siły rosyjskie podejmowano także działania, które miały na celu fizyczne odcięcie dostępu do ukraińskiej infrastruktury internetowej i zastąpienie go dostępem do infrastruktury kontrolowanej przez Federację Rosyjską. Ponadto w tych miejscach ukraińskie kanały telewizyjne zostały zastąpione prze rosyjskie, stanowiące element rosyjskiej antyukraińskiej propagandy. Połączone działania w środkach masowego przekazu i w cyberprzestrzeni – z wykorzystaniem mediów społecznościowych – przynosiły w wielu przypadkach skutek oczekiwany przez stronę rosyjską i skutecznie szerzyły jej dezinformację i propagandę[28].

Zgodnie z rosyjską doktryną funkcjonowanie w cyberprzestrzeni stanowi element wojny informacyjnej, w pełni wkomponowany

zniekształcenia realnego obrazu rzeczy i świata, jak również w celu ochrony godziwych i niegodziwych interesów dezinformatora;

• nieświadome i nieumyślne wprowadzanie w błąd przełożonych, sojuszników, podwładnych bądź otoczenia, współdziałających w dowolnej strukturze społecznej, przez mylne interpretowanie rozkazów, zarządzeń lub innej informacji taktyczno-operacyjnej, bądź pominięcie istotnych wskazówek (wytycznych) wykonawczych, niekiedy niepodanie we właściwym czasie potrzebnej informacji, używanie wieloznacznych bądź niezrozumiałych pojęć;

• świadome, umyślne i najczęściej podstępne wprowadzanie w błąd przełożonych, sojuszników, podwładnych bądź otoczenia, współdziałających w dowolnej strukturze społecznej oraz w przestrzeni fizycznej lub informacyjnej, przez ukrywający rzeczywiste zamierzenia dowolny podmiot, za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanych do podjęcia korzystnych dla dezinformatora (ale niekiedy również dla dezinformowanego) decyzji – działań lub zaniechań: konstruktywnych bądź destruktywnych".

[26] P. Krawczyk, J. Wiśnicki, *Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine*, "Cybersecurity and Law" 2022, nr 2, s. 278–286. Por. także: P. Staniurski, *Trolling, fake news, infotainment. Rola mediów społecznościowych w prowadzeniu wojny informacyjnej na przykładzie działań podejmowanych w tym obszarze przez Federację Rosyjską,* w: D. Boćkowski, E. Dąbrowska-Prokopowska, P. Goryń, K. Gorynia (red.), *Dezinformacja – Inspiracja – Społeczeństwo, Social Cybersecurity*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2022, s. 51–62.

[27] T. Riley, *Russia's information war against Ukraine went stealth after Meta crackdown*, CyberScoop, 23 lutego 2022 r., https://cyberscoop.com/russias-information-war-ukraine-meta/ (dostęp: 4 marca 2024 r.).

[28] C. Gall, O. Chubko, D. Shapoval, *'Our Own Guys Are Shelling Us': How Russian Propaganda Plagues Ukraine*, 19 kwietnia 2023 r., https://www.nytimes.com/2023/04/19/world/europe/ukraine-russia-donbas-ropaganda.html?campaign_id=57&emc=edit_ne_20230419&instance_id=90593&nl=evening-briefing&regi_id=73957933&segment_id=130849&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c (dostęp: 4 marca 2024 r.).

w inne działania propagandowe prowadzone przez Federację Rosyjską. W tym kontekście działaniom w cyberprzestrzeni przypisuje się rolę zakłócenia i przejęcia wrogich kanałów komunikacyjnych i zastąpienia ich własnym przekazem propagandowym[29]. Tego typu aktami były np. próby wykorzystania technologii deepfake[30] ze spreparowanym oświadczeniem ukraińskiego prezydenta Zełenskiego o kapitulacji sił ukraińskich i rozpowszechnienia go za pośrednictwem przejętych wcześniej kanałów komunikacji[31]. Te działania ograniczają się nie tylko do operacji na terenie Ukrainy, lecz także skierowane są do mieszkańców innych państw[32]. W swoich działaniach dezinformacyjnych skierowanych przeciwko Ukrainie i państwom jej sprzyjającym Rosja wykorzystuje także narzędzia oparte o sztuczną inteligencję, m.in. do tworzenia kolejnych deepfake'ów[33].

Z dostępnych danych i analiz wynika, że Federacja Rosyjska wykorzystuje cyberprzestrzeń w powiązaniu z innymi działaniami. Korzysta z niej w ramach ataków na infrastrukturę lub przeciwko

[29] A.E. Levite, *Integrating…*, *op. cit.*, s. 13–14.

[30] K. Basaj wskazuje, że „deepfake jest nową techniką manipulacji pozwalającą zamienić w jednym filmie dwie tożsamości. W szerszej definicji są to treści zsyntetyzowane przez sztuczną inteligencję. Próbki spreparowanych filmów z synchronizacją ust są modyfikowane tak, aby ruchy ust były zgodne z dźwiękiem". Zob.: K. Basaj, *Czym jest deepfake?*, „Biuletyn ACKS" 2021, wydanie specjalne nr 2, s. 3.

[31] Por.: M. Chwistek, *Do sieci trafił deepfake z prezydentem Zełeńskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17 marca 2022 r., https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 (dostęp: 4 marca 2024 r.); S. Gatlan, *Facebook removes deepfake of Ukrainian President Zelensky*, BleepingComputer, 16 marca 2022 r., https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/?mod=djemCybersecruityPro&tpl=cy (dostęp: 7 marca 2024 r.).

[32] R. McMillan, D. Volz, *Actors Recorded Videos for 'Vladimir.' It Turned Into Russian Propaganda*, "The Wall Street Journal", 1 grudnia 2023 r., https://www.wsj.com/tech/cybersecurity/actors-recorded-videos-for-vladimir-it-turned-into-russian-propaganda-7ff2ce8e (dostęp: 4 marca 2024 r.); M. Pomerleau, *Congress wants DOD to study information operations from Russia-Ukraine war*, DefenseScoop, 8 grudnia 2023 r., https://defensescoop.com/2023/12/08/congress-wants-dod-to-study-information-operations-from-russia-ukraine-war/ (dostęp: 4 marca 2024 r.).

[33] S.J. Freedberg Jr., *Brute force: Russia 'doubled down' on often-crude disinformation in 2023, says report*, Breaking Defense, 29 lutego 2024 r., https://breakingdefense.com/2024/02/brute-force-russia-doubled-down-on-often-crude-disinformation-in-2023-says-report/?utm_medium=email&_hsmi=296653794&_hsenc=p2ANqtz-8PNT86_y7kRH5VFfL_R3WIPbHnxphnUHLZ4WW8fGAuSwxWeW1n5l9btBC6KICBaxSq1HnpX4E1lcXf-L188poArC (dostęp: 6 marca 2024 r.).

operacjom militarnym prowadzonym przez stronę ukraińską, podczas akcji o charakterze szpiegowskim[34], ale także jako uzupełnienie działań dezinformacyjnych[35] zarówno w stosunku do społeczeństwa ukraińskiego, jak i mieszkańców państw trzecich – tych wspierających strony konfliktu oraz tych starających się zachować neutralność[36]. W tych działaniach wykorzystywane są zarówno nowe technologie, takie jak sztuczna inteligencja i deepfake czy sieci społecznościowe, jak i bardziej tradycyjne ataki z wykorzystaniem różnego rodzaju narzędzi hakerskich, służących uzyskaniu dostępu do sieci i poszczególnych komputerów. Jednocześnie propaganda rosyjska stara się wykorzystać dominację lewicowej poprawności politycznej w mediach społecznościowych tzw. głównego nurtu i rozprzestrzeniać swoje stanowisko w nieufnych wobec nich portalach przywiązanych do wolności słowa i tworzonych w opozycji do serwisów związanych z Big Tech[37]. Do szczególnie spektakularnych działań skierowanych m.in. do obiorcy nieufnego w stosunku do tzw. głównego nurtu można zaliczyć wywiad udzielony przez prezydenta Putina byłemu popularnemu prezenterowi prawicowej telewizji Fox News[38].

[34] D. Dziwisz, B. Sajduk, *Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej"*, w: A. Gruszczak (red.), *The War must go on. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, 24 lutego 2023 r., s. 43–52.

[35] *The fight against pro-Kremlin disinformation*, The European Council, 20 stycznia 2023 r., https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/ (dostęp: 6 marca 2024 r.).

[36] *Undermining Ukraine: How Russia widened its global information war in 2023*, Digital Forensic Research Lab, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/ (dostęp: 6 marca 2024 r.).

[37] Por.: K. Collier, *Blacklisted Russian propagandists thrive on right-wing apps Gab and Truth Social*, NBC News, 13 grudnia 2022 r., https://www.nbcnews.com/tech/internet/russias-ira-thriving-right-wing-apps-gab-truth-social-study-finds-rcna61449 (dostęp: 6 marca 2024 r.); S. Smalley, *Russian disinformation rampant on far-right social media platforms*, CyberScoop, 13 grudnia 2023 r., https://cyberscoop.com/russia-disinformation-gab-parler/ (dostęp: 6 marca 2024 r.).

[38] *Interview to Tucker Carlson*, Official Internet Resources of the President of Russia, 9 lutego 2024 r., http://en.kremlin.ru/events/president/news/73411 (dostęp: 6 marca 2024 r.). Por. także: T. Stanovaya, *Why Putin's Interview With Tucker Carlson Didn't Go to Plan*, 12 lutego 2024 r., https://carnegieendowment.org/politika/91614 (dostęp: 6 marca 2024 r.); D. Wroe, *Tucker Carlson, Vladimir Putin and the pernicious myth of the free market of ideas*, ASPI Strategist, 28 lutego 2024 r., https://www.aspistrategist.org.au/

Efekty synergii działań dezinformacyjnych z wykorzystaniem mediów społecznościowych i tradycyjnych były wykorzystywane przez Federację Rosyjską już przed wybuchem obecnej fazy kinetycznej agresji przeciwko Ukrainie[39]. Po jej wybuchu rządy państw zachodnich podjęły próbę ograniczenia wpływu rosyjskiej propagandy na swoje społeczeństwa, np. poprzez blokowanie dostępu do ich kanałów dezinformacyjnych. Sprowokowało to zarzuty o wprowadzanie cenzury i zamach na wolność słowa, jednak nie zahamowało działań rosyjskich z wykorzystaniem mediów społecznościowych lub w krajach trzecich, które nie ograniczyły dostępu do rosyjskich kanałów propagandowo-informacyjnych.

Gdy państwa zachodnie dążyły do osłabienia skuteczności rosyjskich działań propagandowych, podjęły jeszcze przed wybuchem obecnej kinetycznej fazy konfliktu bezprecedensowe decyzje o szybkim odtajnieniu informacji o rosyjskich cyberoperacjach przeciwko Ukrainie[40], a także wsparły działania ukraińskie w sferze cyberbezpieczeństwa.

Podsumowanie

Wojna w Ukrainie, która rozpoczęła się w 2014 r. od działań hybrydowych (w związku z zajęciem Krymu przez tzw. „zielone ludziki"), przeszła przez ograniczoną fazę kinetyczną (działania w Donbasie), ponowne działania o charakterze hybrydowym, by od 24 lutego 2022 r. wejść jeszcze raz w intensywną fazę kinetyczną. Elementem działań rosyjskich we wszystkich fazach tej wojny jest aktywnie prowadzona wojna informacyjna, w tym z wykorzystaniem

tucker-carlson-vladimir-putin-and-the-pernicious-myth-of-the-free-market-of-ideas/ (dostęp: 6 marca 2024 r.).

[39] *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, United States Department of State Global Engagement Center, sierpień 2020 r., https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf (dostęp: 6 marca 2024 r.).

