Studia Politicae Universitatis Silesiensis 2023, T. 36/37, s. 51–69
ISSN 2353-9747 (wersja elektroniczna)
www.studiapoliticae.us.edu.pl
Data wpływu: 30.09.2023; data akceptacji: 31.12.2023
DOI: 10.31261/spus.16882

Wojna informacyjna jako instrument polityki zagranicznej Federacji Rosyjskiej – wprowadzenie

Information Warfare as an Instrument of the Foreign Policy of the Russian Federation—Introduction

Jacek Kiera*

Abstrakt
Wojna informacyjna stała się ważnym elementem polityki zagranicznej państw nie tylko w trakcie otwartego konfliktu zbrojnego, lecz przede wszystkim w czasie poprzedzającym jego rozpoczęcie. Celem niniejszego artykułu jest zidentyfikowanie i scharakteryzowanie wojen informacyjnych prowadzonych przez Federację Rosyjską z uwzględnieniem ich roli jako narzędzia polityki zagranicznej. Temat ten został przedstawiony zarówno w wymiarze teoretycznym, jak i poprzez omówienie wybranych przykładów. W pracy wykorzystano analizę treści, analizę krytyczną źródeł oraz syntezę i opis, aby zweryfikować przyjętą hipotezę badawczą, zgodnie z którą wojna informacyjna stała się systemowym instrumentem polityki zagranicznej Kremla, mającym na celu destabilizację

Abstract
Information warfare has become an important element of state's foreign policy not only during an open armed conflict, but especially in the time leading up to it. The purpose of this article is to identify and characterise information warfare conducted by the Russian Federation, taking into account its role as a part of its foreign policy. The topic has been presented both in the theoretical dimension and by discussing selected examples. Content analysis, critical analysis of sources as well as synthesis and description were used in this thesis to verify the adopted research hypothesis, according to which information warfare has become a systemic instrument of the Kremlin's foreign policy, conducted with the aim of destabilising states internally, deepening divisions between participants of international

* Szkoła Doktorska Uniwersytetu Śląskiego w Katowicach; https://orcid.org/0000-0002-6372-6867; jacek.kiera@us.edu.pl

wewnętrzną państw, antagonizowanie uczestników stosunków międzynarodowych oraz realizowanie własnych interesów w sferze zewnętrznej.

Słowa kluczowe: polityka zagraniczna Federacji Rosyjskiej, wojna informacyjna, konflikty międzynarodowe, propaganda, dezinformacja, cyberataki

affairs and pursuing its own interests in the external dimension.

Keywords: Russian Federation foreign policy, information warfare, international conflicts, propaganda, disinformation, cyberattacks

Wstęp

Zjawisko wojny informacyjnej stało się niezwykle ważnym zagadnieniem z uwagi na trwający od lutego 2022 r. konflikt rosyjsko-ukraiński, choć samo w sobie ma o wiele dłuższą historię, sięgającą co najmniej okresu zimnej wojny oraz działań podejmowanych w tym zakresie przez Związek Socjalistycznych Republik Radzieckich (ZSRR). Wojnę informacyjną należy utożsamiać ze wzrostem znaczenia szeroko pojętej informacji w stosunkach międzynarodowych, która jest traktowana jako zasób o charakterze strategicznym (Aleksandrowicz, 2018, s. 33–41) i z którą wiążą się różnego rodzaju zagrożenia polegające na jej potencjalnym szkodliwym zastosowaniu. Użyta jako broń, cechuje się niskim kosztem wytworzenia, uniwersalnym charakterem, łatwą dostępnością i nieograniczonym zasięgiem. Przede wszystkim nie uznaje granic państwowych, a jej kontrola w dzisiejszym społeczeństwie informacyjnym[1] stała się w dużym stopniu utrudniona, by nie powiedzieć: niemożliwa (szerzej zob. Darczewska, 2014, 2015).