[40] Ch. Vasquez, *Ukraine information sharing a model for countering China, top cyber official says*, CyberScoop, 12 czerwca 2023 r., https://cyberscoop.com/information-sharing-china-threat/ (dostęp: 7 marca 2024 r.).

cyberprzestrzeni[41], trwająca zarówno w fazie działań hybrydowych, jak i działań kinetycznych (bez względu na ich skalę). Istotne elementy narracji rosyjskiej to w szczególności kwestionowanie odrębności narodu ukraińskiego, w tym także jego odrębności religijnej (stąd wspieranie działań patriarchatu moskiewskiego przez Federację Rosyjską i jej propagandę[42]), kwestionowanie samodzielności władz ukraińskich, oskarżanie ich o nazistowski charakter, a także o walkę z własnym społeczeństwem. Federacja Rosyjska wykorzystuje też mechanizmy „demokratyczne", takie jak referenda czy wybory, aby w ten sposób legitymizować aneksję części terytoriów ukraińskich.

Celem działań w sferze informacyjnej jest budowanie obrazu zgodnego z narracją promowaną przez Federację Rosyjską oraz dążenie do dezintegracji zarówno społeczeństwa ukraińskiego, jak i wsparcia innych społeczeństw i państw dla Ukrainy[43]. Elementem tych operacji dezinformacyjnych (m.in. z wykorzystaniem fake newsów[44]) jest kompromitacja wizerunku Ukraińców, dezawuacja, a także dyskredytacja i delegitymizacja Ukrainy oraz kwestionowanie jej samodzielności i podkreślanie zależności od państw Zachodu,

[41] G. Wilde, *Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected*, Carnegie Endowment for International Peace, 11 marca 2024 r., https://carnegieendowment.org/2024/03/11/why-cyber-attacks-on-ukrainians-aren-t-working-way-russia-expected-pub-91931?utm_source=ctw&utm_medium=email&utm_campaign=buttonlink&mkt_tok=ODEzLVhZVS00MjIAAAGR3g8_OEaIEaMgnTOIVwcnOaymL8UiszkrN_U8H66y-4zHZauBTuMIraa7isTbjZ3jY_35LsDa1e76YwBRcjyaYvUSv5_3PaU2tuVGjqR6rAg (dostęp: 15 marca 2024 r.).

[42] Por.: N. Dubtsova, *From pulpit to propaganda machine: tracing the Russian Orthodox Church's role in Putin's war*, Reuters Institute, 6 lutego 2024 r., https://reutersinstitute.politics.ox.ac.uk/pulpit-propaganda-machine-tracing-russian-orthodox-churchs-role-putins-war (dostęp: 15 marca 2024 r.); J.K. Melchior, *Is Religious Liberty 'Under Attack' in Ukraine?*, "The Wall Street Journal", 2 marca 2024 r., https://www.wsj.com/articles/is-religious-liberty-under-attack-in-ukraine-russia-war-82b1f198 (dostęp: 23 marca 2024 r.).

[43] Por. *Ukraina 2022, Część I. 10 miesięcy rosyjskiej propagandy. Luty – Grudzień 2022*, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Ośrodek Studiów Przestrzeni Postsowieckiej; *Percepcja rosyjskiej agresji na Ukrainę w wybranych krajach*, kwiecień 2022 r., Ośrodek Studiów Przestrzeni Postsowieckiej; *Metody, narzędzia i kanały rosyjskiej walki informacyjnej w Europie, krajach postsowieckich i Turcji*, sierpień 2022 r., Ośrodek Studiów Przestrzeni Postsowieckiej; D. Gąsiewski, M. Bućka, *Wojna informacyjna Rosji z Ukrainą*, „Biuletyn" 2022, nr 2, Akademickie Centrum Komunikacji Strategicznej.

[44] K. Bąkowicz wskazuje, że fake news „oznacza wiadomość medialną, która jednocześnie nie jest ani prawdą, ani kłamstwem, opiera się na dezinformacji, często zawierając fragmenty prawdziwe". Zob.: K. Bąkowicz, *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, „Studia Medioznawcze" 2019, nr 3, s. 281.

w szczególności USA i innych krajów NATO[45]. Cyberprzestrzeń służy do pozyskiwania i udostępniania z wykorzystaniem narzędzi hakerskich wykradzionych prywatnych informacji, falsyfikowania pochodzenia danych informacji, m.in. dzięki fabrykowaniu portali informacyjnych, fałszowaniu źródeł (z wykorzystaniem technologii deepfake), a także do przejmowania witryn internetowych w celu wykorzystania ich jako źródeł działań dezinformacyjnych[46]. Tym samym cyberprzestrzeń staje się elementem tzw. wojny hybrydowej lub działań nieregularnych, wykracza bowiem poza sferę konfliktu kinetycznego i nie ogranicza się wyłącznie do terytorium Ukrainy i jej mieszkańców[47]. Strona ukraińska konsekwentnie próbuje temu przeciwdziałać m.in. przy wykorzystaniu stworzonych przez siebie odpowiednich struktur organizacyjnych[48].

Z przebiegu tego konfliktu można wyciągnąć szereg wniosków dotyczących zarówno operacji w cyberprzestrzeni, jak i działań w ramach wojny informacyjnej. Rosyjskie próby korzystania z technologii deepfake wskazują na istotną potrzebę budowania mechanizmów pozwalających na ich wykrywanie i odpowiednie oznaczanie oraz oddzielanie ich od informacji. Ukraińskie działania informacyjne z wykorzystaniem memów[49], które zapadają łatwo w pamięć, wskazują, jak prosty przekaz może być wykorzystany do podnoszenia morale własnego społeczeństwa oraz propagowania swojego stanowiska także w innych krajach. Działania informacyjno-propagandowe wykroczyły znacząco poza sferę środków masowej komunikacji i w dużym stopniu przeniosły się do mediów społecznościowych

[45] Ł. Małecki, *Fake news jako front wojny w Ukrainie*, „Studia Ukrainica Posnaniensia" 2023, nr 2, s. 57–70.

[46] S.L. Myers, *Spate of Mock News Sites With Russian Ties Pop Up in U.S.*, "The New York Times", 7 marca 2024 r., https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html?te=1&nl=the-evening&emc=edit_ne_20240307 (dostęp: 14 marca 2024 r.).

[47] Por.: K. Chałubińska-Jentkiewicz, *Dezinformacja …*, *op. cit.*, s. 9–24; M. Pietras, *Wojna informacyjna…*, *op. cit.*, s. 21–41.

[48] M. Zadorożna, *The impact…*, *op. cit.*, s. 290–292.

[49] Mem według definicji słownikowej to „chwytliwa porcja informacji rozpowszechniana w Internecie w formie krótkiego filmu, obrazka lub zdjęcia opatrzonego jakimś tekstem". Zob.: *mem*, w: S. Dubisz, *Wielki Słownik Języka Polskiego PWN*, Warszawa 2018, s. 840.

i cyberprzestrzeni. Często widać było także koordynację działań w środkach masowej komunikacji i cyberprzestrzeni w celu wprowadzania określonych treści do szerszego obiegu. Jednocześnie próby blokowania kanałów szerzących propagandę Federacji Rosyjskiej skutkowały zarzutami o cenzurę i propagowanie tych treści przez obrońców wolności słowa.

Istotnym elementem rosyjskiej propagandy jest oskarżanie strony ukraińskiej o nazizm oraz antysemityzm i to w kontekście żydowskich korzeni prezydenta Ukrainy. W przypadku ataku na Polskę Federacja Rosyjska najprawdopodobniej także chętnie skorzysta z podobnej narracji jako narzędzia do łamania woli oporu społeczeństwa i uzupełni ją zarzutami np. o rasizm (Polacy przyjmowali Ukraińców, a odmawiają przyjmowania osób z innych regionów świata dostarczanych na granicę przez służby białoruskie od 2021 r.), prześladowanie mniejszości narodowych lub religijnych, brak zdolności państwotwórczych, rusofobię, antyniemieckość, antyunijność i niepraworządność. Polska powinna być w pełni przygotowana do przeciwdziałania tego typu argumentom m.in. za pomocą efektywnych mechanizmów weryfikacji informacji, pojawiających się w sieciach społecznościowych i w przekazie medialnym, niekojarzących się jednak z lewicową cenzurą konserwatywnego przekazu.

Działania w cyberprzestrzeni i przestrzeni mediów społecznościowych oraz mass mediów będą traktowane przez Federację Rosyjską jako wsparcie i uzupełnienie działań kinetycznych. Podczas przygotowań do takiej ewentualnej agresji poza rozbudową obronnego potencjału kinetycznego niezbędne jest powiązane z nią budowanie zdolności do działań w cyberprzestrzeni (w tym do obrony elementów infrastruktury krytycznej przed potencjalnymi cyberatakami). Biorąc pod uwagę doświadczenia ukraińskie, ważnymi krokami są zapewnienie szerokiej koordynacji przygotowań militarnych i cywilnych oraz współpraca administracji publicznej i innych podmiotów z Wojskami Obrony Cyberprzestrzeni. Ich uprawnienia do prowadzenia aktywnych działań powinny być zapewnione również w momencie, w którym nie występują działania o charakterze kinetycznym, a zatem poza okresem klasycznego konfliktu zbrojnego.

Doświadczenie ukraińskie pokazuje także istotną wagę współpracy sojuszniczej w sferze cyberprzestrzeni, publikowania informacji wywiadowczych o planowanych działaniach rosyjskich w sferze cyberataków lub wojny informacyjnej czy szybkiej atrybucji rosyjskich cyberataków, tak by usunąć charakterystyczny dla działań hybrydowych element zaprzeczalności.

Jednocześnie należy być przygotowanym na rosyjskie operacje hybrydowe skierowane przeciw państwom i społeczeństwom niebędącym bezpośrednio przedmiotem działań kinetycznych i być w stanie im zapobiegać. Działania Federacji Rosyjskiej zarówno w fazie kinetycznej konfliktu, jak i ją poprzedzające powinny zatem interesować zagrożone państwa. Należy mieć świadomość, że już obecnie Polska jest przedmiotem działań hybrydowych skierowanych przeciwko niej (np. kryzys migracyjny na granicy z Białorusią, cyberataki na elementy infrastruktury krytycznej czy działania dezinformacyjne). Ułatwia to budowę mechanizmów zwiększających odporność na działania hybrydowe, dlatego obecny czas powinien zostać w tym celu jak najlepiej wykorzystany.

Konflikt w Ukrainie ma charakter przewlekły i obecnie nie widać scenariusza wróżącego jego szybkie zakończenie. Wszystko wskazuje na to, że w najbliższej przyszłości działania kinetyczne będą nadal uzupełniane działaniami o charakterze hybrydowym – także z wykorzystaniem cyberprzestrzeni, mediów społecznościowych i środków masowego przekazu w celu osłabienia pomocy Ukrainie przez państwa zachodnie, wsparcia Rosji ze strony państw spoza europejskiego kręgu kulturowego, a także dezintegracji społeczeństwa ukraińskiego i osłabiania jego woli oporu.

Bibliografia
References List

Bajak F., *Ukraine says potent Russian hack against power grid thwarted*, Associated Press News, 13 kwietnia 2022 r., https://apnews.com/article/russia-ukraine-kyiv-technology-business-hacking-0147e33bc1846a3f8039f9c65a1b4b50?user_email=2f13c3ba3bc1824073117048cd530a2587844ce6575de478221117de2a1545ec (dostęp: 23 listopada 2023 r.).

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023.

Basaj K., *Czym jest deepfake?*, „Biuletyn ACKS" 2021, wydanie specjalne nr 2.

Bąkowicz K., *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, „Studia Medioznawcze" 2019, nr 3.

Case Study. Viasat, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.).

Catteler D., Black D., *The Myth of the Missing Cyberwar,* "Foreign Affairs", 6 kwietnia 2022 r., https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberw (dostęp: 31 lipca 2024 r.).

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, nr 2.

Chałubińska-Jentkiewicz K., *Dezinformacja jako akt agresji w cyberprzestrzeni*, "Cybersecurity and Law" 2021, nr 1.

Chałubińska-Jentkiewicz K., *Disinformation – and what else?*, "Cybersecurity and Law" 2021, nr 2.