W odniesieniu do Federacji Rosyjskiej można zauważyć, że w kontekście postępującej rewolucji w świecie cyfrowym Rosja bywa bardzo często postrzegana jako państwo zacofane i do niej całkowicie nieprzystosowane. Jest to jednak założenie zupełnie błędne. Już w 1961 r. Rada Cybernetyczna Akademii Nauk w Moskwie przedłożyła opracowanie pt. *Cybernetyka na usługach komunizmu*, w którym proponowano stworzenie regionalnych ośrodków informatycznych wykorzystujących komputery do przygotowywania statystyk i planowania zadań, co miało skutkować zwiększeniem szybkości podejmowania decyzji przez kadry kierownicze. Z kolei Slava Gerovitch pisał, iż w latach 70. XX w. pośród amerykańskiej administracji rządowej panowała obawa, że Związek Radziecki posiada zaawansowany system zarządzania oparty na sieci komputerów

[1] Społeczeństwo informacyjne można zdefiniować jako społeczeństwo, w którym informacja będąca zasobem o charakterze niematerialnym jest równie ważna co zasoby o charakterze materialnym i staje się jednocześnie istotnym ogniwem w gospodarce danego państwa.

SOVNET, który rzekomo znacznie wyprzedzał pod względem technologicznym amerykański ARPANET, znany dziś pod nazwą Internet (Harrel, 2015, s. 63; szerzej zob. Gerovitch, 2002). Decydenci polityczni na Kremlu, zdając sobie sprawę z ogromnej roli cyberprzestrzeni oraz możliwości, jakie stwarzał jej rozwój, zbudowali podwaliny, z których współcześnie korzysta Federacja Rosyjska.

Aktywność Związku Radzieckiego w okresie zimnej wojny obejmowała ponadto prowadzenie kampanii oddziaływania informacyjnego, zarówno na obywateli ZSRR i krajów satelickich, jak i na obywateli państw obcych oraz wrogich ideom komunizmu. Kreml finansował przedsięwzięcia, które wyrażały krytykę wobec szeroko rozumianego Zachodu, a także promował tam idee społeczeństwa socjalistycznego. W tym celu wspierano antyzachodnie ruchy pokojowe czy też zapraszano myślicieli i artystów z krajów kapitalistycznych do Związku Radzieckiego, aby ukazywali go jako państwo pod każdym względem przewyższające cywilizację zachodnią (Banasik, 2021b, s. 110). Służby specjalne, z KGB[2] na czele, prowadziły kampanie oddziaływania informacyjnego, takie jak operacja Infektion z 1983 r., w ramach której indyjska gazeta „The Patriot", sponsorowana przez służby rosyjskie, opublikowała artykuł oskarżający amerykańskie władze o stworzenie wirusa HIV i wykorzystywanie go w charakterze broni. W 1987 r. wiadomość ukazała się ponad 40 razy w prasie kontrolowanej przez Związek Radziecki, została przedrukowana lub nadana w ponad 80 krajach i w 30 językach (Lucas i Pomeranzev, 2016, s. 17; Rid, 2022, s. 369–415). Innym przykładem mogą być próby skompromitowania amerykańskiego prezydenta Ronalda Reagana czy papieża Jana Pawła II (Aleksandrowicz, 2016, s. 93).

Przytoczone przykłady stanowią tylko drobny wycinek działalności rosyjskich służb specjalnych, a jeśli wierzyć słowom Jurija Biezmienowa, zbiegłego radzieckiego oficera wywiadu KGB, w okresie zimnowojennym tylko 15% środków finansowych wywiadu ZSRR przeznaczano na aktywność szpiegowską, z kolei pozostałą część, tj. 85%, na potrzeby tzw. przewrotu ideologicznego czy też po prostu dywersji (River, 2020, s. 10–12). Działalność ta była głównym rodzajem prowadzonych akcji wywrotowych o charakterze agitacyjno-propagandowym oraz wywiadowczo-organizacyjnym (Wojnowski, 2015a, s. 20–21). Należy również zauważyć, że pojęcie dywersji w terminologii radzieckiej oznacza odwracanie uwagi od wrogiej działalności wobec państwa lub ludności