Chwistek M., *Do sieci trafił deepfake z prezydentem Zełeńskim. W fałszywym wideo „namawiał" do poddania Ukrainy*, Komputer Świat, 17 marca 2022 r., https://www.komputerswiat.pl/aktualnosci/wydarzenia/do-sieci-trafil-deepfake-z-prezydentem-zelenskim-w-falszywym-wideo-namawial-do/n40qel7 (dostęp: 4 marca 2024 r.).

Collier K., *Blacklisted Russian propagandists thrive on right-wing apps Gab and Truth Social*, NBC News, 13 grudnia 2022 r., https://www.nbcnews.com/tech/internet/russias-ira-thriving-right-wing-apps-gab-truth-social-study-finds-rcna61449 (dostęp: 6 marca 2024 r.).

Case Study. Viasat, Cyber Peace Institute, czerwiec 2022 r., https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (dostęp: 20 lutego 2024 r.).

Dubtsova N., *From pulpit to propaganda machine: tracing the Russian Orthodox Church's role in Putin's war*, Reuters Institute, 6 lutego 2024 r., https://reutersinstitute.politics.ox.ac.uk/pulpit-propaganda-machine-tracing-russian-orthodox-churchs-role-putins-war (dostęp: 15 marca 2024 r.).

Dziwisz D., Sajduk B., *Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej"*, w: A. Gruszczak (red.), *The War must go on. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*, 24 lutego 2023 r.

Fijałkowska L., *Elementy historycznoprawne w antyukraińskiej propagandzie Federacji Rosyjskiej w latach 2013–2022*, „Studia Prawno-Ekonomiczne" 2022, t. CXXIV, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzo4bQn7qEAxXxQvEDHdMsAI0QFnoECA4QAQ&url=https%3A%2F%2Fbibliotekanauki.pl%2Farticles%2F2140612.pdf&usg=AOvVaw0qz0ouSHiplnM8CCZGsnnf&opi=89978449 (dostęp: 20 lutego 2024 r.).

Fitzgerald S., *Report: Moscow's Starlink Takedown Efforts Advancing*, Newsmax, 19 kwietnia 2023 r., https://www.newsmax.com/newsfront/russia-ukraine-starlink/2023/04/19/id/1116709/?ns_mail_uid=0fcc12bc-c2de-46ff-bed0-afe9362fd63d&ns_mail_job=DM462397_04192023&s=acs&dkt_nbr=0105024swcvf (dostęp: 4 marca 2024 r.).

Freedberg Jr. S.J., *Brute force: Russia 'doubled down' on often-crude disinformation in 2023, says report*, Breaking Defense, 29 lutego 2024 r., https://breakingdefense.com/2024/02/brute-force-russia-doubled-down-on-often-crude-disinformation-in-2023-says-report/?utm_medium=email&_hsmi=296653794&_hsenc=p2ANqtz-8PNT86_y7kRH5VFfL_R3WIPbHnxphnUHLZ4WW8fGAuSwxWeW1n5l9btBC6KICBaxSq1HnpX4E1lcXf-L188poArC (dostęp: 6 marca 2024 r.).

Gall C., Chubko O., Shapoval D., *'Our Own Guys Are Shelling Us': How Russian Propaganda Plagues Ukraine*, "The New York Times", 19 kwietnia 2023 r., https://www.nytimes.com/2023/04/19/world/europe/ukrai

ne-russia-donbas-ropaganda.html?campaign_id=57&emc=edit_ne_20230419&instance_id=90593&nl=evening-briefing&regi_id=73957933&segment_id=130849&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c (dostęp: 4 marca 2024 r.).

Gatlan S., *Facebook removes deepfake of Ukrainian President Zelensky*, BleepingComputer, 16 marca 2022 r., https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/?mod=djemCybersecruityPro&tpl=cy (dostęp: 7 marca 2024 r.).

Gąsiewski D., Bućka M., *Wojna informacyjna Rosji z Ukrainą*, „Biuletyn" 2022, nr 2, Akademickie Centrum Komunikacji Strategicznej.

GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem, United States Department of State Global Engagement Center, sierpień 2020 r., https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf (dostęp: 6 marca 2024 r.).

Geers K. (red.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallin 2015.

Greenberg T.A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, "Wired", 22 sierpnia 2018 r., https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (dostęp: 20 lutego 2024 r.)

Interview to Tucker Carlson, Official Internet Resources of the President of Russia, 9 lutego 2024 r., http://en.kremlin.ru/events/president/news/73411 (dostęp: 6 marca 2024 r.).

Jakubiak E., *Hybrid warfare as a new type of armed conflict in the modern world*, „Studia Bezpieczeństwa Narodowego" 2022, zeszyt 24.

Krawczyk P., Wiśnicki J., *Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine*, "Cybersecurity and Law" 2022, nr 2.

Krawczyk P., Wiśnicki J., *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, "Cybersecurity and Law" 2023, nr 1.

Krawczyk P., Wiśnicki J., *Mity i stereotypy narzędziem walki psychologiczno-informacyjnej Rosji w wojnie z Ukrainą*, "Cybersecurity and Law" 2023, nr 2.

Levite A.E., *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict,* kwiecień 2023 r., Washington, DC.

Małecki Ł., *Fake news jako front wojny w Ukrainie*, „Studia Ukrainica Posnaniensia" 2023, nr 2.

Marson J., *Russians Have Already Started Hybrid War With Bomb Threats, Cyberattacks, Ukraine Says,* "The Wall Street Journal", 13 lutego 2022 r., https://www.wsj.com/articles/russians-have-already-started-hybrid-war-with-bomb-threats-cyberattacks-ukraine-says-11644748413?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.).

McMillan R., Volz D., *Internet Provider to Ukrainian Military Hit With Major Cyberattack*, "The Wall Street Journal", 22 marca 2022 r., https://www.wsj.com/articles/internet-provider-to-ukrainian-military-hit-with-major-cyberattack-11648504218?mod=djemCybersecruityPro&tpl=cy (dostęp: 20 lutego 2024 r.).

McMillan R., Volz D., *Actors Recorded Videos for 'Vladimir.' It Turned Into Russian Propaganda,* "The Wall Street Journal", 1 grudnia 2023 r., https://www.wsj.com/tech/cybersecurity/actors-recorded-videos-for-vladimir-it-turned-into-russian-propaganda-7ff2ce8e (dostęp: 4 marca 2024 r.).

Melchior J.K., *Is Religious Liberty 'Under Attack' in Ukraine?*, "The Wall Street Journal", 22 marca 2024 r., https://www.wsj.com/articles/is-religious-liberty-under-attack-in-ukraine-russia-war-82b1f198 (dostęp: 23 marca 2024 r.).

Melchior J.K., *The Cyberspace Front in the Attacks on Ukraine,* "The Wall Street Journal", 19 lutego 2022 r.

Mem, w: Dubisz S., *Wielki Słownik Języka Polskiego PWN*, Warszawa 2018.

Metody, narzędzia i kanały rosyjskiej walki informacyjnej w Europie, krajach postsowieckich i Turcji, Ośrodek Studiów Przestrzeni Postsowieckiej, sierpień 2022 r.

Mueller G.B., Jensen B., Valeriano B., Maness R.C., Macias J.M., *Cyber Operations during the Risso-Ukrainian War,* lipiec 2023 r.

Myers S.L., *Spate of Mock News Sites With Russian Ties Pop Up in U.S.*, "The New York Times", 7 marca 2024 r., https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html?te=1&nl=the-evening&emc=edit_ne_20240307 (dostęp: 14 marca 2024 r.).

Percepcja rosyjskiej agresji na Ukrainę w wybranych krajach, Ośrodek Studiów Przestrzeni Postsowieckiej, kwiecień 2022 r.

Pietras M., *Wojna informacyjna jako współczesne narzędzie działań nieregularnyc*h, "Cybersecurity and Law" 2022, nr 1.

Pomerleau M., *Congress wants DOD to study information operations from Russia-Ukraine war*, DefenseScoop, 8 grudnia 2023 r., https://defensescoop.com/2023/12/08/congress-wants-dod-to-study-information-operations-from-russia-ukraine-war/ (dostęp: 4 marca 2024 r.)

Przemówienie Prezydenta Federacji Rosyjskiej Władimira Putina do współobywateli, Ambasada Rosji w Polsce, 3 marca 2022 r., https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/przem_wienie_prezydenta_federacji_rosyjskiej_w_adimira_putina_do_wsp_obywateli_moskwa_24_lutego_2022/ (dostęp: 14 sierpnia 2024 r.).

Riley T., *Russia's information war against Ukraine went stealth after Meta crackdown*, CyberScoop, 23 lutego 2022 r., https://cyberscoop.com/russias-information-war-ukraine-meta/ (dostęp: 4 marca 2024 r.).

Russia seems to be co-ordinating cyber-attacks with its military campaign, https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign?etear=nl_today_7 (dostęp: 4 marca 2024 r.).

Słowiński P., *NotPetya – analiza z perspektywy kryminalistyki i polskiego prawa karnego*, „Problemy Współczesnej Kryminalistyki" 2021, t. 25, https://journals.indexcopernicus.com/api/file/viewByFileId/1584929 (dostęp: 20 lutego 2024 r.).

Smalley S., *Russian disinformation rampant on far-right social media platforms*, CyberScoop, 13 grudnia 2023 r., https://cyberscoop.com/russia-disinformation-gab-parler/ (dostęp: 6 marca 2024 r.).

Staniurski P., *Trolling, fake news, infotainment. Rola mediów społecznościowych w prowadzeniu wojny informacyjnej na przykładzie działań podejmowanych w tym obszarze przez Federację Rosyjską*, w: Boćkowski D., Dąbrowska-Prokopowska E., Goryń P., Gorynia K. (red.), *Dezinformacja – Inspiracja – Społeczeństwo, Social Cybersecurity*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2022.

Stanovaya T., *Why Putin's Interview With Tucker Carlson Didn't Go to Plan*, 12 lutego 2024 r., https://carnegieendowment.org/politika/91614 (dostęp: 6 marca 2024 r.).

The cyber war in Ukraine is as crucial as the battle in the trenches, The Economist, 20 marca 2024 r., https://www.economist.com/europe/2024/03/20/the-cyber-war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches?utm_content=article-link-4&etear=nl_today_4&utm_campaign=r.the-economist-today&utm_medium=email.internal-newsletter.np&utm_source=salesforce-marketing-cloud&utm_term=3%2F20%2F2024&utm_id=1862034&slug=europe&slug=2024&slug=03&slug=20&slug=the-cyber war-in-ukraine-is-as-crucial-as-the-battle-in-the-trenches (dostęp: 21 marca 2024 r.).

The fight against pro-Kremlin disinformation, The European Council, 20 stycznia 2023 r., https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/ (dostęp: 6 marca 2024 r.).

Ukraina 2022, Część I. 10 miesięcy rosyjskiej propagandy. Luty – Grudzień 2022, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Ośrodek Studiów Przestrzeni Postsowieckiej.

Undermining Ukraine: How Russia widened its global information war in 2023, Digital Forensic Research Lab, 29 lutego 2024 r., https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/ (dostęp: 6 marca 2024 r.).

Vasquez Ch., *Ukraine information sharing a model for countering China, top cyber official says*, CyberScoop, 12 czerwca 2023 r., https://cyberscoop.com/information-sharing-china-threat/ (dostęp: 7 marca 2024 r.).

Vasquez Ch., Groll E., *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault*, CyberScoop, 10 sierpnia 2023 r., https://cyberscoop.com/viasat-ka-sat-hack-black-hat/ (dostęp: 4 marca 2024 r.).

Vicens A., *Ukraine's largest mobile communications provider down after apparent cyber attack*, CyberScoop, 12 grudnia 2023 r., https://cyberscoop.com/ukraines-largest-mobile-communications-provider-down-after-apparent-cyber-attack/ (dostęp: 4 marca 2024 r.).