[2] KGB (Komitet Bezpieczeństwa Państwowego przy Radzie Ministrów ZSRR) – jedna z najważniejszych służb specjalnych ZSRR, odpowiedzialna m.in. za prowadzenie działań wywiadowczych i kontrwywiadowczych w kraju i za granicą, inwigilację ludności, działania dezinformacyjne oraz zwalczanie opozycji politycznej. Rozwiązana w 1991 r. po upadku ZSRR i przekształcona w Federacji Rosyjskiej w służby takie jak Służba Wywiadu Zagranicznego Federacji Rosyjskiej, Federalna Służba Bezpieczeństwa Federacji Rosyjskiej oraz Federalna Służba Ochrony Federacji Rosyjskiej. W skład KGB wchodził Zarząd V odpowiedzialny m.in. za walkę ideologiczną.

(River, 2020, s. 10–12), podczas gdy w ujęciu zachodnim United States Department of Defense (2021, s. 66) w *DOD Dictionary of Military and Associated Terms* odnosi ten termin przede wszystkim do szeroko rozumianych akcji sabotażowych – wojskowych oraz odwracających uwagę od rzeczywistego przeciwnika. Rozpad ZSRR z oczywistych względów zrewidował działania podejmowane przez Rosję w globalnej przestrzeni informacyjnej, jednakże ich charakter co do zasady pozostał niezmieniony. Uzasadnione jest zatem twierdzenie, że rosyjska wojna informacyjna posiada trwałe cechy wypracowane w ciągu dziesiątków lat, cechy, które ewoluowały w systemie ustrojowym Związku Radzieckiego, a obecnie ewoluują w systemie ustrojowym Federacji Rosyjskiej (szerzej zob. Darczewska, 2014).

Rosyjskie koncepcje wojny informacyjnej

Termin „wojna informacyjna" nie doczekał się jednej definicji powszechnie akceptowanej przez badaczy w państwach zachodnich. Przykładowo Dorothy E. Denning wskazuje, że są to działania, które mają na celu „zdobycie lub wykorzystanie zasobów informacyjnych" (Denning, 2002, s. 23). Według Martina C. Libickiego jest to „ciąg działań wywołanych potrzebą modyfikacji przepływu informacji kierowanych do drugiej strony przy jednoczesnej ochronie własnych; takie działania obejmują atak fizyczny, atak radioelektroniczny, ataki na systemy i czujniki, kryptografię, ataki na komputery i operacje psychologiczne"[3] (Ventre, 2016, s. 4), z kolei Vladimir Volkoff formułuje pogląd, zgodnie z którym wojna informacyjna oznacza „ofensywne i defensywne używanie informacji i systemów informacyjnych, by wykorzystywać, psuć i niszczyć informacje i systemy informacyjne przeciwnika, chroniąc zarazem własne informacje i własne systemy" (Volkoff, 2022, s. 235–236). Thomas Rona natomiast uważa, że chodzi o „rywalizację na poziomie strategicznym, operacyjnym i taktycznym w całym spektrum pokoju, kryzysu, eskalacji kryzysu, konfliktu, wojny, zakończenia wojny i rekonstrukcji/odbudowy, prowadzoną między konkurentami, przeciwnikami lub wrogami przy użyciu środków informacyjnych i służącą osiągnięciu swoich celów" (Libicki, 1995, s. 4). Wszystkie przytoczone definicje zawierają pewne elementy wspólne i można stwierdzić, że odnoszą się głównie do działalności militarnej. Jednakże ostatni z przywołanych autorów traktuje wojnę informacyjną zdecydowanie szerzej, nie ogranicza jej wyłącznie do operacji zbrojnych. W tym kontekście można wskazać największe odmienności

[3] Wszystkie teksty nieprzetłumaczone wcześniej na język polski są cytowane w przekładzie autora.

pomiędzy definicjami zachodnimi wojny informacyjnej a jej definicjami występującymi w rosyjskiej literaturze przedmiotu.