Vincens A., *Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs,* CyberScoop, 21 marca 2024 r., https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/ (dostęp: 21 marca 2024 r.).

Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1–2.

Wilde G., *Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected*, Carnegie Endowment for International Peace, 11 marca 2024 r., https://carnegieendowment.org/2024/03/11/why-cyber-attacks-on-ukrainians-aren-t-working-way-russia-expected-pub-91931?utm_source=ctw&utm_medium=email&utm_campaign=buttonlink&mkt_tok=ODEzLVhZVS00MjIAAAGR3g8_OEaIEaMgnTOIVwcnOaymL8UiszkrN_U8H66y4zHZauBTuMIraa7isTbjZ3jY_35LsDa1e76YwBRcjyaYvUSv5_3PaU2tuVGjqR6rAg (dostęp: 15 marca 2024 r.).

Wilk A., Domańska M., *Rosyjski atak na Ukrainę (24 lutego, godz. 9.00)*, Ośrodek Studiów Wschodnich, 24 lutego 2022 r., https://www.osw.waw.pl/pl/publikacje/analizy/2022-02-24/rosyjski-atak-na-ukraine-24-lutego-godz-900 (dostęp: 20 lutego 2024 r.).

Wroe D., *Tucker Carlson, Vladimir Putin and the pernicious myth of the free market of ideas,* ASPI Strategist, 28 lutego 2024 r., https://www.aspistrategist.org.au/tucker-carlson-vladimir-putin-and-the-pernicious-myth-of-the-free-market-of-ideas/ (dostęp: 6 marca 2024 r.).

Zadorożna M., *The impact of wartime information strategy on defence capabilities. The case of the Russo-Ukrainian war*, "Cybersecurity and Law" 2023, nr 2.

DOI:10.59800/bn/196692

Stanisław Waszczykowski[1]
Biuro Polityki Międzynarodowej, Kancelaria Prezydenta RP, Warszawa, Polska

SZTUCZNE OBIEKTY I SPRZĘT WOJSKOWY JAKO ELEMENT DEZINFORMACJI WOJSKOWEJ. PRZYKŁADY ZASTOSOWANYCH CELÓW POZORNYCH PRZEZ SIŁY ZBROJNE UKRAINY PODCZAS KONFLIKTU ZBROJNEGO Z FEDERACJĄ ROSYJSKĄ

FAKE MILITARY OBJECTS AND EQUIPMENT AS AN ELEMENT OF MILITARY DECEPTION. EXAMPLES OF USING DUMMY TARGETS BY THE UKRAINIAN ARMED FORCES DURING THE ARMED CONFLICT WITH THE RUSSIAN FEDERATION

Abstrakt: Dezinformacja wojskowa jest kluczem do zbudowania niematerialnej przewagi nad przeciwnikiem. Jedna z jej metod to maskowanie operacyjne. W jego ramach wykorzystuje się m.in. sztuczne obiekty i sprzęt wojskowy, które stanowią środki pozoracji mające zmylić przeciwnika. To zjawisko jest obecne od czasów starożytnych, a współczesnymi przykładami wykorzystania makiet wojskowych były wojny w Zatoce Perskiej. Z takich rozwiązań korzysta również Ukraina od czasu pełnoskalowej agresji rosyjskiej. Ukraińskie siły używają prawdopodobnie głównie makiet imitujących środki artyleryjskie, systemów obrony powietrznej i rakietowej oraz systemów radarowych. W ten sposób skutecznie wprowadzają w błąd Rosjan, którzy stosują znacznie droższe środki w celu wyeliminowania sztucznych obiektów.

Słowa kluczowe: Ukraina, Rosja, dezinformacja wojskowa, makieta, sprzęt wojskowy

[1] https://orcid.org/0000-0002-2035-8785, swaszczyk@wp.pl.

Abstract: Military deception is the core of achieving an intangible advantage over the adversary. One of its methods is operational camouflage, which uses, among other things, dummy military objects and equipment as a means of decoy to deceive the opponent. This phenomenon has been around since ancient times, and contemporary examples of the use of military dummies could be seen during the Gulf Wars. Ukraine has also been using such approaches since the full-scale Russian aggression. Ukrainian forces are likely using mainly dummy units imitating artillery assets, air and missile defence systems, and radar systems. Thus, they effectively mislead the Russians, who use much more expensive resources to eliminate fake objects.

Keywords: Ukraine, Russia, military deception, dummy, military equipment

Wprowadzenie

Doświadczenia z toczonych w ciągu wieków wojen i konfliktów zbrojnych ukształtowały kanon praw walki zbrojnej i zasad sztuki wojennej, który w swoim założeniu powinien wskazywać reguły umożliwiające odniesienie zwycięstwa nad przeciwnikiem. Mimo ewolucji wielu czynników związanych z teorią i praktyką sztuki wojennej jako najważniejszą zasadę niezmiennie wymienia się przewagę[2], którą najprościej można definiować jako „górowanie nad przeciwnikiem”[3].

W literaturze przewaga nazywana jest „zasadą zasad”, która stanowi punkt centralny w sztuce wojennej, gdyż stosowanie pozostałych zasad i prawidłowości powinno umożliwić jej osiągnięcie i utrzymanie. To z kolei sprawia, że górująca strona może decydować o przebiegu i wyniku walki zbrojnej[4].

[2] S. Koziej, *Teoria sztuki wojennej*, Wydawnictwo Bellona, Warszawa 1993, s. 68-70.
[3] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (red.), *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020, s. 186.
[4] S. Koziej, *op. cit.*, s. 68-70.

Przewaga nad przeciwnikiem może mieć charakter zarówno materialny, jak i niematerialny, na który szczególną uwagę zwracał już Sun-Tzu, gdy wyodrębniał działania zmierzające m.in. do zaskoczenia nieprzyjaciela czy zmniejszenia jego woli walki. Dąży do niego często strona konfliktu słabsza pod względem konwencjonalnym czy liczebnym. Dzięki zastosowaniu wszelkiego rodzaju forteli czy maskowania[5] może ona zmylić i wprowadzić w błąd przeciwnika. Upraszczając, istotą tych działań jest prowadzenie dezinformacji wojskowej.

Jednym ze sposobów na wdrożenie skutecznej dezinformacji na polu walki dla osiągnięcia przewagi jest wykorzystanie odpowiednich narzędzi z zakresu maskowania wojskowego – zaliczyć do nich można oprócz stosowania kamuflażu także użycie środków pozornych, takich jak makiety i atrapy obiektów czy sprzętu wojskowego. Dzięki tego typu narzędziom da się zmylić przeciwnika co do planowanych działań lub w kontekście dysponowanego potencjału sił własnych.

Wykorzystanie celów pozornych podczas działań wojennych to praktyka znana od starożytności. W ciągu ostatnich wieków przykładów takiego sposobu dezinformacji na polu walki można doszukiwać się m.in. podczas wojny secesyjnej, gdy za pomocą drewnianych kłód imitowano armaty, I wojny światowej i bitwy pod Megiddo, podczas których Brytyjczycy użyli drewnianych koni, czy też II wojny światowej, kiedy wykorzystanie dmuchanych czołgów oraz innego rodzaju sztucznego sprzętu wojskowego i obiektów stało się powszechną praktyką[6]. Bardziej współczesnymi wzorcami mogą być działania strony irackiej podczas wojen w Zatoce Perskiej w 1991 oraz 2003 r. (użycie makiet czołgów i wyrzutni rakietowych)[7] czy armii jugosłowiańskiej podczas operacji NATO pod kryptonimem Allied Force (użycie makiet myśliwców i czołgów oraz pozorowanie

[5] *ibidem*, s. 70.

[6] R. Hémez, *To Survive, Deceive: Decoys in Land Warfare*, War on the Rocks, 22 kwietnia 2021 r., https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/ (dostęp: 27 marca 2024 r.).

[7] M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, Akademia Obrony Narodowej, Warszawa 2005, s. 52-56.

dróg i mostów)[8]. Przytoczone przykłady wskazują, że współcześnie pozorowanie na polu walki może stanowić w dalszym ciągu skuteczny sposób na dezinformowanie przeciwnika poprzez wprowadzanie go w błąd co do naszych sił, środków czy zamiarów.

W obliczu zapoczątkowanej 24 lutego 2022 r. agresji rosyjskiej na Ukrainę zasadne jest zbadanie wykorzystania celów pozornych przez stronę ukraińską (w ocenie autora stosunkowo słabszą pod względem ilościowo-materialnym) w ramach prowadzonej dezinformacji wojskowej. Pomimo pojawiających się na ten temat doniesień z mediów krajowych i zagranicznych warto usystematyzować obecny stan wiedzy dotyczący rodzajów wykorzystywanych sztucznych obiektów i sprzętu wojskowego przez Ukrainę.

Przedmiotem badań w niniejszym artykule jest wykorzystanie sztucznych obiektów i sprzętu wojskowego przez Ukrainę w celu dezinformacji wojskowej. Analiza ma doprowadzić do ustalenia rodzajów sztucznych obiektów i sprzętu wojskowego, zastosowanych przez stronę ukraińską. Wobec tak określonego celu problem badawczy został wyrażony w postaci pytania, jakie rodzaje sztucznych obiektów i sprzętu wojskowego wykorzystuje strona ukraińska w ramach prowadzenia dezinformacji wojskowej podczas konfliktu zbrojnego z Federacją Rosyjską. Do rozwiązania problemu zostały wykorzystane teoretyczne metody badawcze związane z analizą literatury przedmiotu i dostępnych źródeł internetowych (przekazów medialnych). Następnie przeanalizowany materiał został poddany syntezie i abstrahowaniu, co pozwoliło wybrać i przedstawić w niniejszej pracy jedynie treści potrzebne do rozwiązania problemu badawczego. Materiał poddano dedukcji w celu usystematyzowania dotychczasowej wiedzy oraz stworzenia katalogu przykładów potencjalnie wykorzystywanych sztucznych obiektów i sprzętu wojskowego przez Ukrainę. Jednocześnie pośrednią intencją niniejszej pracy jest zebranie w jednym miejscu potrzebnej terminologii i definicji, które odnoszą się do badanego zjawiska. Wykazanie zależności między nimi, wraz z próbą odpowiedniego ich uporządkowania, może

[8] M. Błaszczak, *Maskowanie w operacji „Allied Force”*, „Przegląd Sił Zbrojnych” 2020, nr 2, Wojskowy Instytut Wydawniczy, Warszawa 2020, s. 65–67.

stanowić podstawę do prowadzenia dalszych badań w tym zakresie. Tak kompleksowe podejście do tematu ma pozwolić na sformułowanie odpowiednich rekomendacji dla Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP).

Dezinformacja wojskowa, maskowanie i makiety – teoria i podejście wybranych podmiotów

Analiza badanego zjawiska wymaga wyjaśnienia, uporządkowania i sprecyzowania wcześniej przytoczonych terminów. Jak zaznaczono na wstępie, możliwym sposobem na uzyskanie przewagi jest zastosowanie działań mających na celu zmylenie i wprowadzenie w błąd potencjalnego przeciwnika. Jest to możliwe dzięki zastosowaniu dezinformacji wojskowej, którą można definiować jako „zamierzone przekazywanie (…) przygotowanych (fałszywych) informacji, pogłosek, specjalnie opracowanych dokumentów oraz demonstrowanie działań wojsk, których celem jest wprowadzenie w błąd przeciwnika w odniesieniu do prawdziwych zamierzeń, planów i przedsięwzięć o znaczeniu militarnym”[9]. Przytoczona definicja wskazuje, że dezinformacja wojskowa stanowi istotę działań niematerialnych wyszczególnionych we wcześniejszym rozdziale, pozwalających osiągnąć przewagę nad przeciwnikiem. Ponadto eksperci wojskowi podkreślają, że ma ona także znaczący wpływ na osiągnięcie efektu zaskoczenia[10], równie istotnego w przypadku chęci przejęcia inicjatywy i uzyskania uprzywilejowanej pozycji.