Sun Tzu napisał, że „osiągnąć sto zwycięstw w stu bitwach nie jest szczytem osiągnięć. Największym osiągnięciem jest pokonanie wroga bez walki. […] Dlatego najwyższą sztuką jest zwyciężyć armię wroga bez wydania bitwy. Zająć miasto wroga bez oblegania i zająć tereny jego państwa bez inwazji" (Sun Tzu, 1994, s. 35). Cytat ten po ponad 2500 latach nadal pozostaje aktualny. Z rozważań chińskiego myśliciela niewątpliwie czerpał Jewgienij Messner[4], którego poglądy stanowiły podwaliny pod współczesne rosyjskie koncepcje wojen informacyjnych. Sformułował on teorię tzw. wojen buntowniczych i sklasyfikował ich cele w następującej hierarchii: „1) zniszczenie morale ludności przeciwnika, 2) pokonanie aktywnych jednostek (wojska, partyzantów, walczących ruchów ludowych), 3) zagarnięcie lub zniszczenie przedmiotów o wartości psychologicznej, 4) zagarnięcie lub zniszczenie przedmiotów o wartości materialnej, 5) osiągnięcie efektów zewnętrznych w postaci znalezienia nowych sojuszników i zaszkodzenia duchowi sojuszników przeciwnika" (Messner, 2005, s. 132)[5]. Zauważył też, że w tym samym czasie należy dążyć do „a) ochrony morale swojego narodu, b) ochrony swojej aktywnej siły wojskowej, c) obrony psychologicznie lub życiowo niezbędnych obiektów oraz d) unikania wszystkiego, co mogłoby wywołać nieprzychylną reakcję w państwach neutralnych, ale będących przedmiotem naszego zainteresowania" (Messner, 2005, s. 132)[6]. Odchodzi się tu więc od tradycyjnego postrzegania przeciwnika, czyli utożsamiania go z siłami zbrojnymi danego państwa, na rzecz społeczeństwa i występującego w nim konfliktu w sferze ludzkiej świadomości (Kiera, 2019,

[4] Jewgienij Messner był pułkownikiem Armii Imperium Rosyjskiego oraz Białej Armii (złożonej ze zwolenników caratu). Po rozpoczęciu rewolucji bolszewickiej w 1917 r. brał udział w walkach z komunistami w szeregach Białej Armii, a następnie musiał wyemigrować do Belgradu, gdzie od 1931 r. wykładał w akademii wojskowej. Po zajęciu Królestwa Jugosławii przez III Rzeszę i rozpoczęciu wojny z ZSRR wstąpił do Wehrmachtu, gdzie służył w 1. Rosyjskiej Armii Narodowej (formacji kolaborującej z Niemcami), pełniąc funkcję oficera propagandy. W 1945 r. został internowany w Liechtensteinie, a dwa lata później wyemigrował do Argentyny. Posiadał stopień naukowy doktora i tworzył prace dotyczące teorii wojskowości, przede wszystkim *Oblicze współczesnej wojny* (1959), *Miatież – nazwa III wojny światowej* (1960), *Współcześni oficerowie* (1961), *Ogólnoświatowa miatieżewojna* (1971).

[5] Tekst w oryginale: „1) развал морали вражеского народа, 2) разгром его активной части (воинства, партизанства, борющихся народных движений), 3) захват или уничтожение объектов психологической ценности, 4) захват или уничтожение объектов материальной ценности, 5) эффекты внешнего порядка ради приобретения новых союзников, потрясения духа союзников врага".