Istnieje kilka metod prowadzenia operacji o charakterze dezinformacji wojskowej, takich jak np. dezinformowanie agenturalne, radioelektroniczne czy maskowanie operacyjne[11], które stanowi kluczowy element do zrozumienia istoty postawionego problemu badawczego.

[9] M. Wrzosek, *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON” 2012, nr 2 (87), s. 23.

[10] T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego” 2015, nr 2 (24), Wydawnictwo Adam Marszałek, s. 49–65.

[11] R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022, s. 116–118.

Taki rodzaj maskowania w ujęciu metody prowadzenia wojskowej operacji dezinformacyjnej definiuje się jako „utrudnianie przeciwnikowi podejmowania prawidłowych decyzji i skutecznego prowadzenia działań zbrojnych; obejmuje ono ukrywanie wojsk i infrastruktury obronnej przed rozpoznaniem przeciwnika (np. z wykorzystaniem atrap, makiet), a także wprowadzenia go w błąd co do faktycznego położenia sił własnych i zamiaru prowadzonych działań”[12]. Z tak sformułowanej definicji wynika, że jednym z głównych narzędzi maskowania operacyjnego są makiety, które mają na celu imitowanie np. pododdziałów czy zasobów za pomocą wykorzystania sztucznych obiektów[13] i sprzętu wojskowego[14]. Przy tak postawionej konkluzji warto zaznaczyć, iż samo zjawisko maskowania w zależności od podejścia badawczego czy odmiennych założeń np. doktrynalnych może być inaczej definiowane i klasyfikowane[15]. Mając to na uwadze, autor przytacza definicję, która w jego opinii odzwierciedla uogólniony charakter pojęcia, prezentujący istotę badanego zagadnienia.

Kluczowym narzędziem maskowania operacyjnego są makiety, które „wykonuje się w celu pozorowania sprzętu bojowego i technicznego, uzbrojenia i obiektów tam, gdzie ich nie ma w rzeczywistości”[16]. Wobec tak określonego przeznaczenia zastosowania makiet warto na potrzeby badań uogólnić to pojęcie i zdefiniować jako egzemplarze całokształtu sztucznych obiektów i sprzętu wojskowego.

[12] *ibidem*, s. 118.

[13] Obiekt wojskowy – „(…) obiekt o znaczeniu obronnym, eksploatowany przez jednostki sił zbrojnych, często stanowiący część ugrupowania bojowego wojsk”. Za: J. Pawłowski, B. Zdrodowski, M. Kuliczkowski (red.), *op. cit.*, s. 134.

[14] Sprzęt wojskowy – „(…) wyposażenie specjalnie zaprojektowane lub zaadaptowane do potrzeb wojskowych, przeznaczone do użycia jako broń, amunicja lub materiały wojenne, techniczne środki walki, sprzęt techniczny oraz wyposażenie i środki zaopatrzenia (…)”. Za: *ibidem*, s. 207.

[15] „W literaturze przedmiotu niekiedy to maskowanie (klasyfikowane ze względu na poziomy: strategiczne, operacyjne i taktyczne) może stanowić nadrzędny rodzaj aktywności, w ramach którego rozróżnia się jego formy, dzieląc je na np. ukrywanie, pozorowanie i dezinformację. W takim układzie to pozorowanie będzie formą maskowania, w której wykorzystuje się sztuczne obiekty i sprzęt wojskowy. Taką klasyfikację można spotkać m.in. w polskich wojskowych dokumentach doktrynalnych”. Za: K. Wysocki, *Maskowanie jako antyfora rozpoznania*, w: K. Wysocki, W. Kuchta (red.), *Techniki i organizacyjne aspekty współczesnego maskowania*, Akademia Sztuki Wojennej, Warszawa 2022, s. 205-250.

[16] *ibidem*, s. 238.

Umiejętnie wykorzystane makiety mogą zostać użyte do pozorowania zarówno różnych obiektów infrastruktury, jak i śladów aktywności wojsk. Przykładowo da się w ten sposób stworzyć sztuczne lotniska (wraz z pasami startowymi), bazy zaopatrzenia, składy, stacje załadowania i wyładowania, węzły dróg, przeprawy i mosty, pozorne rozmieszczenia wojsk, ich pozycje, rubieże obronne, stanowiska dowodzenia czy stanowiska ogniowe artylerii[17]. Należy jednak zauważyć, że część wymienionych przykładów nie zawsze wymaga obecności makiet do skutecznego upozorowania ich istnienia. Są to szczególnie te sytuacje, gdy za skonstruowanie odpowiadają pododdziały inżynieryjne. Wykorzystują one specjalistyczny sprzęt, dzięki któremu mogą budować m.in. pozorne odcinki dróg manewru czy pozorne stanowiska startowe[18]. Wówczas samo odwzorowanie charakterystycznych śladów czy ukształtowania terenu może być wystarczające. Kolejny aspekt, o którym warto pamiętać przy pozorowaniu z użyciem makiet, to imitowanie charakterystycznych oznak aktywności danych jednostek sprzętu i pododdziałów, takich jak ruch pojazdu czy praca radaru[19].

W zależności od specyfiki sprzętu czy obiektu wojskowego, który ma pozorować makieta, powinna ona być skonstruowana z odpowiedniego tworzywa i mieć określone parametry. O ile w przeszłości było to łatwiejsze – do pozorowania podczas wojny secesyjnej wystarczyło użyć pomalowanego drewna o odpowiednich wymiarach (w celu stworzenia sztucznej armaty) – o tyle obecnie jest to bardziej złożona kwestia. Wpływają na to zwiększone możliwości rozpoznania wojskowego w aspekcie technicznym, a więc percepcji wyników obserwacji.

Sztuczne obiekty i sprzęt wojskowy w zależności od konkretnego przedmiotu, który mają pozorować, powinny odwzorowywać go jak najlepiej przede wszystkim w zakresach widzialnym, termalnym i radiolokacyjnym[20].

---

[17] *ibidem*, s. 213, 238.

[18] B. Bębenek, *Inżynieryjne aspekty maskowania wojsk*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2016, nr 1 (17), s. 5-16.

[19] K. Wysocki, *Maskowanie jako antyfora…*, *op. cit.*, s. 238.

[20] *ibidem*, s. 238.

W zakresie widzialnym makieta powinna być jak najdokładniej odwzorowana na kształt swojego pierwowzoru. Przyjmując za przykład bojowy wóz piechoty, jego makieta musi uwzględniać rzeczywistą wielkość pojazdu, jego kształt, detale czy wyposażenie widoczne z zewnątrz. Najlepiej, aby takiej makiety nie można było odróżnić od rzeczywistego sprzętu z odległości 1 km (lub 2,5 km z użyciem optyki)[21]. Z kolei w przypadku opisywanych w literaturze sposobów uzyskiwania efektu termalnego w makietach w ich konstrukcji pneumatycznej stosuje się odpowiedni mechanizm, który wytwarza ciepło. W zakresie radiolokacyjnym pozoracja możliwa jest natomiast dzięki użyciu specjalnych warstw zapewniających odbijanie pokrycia zewnętrznego[22].

Materiał, z którego skonstruowana jest makieta, będzie się różnił w zależności od charakteru pierwowzoru obiektu pozorowanego. W odniesieniu do zastosowanego przykładu pojazdu bojowego może on być z tworzywa sztucznego czy gumy[23], sklejki wodoodpornej, aluminium i stali, zamontowanej na stelażu pneumatycznym, pokrytym odpowiednim materiałem maskującym[24]. Metoda maskowania operacyjnego z wykorzystaniem makiet to sposób dezinformacji wojskowej, który ma współcześnie swoje odzwierciedlenie wśród wielu podmiotów – zarówno państw, jak i sojuszy.

Podejście Sojuszu Północnoatlantyckiego można zaprezentować na przykładzie zapisów ze „Słownika terminów i definicji NATO" (AAP – 6), w którym dezinformacja to „wszelkie przedsięwzięcia, mające na celu wprowadzenie przeciwnika w błąd poprzez (…) działania pozorujące (…)"[25]. Te działania według AAP-6 mają odwrócić uwagę i siły przeciwnika od zasadniczych przedsięwzięć. Mogą być do tego użyte cele pozorne, które mają imitować m.in. obiekty[26].

[21] M. Michalski, *Współczesne aspekty maskowania operacyjnego*, „Przegląd Sił Zbrojnych" 2020, nr 3, Wojskowy Instytut Wydawniczy, s. 89-95.

[22] B. Bębenek, *op. cit.*, s. 13.

[23] K. Wysocki, *Maskowanie jako antyfora…*, *op. cit.*, s. 239.

[24] B. Bębenek, *op. cit.*, s. 13.

[25] *AAP-6 Słownik terminów i definicji NATO. Zawierający wojskowe terminy i ich definicje stosowane w NATO*, Ministerstwo Obrony Narodowej, Warszawa 2017, s. 144.

[26] *ibidem*, s. 142, 162.

Dorobek Sun Tzu, wspomnianego wcześniej dalekowschodniego teoretyka wojennego, stanowi bardzo istotny element kształtujący współczesną chińską myśl strategiczną, w której podstęp i mistyfikacja odgrywają ważną rolę. Obecnie dezinformacja, ukrywanie i przede wszystkim pozorowanie, będące podstawową formą maskowania działań, są szeroko stosowane przez Chińską Armię Ludowo-Wyzwoleńczą. W skład jej struktury wchodzą dedykowane pododdziały, które używają makiet w celu imitacji sprzętu wojskowego i zmylenia przeciwnika[27].

Dezinformacja, maskowanie, pozorowanie i użycie makiet są obecne również w rosyjskich doktrynach, w których określa się te działania jako maskirowka (ten termin jest czasem traktowany wprost jako synonim dezinformacji)[28]. To bardzo szerokie pojęcie, które nie odnosi się jedynie do maskowania (na co może wskazywać nazwa), lecz także do większego wachlarzu możliwości, mających na celu wprowadzenie w błąd, zaskoczenie i zmylenie adwersarza. W ramach maskirowki wykorzystywane są również makiety do imitacji i kreowania fałszywej oceny sytuacji[29]. Obecnie Rosjanie stosują makiety podczas agresji na Ukrainę, o czym świadczą doniesienia medialne i materiały wideo publikowane przez stronę ukraińską[30].

Przedstawione definicje pozwalają lepiej zrozumieć charakter działań stanowiących główny obszar badań w niniejszym artykule. Jednocześnie należy dostrzec, że dezinformacja wojskowa, maskowanie i użycie makiet, czyli sztucznych obiektów i sprzętu wojskowego, to zjawiska, które stosowano zarówno w przeszłości, jak i na

[27] K. Wysocki, *Dalekowschodnie podejście do problematyki maskowania*, w: K. Wysocki, M. Depczyński (red)., *Teoria i praktyka współczesnego maskowania*, Akademia Sztuki Wojennej, Warszawa 2022, s. 235-257.

[28] Maskirowka w dosłownym tłumaczeniu oznacza maskowanie i jest używana do opisu radzieckiej (...) i rosyjskiej doktryny wojskowej zaskoczenia poprzez oszustwo, w którym znaczącą rolę odgrywa kamuflaż. Informacje za: Z. Modrzejewski, *Ewolucja rosyjskiej maskirowki*, „Przegląd Geopolityczny" 2020, nr 33, s. 65-79.

[29] Sz. Helma, *Dezinformacja i wojna psychologiczna jako element polityki Związku Sowieckiego i Federacji Rosyjskiej*, „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego. Nauki Społeczne" 2018, nr 22 (3), s. 79-98.

[30] S. Ankel, *Russia's inflatable decoy tanks are 'not credible' and need to be way better to trick Ukraine, expert says*, Business Insider, 27 września 2023 r., https://www.businessinsider.com/russia-inflatable-tanks-misused-not-credible-expert-2023-9?IR=T (dostęp: 28 marca 2024 r.).

obecnym polu walki. Wykorzystanie makiet przez Federację Rosyjską nie jest zaskoczeniem ze względu na jej długą historię dezinformacji wojskowej (maskirowki). Zasadne jednak wydaje się zbadanie użycia makiet przez stronę ukraińską, której siły zbrojne zmieniały się wielokrotnie w ciągu ostatnich 30 lat[31].

Ukraińskie doświadczenia – przykłady użycia makiet podczas pełnoskalowej agresji rosyjskiej

Chociaż Ukraina walczy z Federacją Rosyjską od 2014 r., to wykorzystanie przez Kijów sztucznych obiektów i sprzętu wojskowego zostało zastosowane najprawdopodobniej dopiero w chwili pełnoskalowej rosyjskiej agresji w 2022 r. Możliwy brak wykorzystania danego sprzętu (lub wykorzystania marginalnej liczby) w okresie od 2014 do 2022 r. wynika przypuszczalnie z początkowego prowadzenia operacji antyterrorystycznej przez dowództwo i pododdziały resortów siłowych, które mogły nie dysponować makietami. Po drugie, w skutek podpisania porozumień mińskich (szczególnie Mińsk II w 2015 r.) utworzona strefa bezpieczeństwa zakładała wycofanie ciężkiego sprzętu wojskowego, który w ocenie autora jest najczęściej imitowany za pomocą makiet. Te założenia potwierdzają pośrednio ukraińskie doniesienia medialne sprzed 24 lutego 2022 r., wskazujące na wykorzystanie makiet np. BM-21 Grad przez prorosyjskich separatystów. Dążyli oni do zmylenia i sprowokowania sił ukraińskich, które w przeciwieństwie do Rosjan starały się przestrzegać zapisów porozumień w rejonie strefy ówczesnej linii demarkacyjnej w Donbasie[32].

[31] Szerzej o zmianach, które zachodziły w ukraińskich siłach zbrojnych na przestrzeni ostatnich trzech dekad zob. w: S. Waszczykowski, *Siły Zbrojne Ukrainy w latach 2014-2020. Zarys struktury i wyposażenia*, 3 sierpnia 2020 r., https://www.konflikty.pl/technika-wojskowa/na-ladzie/sily-zbrojne-ukrainy-struktura-wyposazenie/ (dostęp: 28 marca 2024 r.).

[32] *ОБСЄ виявило макет "Граду" окупантів у районі роботи Bayraktar* [*OBWE ujawniło makietę Grad należącą do okupantów w obszarze działalności Bayraktara*], Militarnyi, 4 listopada 2021 r., https://mil.in.ua/uk/news/obsye-vyyavylo-mak1et-gradu-okupantiv-u-rajoni-roboty-bayraktar/ (dostęp: 28 marca 2024 r.).

Sytuacja zmieniła się w momencie wspomnianej pełnoskalowej rosyjskiej agresji na Ukrainę w 2022 r. Szczególne zainteresowanie tematem wykorzystania makiet zbiegło się z pierwszymi dostawami amerykańskich systemów artylerii rakietowej M142 High Mobility Artillery Rocket System (HIMARS) dla Ukrainy. Broń o parametrach, które dla Ukrainy były wcześniej nieosiągalne, Rosjanie traktowali jako cel priorytetowy. Ukraina wykorzystała to i zaczęła używać makiety HIMARS-ów. Te skutecznie zwabiały m.in. rosyjskie pociski manewrujące Kalibr, których koszt produkcji przewyższał wielokrotnie koszt wytworzenia makiety. Szacuje się, że wyprodukowanie zaawansowanej imitacji np. systemu HIMARS może oscylować w granicach do 100 tys. dolarów amerykańskich[33], a cena rosyjskiego pocisku Kalibr może być nawet dziesięciokrotnie większa i wynosić mln dolarów amerykańskich za sztukę[34]. Wprowadzeni w błąd Rosjanie informowali opinię publiczną o kolejnych egzemplarzach zniszczonych systemów. Amerykanie natomiast w sposób satyryczny komentowali rosyjskie sukcesy i wskazywali, że zniszczyli więcej HIMARS-ów, niż łącznie zostały w tym czasie przekazane Ukrainie przez Stany Zjednoczone. Tak skuteczne pierwsze zmylenia przeciwnika zmotywowały stronę ukraińską do rozszerzenia produkcji i zwiększenia wykorzystania sztucznych obiektów i sprzętu wojskowego[35].

Spektakularne i obiecujące wykorzystanie sztucznych drewnianych HIMARS-ów poprzedzały mniejsze projekty, których autorami byli ukraińscy ochotnicy konstruujący makiety niewielkiego i mniej skomplikowanego sprzętu. Przykładem są proste konstrukcje imitujące ukraiński przeciwpancerny pocisk kierowany (ppk.) Stugna-P,

[33] *Inflatable tanks, missiles: Czech firm makes decoy armaments*, Associated Press News, 6 marca 2023 r., https://apnews.com/article/czech-decoys-war-ukraine-russia-inflatable-a9c478adb9d7ecaa615cb19b25f4833f (dostęp: 28 marca 2024 r.).

[34] *What is the Real Price of russian Missiles: About the Cost of 'Kalibr', Kh-101 and 'Iskander' Missiles*, Defense Express, 1 listopada 2022 r., https://en.defence-ua.com/news/what_is_the_real_price_of_russian_missiles_about_the_cost_of_kalibr_kh_101_and_iskander_missiles-4709.html (dostęp: 28 marca 2024 r.).

[35] J. Hudson, *Ukraine lures Russian missiles with decoys of U.S. rocket system*, "Washington Post", 30 sierpnia 2022 r., https://www.washingtonpost.com/world/2022/08/30/ukraine-russia-himars-decoy-artillery/ (dostęp: 28 marca 2024 r.).

produkowane z metalu, drewna i plastiku. Koszt produkcji jednego egzemplarza może wynosić nawet mniej niż 30 dolarów, co sprawia, że podobnie jak w przypadku drewnianych HIMARS-ów środek użyty do zniszczenia takiej makiety kosztuje wielokrotnie więcej. Kolejnymi przykładami sztucznego sprzętu wojskowego, który wytwarzają ukraińscy obywatele, są posowieckie 152 mm haubicoarmaty D-20[36].

Należy mieć w pamięci, iż Federacja Rosyjska również nie rezygnuje z wykorzystywania sztucznych obiektów i sprzętu wojskowego. Skuteczne użycie atrap w pierwszych miesiącach wojny zainicjowało rozpoczęcie „wyścigu zbrojeń makiet"[37] między stronami konfliktu. Zarówno Ukraina, jak i Rosja zostały zmuszone do poszukiwania coraz lepszych rozwiązań i metod ich konstruowania, które jak najdokładniej odwzorowują imitowany sprzęt pod względem widzialnym, termalnym i radiolokacyjnym.

Wraz ze wzrostem zapotrzebowania ukraińskich sił zbrojnych na sztuczne obiekty i sprzęt wojskowy oprócz oddolnych inicjatyw obywateli pojawiły się fabryki, które rozpoczęły produkcję makiet na szerszą skalę. Przykład stanowią warsztaty prowadzone przez pracowników firmy hutniczej Metinvest, która zarządzała hutą Azovstal w Mariupolu[38]. Wytwarzane przez nich makiety imitują m.in. amerykańskie haubice kalibru 155 mm M777. Wykorzystują do tego materiały, które pozwalają jak najlepiej odwzorować oryginał przy poniesieniu jak najniższych kosztów. W efekcie np. lufę działa wykonuje się z rur kanalizacyjnych. Tak wyprodukowany sprzęt pakowany jest w paczki i wysyłany na front, gdzie jego montaż zajmuje

[36] M. Krygel, *Destroy me quickly. How Ukrainian fake HIMARS, guns and tanks fight with Russian Kalibr and Iskander missiles*, Українська правда, 11 marca 2024 r., https://www.pravda.com.ua/eng/articles/2024/03/11/7445807/ (dostęp: 28 marca 2024 r.).

[37] C. Panella, *A 'decoy arms race' is playing out in Ukraine, where deception is getting harder and troops have to treat fakes like they're real to fool the enemy*, Business Insider, 2 października 2023 r., https://www.businessinsider.com/decoy-arms-race-playing-out-ukraine-harder-fake-tanks-weapons-2023-10?IR=T (dostęp: 28 marca 2024 r.).

[38] E. Graham-Harrison, *'A psychological weapon': inside a Ukrainian factory making decoy kit*, "The Guardian", 4 września 2023 r., https://www.theguardian.com/world/2023/sep/04/a-psychological-weapon-inside-a-ukrainian-factory-making-decoy-kit (dostęp: 28 marca 2024 r.).

mniej niż 30 minut[39]. Oprócz haubic M777 fabryki Metinvest produkują również sowieckie haubice D-20 i D-30 oraz kilka rodzajów stacji radarowych (np. system radarowy 35D6[40] oraz stację radiolokacyjną Malachit[41]) i walki radioelektronicznej. W zależności od rodzaju imitowanego obiektu lub sprzętu wojskowego pracownicy fabryki wskazują, że makiety, jeśli zachodzi taka potrzeba, są montowane na ruchomych platformach (pojazdach), mogących samodzielnie poruszać się i zmieniać pozycję[42].

Ukraina jest najprawdopodobniej wspierana przez zagranicznych dostawców. Czeska firma Inflatech, chociaż przez długi czas nie potwierdzała współpracy z Kijowem, była zaktywizowana w ukraińskiej infosferze. W mediach prezentowano szeroki wachlarz makiet czeskiej produkcji, w tym dmuchanych systemów obrony powietrznej Patriot, HIMARS-y, czołgi Leopard 2 czy samobieżne przeciwlotnicze zestawy rakietowe SA-8[43]. Dopiero w maju 2023 r. firma poinformowała, że dostarcza na Ukrainę dmuchane czołgi Leopard 2A4, których waga nie przekracza 44 kg, a ich rozłożenie jest możliwe nawet w 10 minut. Ukraińskie media podają, że oprócz wersji 2A4 ukraińscy żołnierze wykorzystują również makiety czołgów Leopard 2A6[44].

W mediach pojawiają się (bez jednoznacznego wskazania wykonawcy lub dostawcy) także inne makiety, z których mają korzystać

[39] S. Miller, *Battlefield Decoys and Deception: Reaffirmed in Ukraine*, Armada International, 20 września 2023 r., https://www.armadainternational.com/2023/09/battlefield-decoys-and-deception-reaffirmed-in-ukraine/ (dostęp: 28 marca 2024 r.).

[40] Наче "примарна армія" Паттона*:* як макети техніки ЗСУ вводять в оману російських окупантів [*To jak „armia duchów" Pattona: jak makiety sprzętu wojskowego wprowadzają w błąd rosyjskich okupantów*], MRPL.CITY, 5 października 2023 r., https://mrpl.city/news/view/nache-primarna-armiya-pattona-yak-maketi-tehniki-zsu-vvodyat-v-omanu-rosijskih-okupantiv (dostęp: 28 marca 2024 r.).

[41] M. Krygel, *op. cit.*

[42] «Наші «Хаймарси» вміють навіть рухатися», – Метінвест про макети зброї для фронту [*"Nasze HIMARsy mogą się nawet poruszać", Metinvest o modelach uzbrojenia na pierwszej linii frontu*], TSN.ua, 30 października 2023 r., https://tsn.ua/zbroya/nashi-haymarsi-vmiyut-navit-ruhatisya-metinvest-pro-maketi-zbroyi-dlya-frontu-2440198.html (dostęp: 28 marca 2024 r.).