[6] Tekst w oryginale: „а) к сбережению морали своего народа, б) к сбережению своей активной, воюющей силы, в) к обороне психологически или жизненно необходимых объектов и г) к избежанию всего, что даст неблагоприятный отклик в государствах нейтральных, но для нас интересных".

s. 162–164). Zasadniczym celem wojen buntowniczych jest zdobycie duszy wrogiego narodu, stąd „istotną rolę odgrywają w ni[ch] dziennikarze, dywersanci, prowokatorzy, propagandyści, a pojęcie linii frontu w takiej wojnie odnosi się do poszczególnych sfer aktywności danego społeczeństwa" (Aleksandrowicz, 2021, s. 103). Można z całą pewnością uznać, że koncepcje Messnera są obecne we współczesnych założeniach rosyjskich wojen informacyjnych, traktowanych jako instrument polityki zagranicznej Kremla.

Wreszcie należy wskazać, że podstawową różnicę w definicjach pojęcia wojny informacyjnej w wydaniu rosyjskim oraz zachodnim stanowi cel, jaki ma ona realizować. Ponadto teorie rosyjskie, choć powstały dawno, cechuje dynamiczność – nieustannie ewoluują i dostosowują się do zmieniającego się otoczenia międzynarodowego. Prowadzone przez Kreml kampanie oddziaływania informacyjnego i szerzona w ich ramach propaganda *sensu largo* odróżniają się od tradycyjnych ich wyobrażeń i koncepcji, jakie znamy na Zachodzie. Edward Lucas i Peter Pomeranzev piszą, że w Rosji takie kampanie nazywane są wojnami informacyjno-psychologicznymi, a ich celem „nie jest przekonanie czy perswazja, ale raczej podważenie. Zamiast pobudzać odbiorców do działania, usiłuje się utrzymać ich w stanie zawieszenia i dekoncentracji, pasywności, paranoi. […] Owa taktyka jest stosowana po to, aby zdezorganizować i zdemoralizować przeciwnika. Walka toczy się w sferze percepcji i umysłów ludzkich. Trwa zarówno w czasie oficjalnego pokoju, jak i w czasie wojny. Rosyjska dezinformacja jest rozpowszechniana zarówno jawnie – za pośrednictwem obcojęzycznej telewizji (zwłaszcza wielojęzycznej RT) i samozwańczej agencji informacyjnej Sputnik International – jak i potajemnie, z pomocą pozornie niezależnych dziennikarzy, ekspertów i komentatorów" (Lucas i Pomeranzev, 2016, s. 5)[7]. Natomiast Jolanta Darczewska, omawiając kwestie związane z definicją „wojny informacyjnej" w ujęciu rosyjskim, zaznaczyła, że „nie mieszczą się one w żadnej z definicji terminów przyjętych na Zachodzie. Terminy »wojna cybernetyczna«, »wojna informacyjna« czy »wojna sieciowa« mają w Rosji zdecydowanie odmienny zakres pojęciowy. Tylko nieliczni teoretycy rozróżniają *cyberwar* i *netwar*, przeciwstawiając technologiczny i społeczny wymiar wojen IV generacji. Dotyczy to jednak z reguły publikacji omawiających zachodnią literaturę przedmiotu; w zdecydowanej większości rosyjscy autorzy pod pojęciem »wojna informacyjna« rozumieją oddziaływanie na masową świadomość

[7] Tekst w oryginale: „Its aim is not to convince or persuade, but rather to undermine. Instead of agitating audiences into action, it seeks to keep them hooked and distracted, passive and paranoid. […] It is a tactic used to disorganize and demoralize an opponent. It is fought in the realms of perception and the minds of men. It continues through both official peace and wartime. Russian disinformation is disseminated both overtly though foreign-language television (notably the multilingual RT) and the self-styled news agency Sputnik International and covertly, using notionally independent journalists, experts and commentators".

w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, a używane w charakterze »broni informacyjnej«. Niejako z definicji mieszają w ten sposób porządek militarny z pozamilitarnym" (Darczewska, 2014, s. 12).