[43] Наче "примарна армія" Паттона*:…* [*To jak „armia duchów" Pattona:…], op. cit.*

[44] Україна у війні застосовує макети танків *Leopard 2* [*Ukraina używa podczas wojny makiet czołgów Leopard 2*], Militarnyi, 2 listopada 2023 r., https://mil.in.ua/uk/news/ukrayina-u-vijni-zastosovuye-makety-tankiv-leopard-2/ (dostęp: 28 marca 2024 r.).

ukraińskie siły. Blogerzy i dziennikarze wskazują na pojawienie się z początkiem 2024 r. makiet dostarczanego przez Niemcy systemu przeciwlotniczego IRIS-T SLM czy produkowanego w USA systemu radarowego AN/MPQ-64 Sentinel. Równocześnie przedstawiane są nagrania, na których widać, jak Rosjanie niszczą fałszywe systemy, co w efekcie potwierdza zasadność stosowania danych makiet[45]. Z analizy podobnych nagrań wynika, że oprócz m.in. artylerii, naziemnych systemów obrony powietrznej czy radarów Ukraina korzysta również z makiet statków powietrznych, takich jak np. samolot szturmowy Su-25[46]. Wykorzystując taką makietę, można skutecznie odwzorowywać pozorne lotniska czy miejsca dyslokacji sprzętu.

Z upływem czasu również oddolni ochotniczy konstruktorzy dzięki zdobytemu doświadczeniu poszerzyli wachlarz produkowanych makiet o kolejne rodzaje mniejszego sprzętu i obiektów wojskowych. W chwili prowadzenia niniejszych badań, to jest w marcu 2024 r., najnowsze doniesienia medialne wskazują na konstruowanie przez ukraińskich obywateli makiet terminali Starlink, produkowanych z drewna, metalu i plastiku. Oprócz wspomnianych wcześniej ppk. Stugna-P jednocześnie powstają prawdopodobnie makiety moździerzy 82 mm i 120 mm, które w ocenie ukraińskiego wojska są odwzorowane bardzo precyzyjnie[47]. Na szczególną uwagę zasługują nowe komunikaty medialne, które dotyczą planowania stworzenia i wykorzystania przez Kijów makiet imitujących amerykańskie systemy obrony powietrznej i przeciwrakietowej Patriot[48]. Jak wskazano wcześniej, mogą one być już używane na polu walki.

[45] T. Newdick, *Ukraine's Air Defense Decoys Keep Getting Better*, The War Zone, 2 lutego 2024 r., https://www.twz.com/land/ukraines-air-defense-decoys-keep-getting-better (dostęp: 28 marca 2024 r.).

[46] *ibidem*.

[47] I. Refagi, Обдурити росіян*:* українські волонтери створюють макети терміналів *Starlink* для ЗСУ [*By oszukać Rosjan: ukraińscy wolontariusze tworzą makiety terminali Starlink dla sił zbrojnych*], „Фокус", 27 marca 2024 r., https://focus.ua/uk/digital/636081-obduriti-rosiyan-ukrajinski-volonteri-stvoryuyut-maketi-terminaliv-starlink-dlya-zsu (dostęp: 28 marca 2024 r.).

[48] J. Szewczenko, Український фронт заполонили муляжі військової техніки*:* чому зріс попит на фальш-зброю [*Makiety sprzętu wojskowego zalały front ukraiński: dlaczego wzrosło zapotrzebowanie na podrabianą broń*], „Фокус", 30 marca 2024 r., https://focus.ua/uk/amp/voennye-novosti/636939-ukrajinskiy-front-zapolonili-mulyazhi-viyskovoji-tehniki-chomu-zris-popit-na-falsh-zbroyu-foto (dostęp: 30 marca 2024 r.).

Na podstawie przytoczonych informacji można określić następujący katalog wykorzystywanych przez Ukrainę sztucznych obiektów i sprzętu wojskowego, które składają się na makiety pozorujące:

1. Środki artyleryjskie (wraz z ppk.): ppk. Stugna-P, moździerze 82 mm i 120 mm, haubicoarmaty D-20, haubice D-30, 155 mm haubice M777 oraz systemy artylerii rakietowej wysokiej mobilności M142 HIMARS;
2. Systemy obrony powietrznej i przeciwrakietowej: Patriot, przeciwlotnicze zestawy SA-8, systemy przeciwlotnicze IRIS-T SLM;
3. Stacje radiolokacyjne i systemy radarowe: radar 35D6, AN/MPQ-64 Sentinel, stacje radiolokacyjne Malachit;
4. Wozy bojowe: czołgi Leopard 2A4 i 2A6;
5. Statki powietrzne: Su-25;
6. Inne obiekty i sprzęt wojskowy: telekomunikacyjne systemy satelitarne – terminale Starlink.

Tak zebrane i uporządkowane informacje pozwalają wysnuć tezę, że najczęściej i najliczniej pozorowanymi obiektami i sprzętami wojskowymi są środki artyleryjskie wraz z systemami obrony powietrznej i rakietowej oraz systemy radarowe. Jednocześnie szczególną uwagę należy zwrócić na pozorowanie mniejszego gabarytowo sprzętu, jak ppk. czy moździerz, w które mogą być wyposażane najmniejsze pododdziały (drużyny, sekcje, działony, załogi).

Od początku wojny ukraińskie możliwości w zakresie tworzenia i użycia sztucznych obiektów i sprzętu wojskowego ewoluowały i w efekcie stawały się coraz bardziej docenianym sposobem prowadzenia dezinformacji wojskowej. Główne media w Ukrainie wskazywały w marcu 2024 r., że istnieją plany utworzenia w każdej brygadzie specjalnie dedykowanego pododdziału (kompanii), którego zadania będą związane stricte z maskowaniem (w aspekcie kamuflażu i pozoracji). Jednym z czynników warunkujących te decyzje są wnioski z dotychczasowej praktyki wskazujące, iż umiejętne wykorzystanie makiet może wpłynąć na zmniejszenie strat prawdziwych obiektów i sprzętu wojskowego od 30 do 50 proc. Do przytoczonych informacji odniósł się Aleksander Kamyshyn (piastujący w czasie prowadzenia badań stanowisko Ministra Przemysłu Strategicznego Ukrainy), który

w wywiadzie dla gazety internetowej Ukraińska Prawda podkreślił, że po wojnie kraj będzie mógł podzielić się swoimi doświadczeniami i know-how z efektywnego wykorzystania makiet[49].

Przeprowadzone badania pozwalają stwierdzić, że Ukraina stale podejmuje działania z zakresu dezinformacji wojskowej przy zastosowaniu sztucznego sprzętu i obiektów wojskowych, które w efekcie osiągają zamierzone cele. Wskazane przykłady udowadniają, że Ukraina stosując dużo tańsze w przygotowaniu makiety, skutecznie wabi do ich zniszczenia dużo droższą rosyjską amunicję. Makiety spełniają więc swoją rolę, którą określono w rozdziale teoretycznym. Jednocześnie należy zauważyć, że Ukraina stale rozwija i dostosowuje produkcję wojskowych atrap. Po pierwsze, tworzy je z odpowiednich lub bardziej przystosowanych do potrzeb materiałów. Po drugie, imituje nowe rodzaje i typy środków, które ukraińskie siły zbrojne już posiadają na wyposażeniu lub otrzymują od zagranicznych partnerów i sojuszników.

Podsumowanie

Wykorzystanie sztucznych obiektów i sprzętu wojskowego jako elementu dezinformacji podczas konfliktów zbrojnych ma swoją długą historię. Doświadczenia z przeszłości wielokrotnie pokazywały, że można w ten sposób zmylić przeciwnika i dzięki tak zbudowanej przewadze odnieść zwycięstwo nawet z liczebnie silniejszym adwersarzem. Trwająca wojna w Ukrainie pokazuje, że zastosowanie makiet jako środka pozoracji stanowi w dalszym ciągu skuteczne narzędzie do prowadzenia dezinformacji wojskowej.

Przeprowadzona analiza potwierdza zasadność przypuszczeń dotyczących wykorzystywania makiet przez stronę ukraińską podczas starć z Federacją Rosyjską. Na podstawie badań opracowano katalog potencjalnie wykorzystywanych rodzajów sztucznych obiektów i sprzętu wojskowego przez siły zbrojne Ukrainy. Przypuszczalnie najczęściej i najliczniej pozorowane są przez nich środki artyleryjskie,

[49] M. Krygel, *op. cit.*

systemy obrony powietrznej i rakietowej oraz systemy radarowe. Przy ich użyciu prawdopodobnie mogą być tworzone m.in. pozorne pozycje wojsk, rubieże obronne oraz stanowiska ogniowe artylerii. Nie jest to jednak zamknięty katalog, ponieważ w przyszłości będzie można stworzyć bardziej zróżnicowany i uszczegółowiony wykaz wykorzystywanych środków. Wobec tak uzyskanych i uporządkowanych informacji należy uznać, że dzięki analizie udało się rozwiązać postawiony problem badawczy. Ponadto całościowo opracowany materiał, przy uwzględnieniu przytoczonych i usystematyzowanych ram teoretycznych, może stanowić podstawę do dalszych interpretacji w zakresie dezinformacji wojskowej.

Opisane ukraińskie doświadczenia z wykorzystania sztucznych obiektów i sprzętu wojskowego dają również cenne wskazówki Polsce. Siły Zbrojne RP badały intensywnie kwestię wykorzystania makiet jako środka pozoracji szczególnie w latach 90. ubiegłego wieku. Wojskowe instytuty, które zajmowały się tą kwestią, projektowały makiety imitujące sprzęt bojowy etatowo eksploatowany przez polskie wojska lądowe (m.in. czołgi T-72, Bojowe Wozy Piechoty czy pojazdy STAR 266)[50]. Później projektami aktualnego sprzętu (np. KTO Rosomak) zajmowały się polskie spółki współpracujące z SZ RP. Wnioski wynikające z przeprowadzonych badań wskazują, że wykorzystanie makiet jako środka pozoracji może skutecznie wprowadzać przeciwnika w błąd oraz ochronić rzeczywiste siły przed ich wyeliminowaniem. Zasadne jest zatem wznowienie lub kontynuowanie prac w zakresie pozyskiwania i wzmocnienia zdolności do pozorowania sztucznych obiektów i sprzętu wojskowego przez SZ RP. Jednocześnie wojsko nie powinno zostać osamotnione w zakresie tych działań. Sama produkcja makiet stała się bowiem osobną gałęzią działalności zarówno przedsiębiorców (zagranicznych i ukraińskich), jak i ludności cywilnej. Świadczy to o możliwości współpracy cywilno-wojskowej na różnych poziomach. Umiejętności i zdolności wytworzenia sztucznych obiektów i sprzętu wojskowego przez różne podmioty (firmy, osoby) powinny być identyfikowane i wspierane

[50] B. Bębenek, *op. cit.*, s. 13.

zawczasu, tak aby ludność cywilna mogła wspierać realnie SZ RP w czasie pokoju, kryzysu i wojny.

Uwaga: opinie zawarte w tym artykule są opiniami autora i nie powinny być identyfikowane z oficjalnym stanowiskiem Biura Polityki Międzynarodowej czy Kancelarii Prezydenta RP.

Bibliografia
References list

AAP-6 Słownik terminów i definicji NATO. Zawierający wojskowe terminy i ich definicje stosowane w NATO, Ministerstwo Obrony Narodowej, Warszawa 2017.

Ankel S., *Russia's inflatable decoy tanks are 'not credible' and need to be way better to trick Ukraine, expert says*, Business Insider, 27 września 2023 r., https://www.businessinsider.com/russia-inflatable-tanks-mis used-not-credible-expert-2023-9?IR=T (dostęp: 28 marca 2024 r.).

Bębenek B., *Inżynieryjne aspekty maskowania wojsk*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2016, nr 1 (17).

Błaszczak M., *Maskowanie w operacji „Allied Force"*, „Przegląd Sił Zbrojnych" 2020, nr 2, Wojskowy Instytut Wydawniczy.

Graham-Harrison E., *'A psychological weapon': inside a Ukrainian factory making decoy kit*, "The Guardian", 4 września 2023 r., https://www.theguardian.com/world/2023/sep/04/a-psychological-weapon-inside-a-ukrainian-factory-making-decoy-kit (dostęp: 28 marca 2024 r.).

Helma Sz., *Dezinformacja i wojna psychologiczna jako element polityki Związku Sowieckiego i Federacji Rosyjskiej*, „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego. Nauki Społeczne" 2018, nr 22 (3).

Hémez R., *To Survive, Deceive: Decoys in Land Warfare*, War on the Rocks, 22 kwietnia 2021 r., https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/ (dostęp: 27 marca 2024 r.).

Hudson J., *Ukraine lures Russian missiles with decoys of U.S. rocket system*, "Washington Post", 30 sierpnia 2022 r., https://www.washingtonpost.com/world/2022/08/30/ukraine-russia-himars-decoy-artillery/ (dostęp: 28 marca 2024 r.).

Inflatable tanks, missiles: Czech firm makes decoy armaments, Associated Press News, 6 marca 2023 r., https://apnews.com/article/czech-decoys-war-ukraine-russia-inflatable-a9c478adb9d7ecaa615cb19b25f4833f (dostęp: 28 marca 2024 r.).

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2 (24), Wydawnictwo Adam Marszałek.

Koziej S., *Teoria sztuki wojennej*, Wydawnictwo Bellona, Warszawa 1993.

Krygel M., *Destroy me quickly. How Ukrainian fake HIMARS, guns and tanks fight with Russian Kalibr and Iskander missiles*, Українська правда, 11 marca 2024 r., https://www.pravda.com.ua/eng/articles/2024/03/11/7445807/ (dostęp: 28 marca 2024 r.).

Kupiecki R., Bryjka F., Chłoń T., *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022.

Michalski M., *Współczesne aspekty maskowania operacyjnego*, „Przegląd Sił Zbrojnych" 2020, nr 3, Wojskowy Instytut Wydawniczy.

Miller S., *Battlefield Decoys and Deception: Reaffirmed in Ukraine*, Armada International, 20 września 2023 r., https://www.armadainternational.com/2023/09/battlefield-decoys-and-deception-reaffirmed-in-ukraine/ (dostęp: 28 marca 2024 r.).

Modrzejewski Z., *Ewolucja rosyjskiej maskirowki*, „Przegląd Geopolityczny" 2020, nr 33.

«Наші «Хаймарси» вміють навіть рухатися», – Метінвест про макети зброї для фронту [*„Nasze HIMARsy mogą się nawet poruszać", Metinvest o modelach uzbrojenia na pierwszej linii frontu*], TSN.ua, 30 października 2023 r., https://tsn.ua/zbroya/nashi-haymarsi-vmiyut-navit-ruhatisya-metinvest-pro-maketi-zbroyi-dlya-frontu-2440198.html (dostęp: 28 marca 2024 r.).

Newdick T., *Ukraine's Air Defense Decoys Keep Getting Better*, The War Zone, 2 lutego 2024 r., https://www.twz.com/land/ukraines-air-defense-decoys-keep-getting-better (dostęp: 28 marca 2024 r.).

ОБСЄ виявило макет "Граду" окупантів у районі роботи Bayraktar [OBWE ujawniło makietę Grad należącą do okupantów w obszarze działalności Bayraktara], Militarnyi, 4 listopada 2021 r., https://mil.in.ua/uk/news/obsye-vyyavylo-mak1et-gradu-okupantiv-u-rajoni-roboty-bayraktar/ (dostęp: 28 marca 2024 r.).

Panella C., *A 'decoy arms race' is playing out in Ukraine, where deception is getting harder and troops have to treat fakes like they're real to fool the enemy*, Business Insider, 2 października 2023 r., https://www.businessinsider.com/decoy-arms-race-playing-out-ukraine-harder-fake-tanks-weapons-2023-10?IR=T (dostęp: 28 marca 2024 r.).

Pawłowski J., Zdrodowski B., Kuliczkowski M. (red.), *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020.

Refagi I., Обдурити росіян*:* українські волонтери створюють макети терміналів *Starlink* для ЗСУ [*By oszukać Rosjan: ukraińscy wolontariusze tworzą makiety terminali Starlink dla sił zbrojnych*], „Фокус", 27 marca 2024 r., https://focus.ua/uk/digital/636081-obduriti-rosiyan-ukrajinski-volonteri-stvoryuyut-maketi-terminaliv-starlink-dlya-zsu (dostęp: 28 marca 2024 r.).

Szewczenko J., Український фронт заполонили муляжі військової техніки*:* чому зріс попит на фальш-зброю [*Makiety sprzętu wojskowego zalały front ukraiński: dlaczego wzrosło zapotrzebowanie na podrabianą broń*], „Фокус", 30 marca 2024 r., https://focus.ua/uk/amp/voennye-novosti/636939-ukrajinskiy-front-zapolonili-mulyazhi-viyskovoji-tehniki-chomu-zris-popit-na-falsh-zbroyu-foto (dostęp: 30 marca 2024 r.).

Наче „примарна армія" Паттона*:* як макети техніки ЗСУ вводять *в* оману російських окупантів [*To jak „armia duchów" Pattona: jak makiety sprzętu wojskowego wprowadzają w błąd rosyjskich okupantów*], MRPL.CITY, 5 października 2023 r., https://mrpl.city/news/view/nache-primarna-armiya-pattona-yak-maketi-tehniki-zsu-vvodyat-v-omanu-rosijskih-okupantiv (dostęp: 28 marca 2024 r.).

Україна у війні застосовує макети танків *Leopard 2* [*Ukraina używa podczas wojny makiet czołgów Leopard 2*], Militarnyi, 2 listopada 2023 r., https://mil.in.ua/uk/news/ukrayina-u-vijni-zastosovuye-makety-tanki-v-leopard-2/ (dostęp: 28 marca 2024 r.).

What is the Real Price of russian Missiles: About the Cost of 'Kalibr', Kh-101 and 'Iskander' Missiles, Defense Express, 1 listopada 2022 r., https://en.defence-ua.com/news/what_is_the_real_price_of_russian_missiles_about_the_cost_of_kalibr_kh_101_and_iskander_missiles-4709.html (dostęp: 28 marca 2024 r.).

Wrzosek M., *Dezinformacja – skuteczny element walki informacyjnej*, „Zeszyty Naukowe AON" 2012, nr 2 (87).

Wrzosek M., *Dezinformacja jako komponent operacji informacyjnych*, Akademia Obrony Narodowej, Warszawa 2005.

Wysocki K., *Dalekowschodnie podejście do problematyki maskowania,* w: Wysocki K., Depczyński M. (red)., *Teoria i praktyka współczesnego maskowania,* Akademia Sztuki Wojennej, Warszawa 2022.

Wysocki K., *Maskowanie jako antyfora rozpoznania*, w: Wysocki K., Kuchta W. (red.), *Techniki i organizacyjne aspekty współczesnego maskowania*, Akademia Sztuki Wojennej, Warszawa 2022.

NOTKA BIOGRAFICZNA

Krzysztof Kaczmarek
Politolog i matematyk. Doktor nauk społecznych w dyscyplinie nauki o polityce i administracji, adiunkt na Wydziale Humanistycznym Politechniki Koszalińskiej. Autor publikacji dotyczących m.in. zagrożeń hybrydowych, ukrytych zasobów Internetu oraz szeroko rozumianego bezpieczeństwa obszarów arktycznych Europy.

Łukasz Dryblak
Dr, ad. w Zakładzie Historii XX w. Instytutu Historii im. Tadeusza Manteuffla PAN oraz analityk w Biurze Bezpieczeństwa Narodowego. Specjalizuje się w historii dziejów emigracji rosyjskiej, polskiej myśli politycznej i sowietologicznej. Autor monografii „Pozyskać przeciwnika. Stosunki polityczne między państwem polskim a mniejszością i emigracją rosyjską w latach 1926–1935" (Warszawa 2021) oraz „Szermierze wolności i zakładnicy imperium. Emigracyjny dialog polsko-rosyjski w latach 1939–1956. Konfrontacje idei, koncepcji oraz analiz politycznych" (Warszawa 2023).

Marek Wrzosek
Prof. dr hab. płk rez. Wykładowca Wydziału Wojskowego Akademii Sztuki Wojennej. Służbę wojskową pełnił w jednostkach rozpoznawczych, był dowódcą plutonu rozpoznawczego, kompanii rozpoznawczej, szefem rozpoznania pułku i oficerem wydziału

rozpoznawczego dywizji. W latach 2007–2015 prodziekan Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej w Warszawie. Następnie prorektor ds. naukowych Akademii Obrony Narodowej, a potem Akademii Sztuki Wojennej (do 2018 r.). Od wielu lat w pracy zawodowej, dydaktycznej i naukowej zajmuje się kwestiami bezpieczeństwa militarnego, w tym zagadnieniami związanymi z systemem rozpoznania wojskowego i oceną zagrożeń militarnych i niemilitarnych. Jest autorem licznych opracowań o charakterze teoretycznym i praktycznym, realizatorem i uczestnikiem prac naukowo-badawczych oraz projektów, również z udziałem podmiotów zagranicznych.

Paweł Pelc
Radca prawny, prowadzi Kancelarię Radcy Prawnego Pawła Pelca. W 2024 r. na Akademii Sztuki Wojennej obronił rozprawę doktorską pt. „Aspekty prawne nadzoru nad rynkiem otwartych funduszy emerytalnych w Polsce". Specjalizuje się w kwestiach związanych z regulacjami dotyczącymi cyberbezpieczeństwa, z nadzorem nad instytucjami finansowymi, rynkami finansowymi i rynkiem kapitałowym oraz kapitałowymi systemami emerytalnymi. Był m.in. wiceprezesem Urzędu Nadzoru nad Funduszami Emerytalnymi, Wiceprzewodniczącym Komisji Papierów Wartościowych i Giełd oraz Komisji Nadzoru Ubezpieczeń i Funduszy Emerytalnych, członkiem Komisji Nadzoru Finansowego, dyrektorem zarządzającym pionem nadzoru w Urzędzie Komisji Nadzoru Finansowego, doradcą Prezesa oraz Dyrektorem Departamentu Audytu Wewnętrznego w Narodowym Banku Polskim. Doradzał Komisji Papierów Wartościowych na Litwie, Komisji Nadzoru Finansowego w Bułgarii, Urzędowi Nadzoru nad Funduszami Emerytalnymi w Macedonii oraz Ghanie. Był badaczem w Akademickim Centrum Polityki Cyberbezpieczeństwa, a także członkiem zarządu Polskiej Grupy Zbrojeniowej i Wiceprezesem Agencji Ratingu Społecznego. Publikował m.in. w czasopismach: „Cybersecurity and Law", „Prawo i Więź", „Prawo Kanoniczne", „Prawo Bankowe", „Pieniądze i Więź", „Forum Prawnicze. Gazeta Bankowa", „Rachunkowość Bankowa", „Gazeta Ubezpieczeniowa", „Forum

Dyskusyjne Ubezpieczeń i Funduszy Emerytalnych", „Radca Prawny", a także w monografiach krajowych i zagranicznych.

Stanisław Waszczykowski
Urzędnik państwowy, oficer rezerwy. Absolwent Akademii Sztuki Wojennej, ukończył tam studia licencjackie na kierunku Obronność na Wydziale Wojskowym, studia magisterskie na kierunku Bezpieczeństwo Międzynarodowe i Dyplomacja na Wydziale Bezpieczeństwa Narodowego oraz studia podyplomowe na kierunku Międzynarodowe Stosunki Wojskowe. Stażysta w Biurze Bezpieczeństwa Narodowego w Departamencie Analiz Strategicznych oraz Departamencie Zwierzchnictwa nad Siłami Zbrojnymi. Autor publikacji na portalu konflikty.pl oraz były członek zespołu i analityk Instytutu Nowej Europy. Obecnie specjalista w Zespole Analiz Biura Polityki Międzynarodowej w Kancelarii Prezydenta RP. Jego zainteresowania badawcze obejmują zagadnienia związane z misjami i operacjami pokojowymi ONZ, funkcjonowaniem OBWE oraz szeroko rozumianą polityką bezpieczeństwa.

ISSN 1896-4923
e-ISSN 2956-8536