Przytoczone twierdzenia skłaniają więc do wniosku, że rosyjskie definicje nie tyle nie są tożsame ze swoimi zachodnimi odpowiednikami, ile wręcz nie powinny być z nimi w ogóle zestawiane. W tym kontekście Keir Giles zauważył, że „w haśle »wojna informacyjna« (*informatsionnaya voyna*) w glosariuszu kluczowych terminów z zakresu bezpieczeństwa informacyjnego opracowanym przez Akademię Wojskową Sztabu Generalnego wyraźnie odróżniono definicję rosyjską – wszechstronną i nieograniczoną do czasu wojny – od zachodniej – ograniczonych, taktycznych operacji informacyjnych prowadzonych podczas działań wojennych" (Giles, 2016b, s. 2)[8]. Istotne ustalenia poczynił Robert Bebber, który usystematyzował kremlowskie oddziaływanie informacyjne i wyróżnił takie jego elementy jak: a) wpływanie przy pomocy dyplomatów, wynajętych „ekspertów" i naukowców na opinie ludności danego kraju i na postrzeganie przez nią rzeczywistości; b) wykorzystanie operacji informacyjnych, aby kontrolować przekaz; c) ofensywne operacje cybernetyczne przeciwko komputerom i systemom komunikacyjnym (Bebber, 2016, s. 44). Warto podkreślić, że przedstawiona charakterystyka nie dotyczy wyłącznie sfery militarnej aktywności państwa, wręcz przeciwnie – wychodzi w znacznej mierze poza nią. Ponadto bardzo widoczne jest traktowanie wojny informacyjnej w ujęciu rosyjskim jako zarówno oddziaływania informacyjnego na odbiorców, jak i dokonywania cyberataków, a operacje te są wobec siebie komplementarne. Bebber stwierdził również – co niezwykle ważne – że Rosjanie wykorzystują informacje do „dezorientacji, paraliżu i przewrotu, w przeciwieństwie do amerykańskiego/zachodniego modelu, w którym wykorzystuje się informacje do przekonywania" (Bebber, 2016, s. 44)[9]. Zakładają oni prowadzenie działań z zakresu oddziaływania informacyjnego przede wszystkim poza otwartym konfliktem zbrojnym (Giles i Seaboyer, 2019, s. 5). Dochodzi tutaj zatem do swoistego przemieszania porządku militarnego z porządkiem pozamilitarnym (Darczewska, 2014, s. 12), wskutek czego wojna informacyjna w ujęciu rosyjskim będzie realizować takie same cele, jakie są osiągane w wyniku wojny konwencjonalnej, z tym że na innej płaszczyźnie (Modrzejewski, 2018, s. 106). O ile badacze zachodni ograniczają się do

[8] Tekst w oryginale: „The entry for »Information war« (*informatsionnaya voyna*) in a glossary of key information security terms produced by the Military Academy of the General Staff makes a clear distinction between the Russian definition – all-encompassing, and not limited to wartime – and the Western one – limited, tactical information operations carried out during hostilities".

[9] Tekst w oryginale: „confuse, paralyze, and subvert, unlike the American/Western model, which uses information to persuade".

upatrywania wojny informacyjnej głównie w sferze militarnej (np. w dostarczaniu sfabrykowanych lub błędnych informacji dowódcom wojsk przeciwnika czy paraliżowaniu wojskowych systemów teleinformatycznych), o tyle Rosjanie rozszerzają działania tego rodzaju m.in. o sferę polityki, wywiadu, dyplomacji, propagandy, psychologii, edukacji, kultury czy religii (Banasik, 2021b, s. 56; Darczewska, 2014, s. 10; Giles, 2016b, s. 2).

Wojna informacyjna jako instrument polityki zagranicznej Rosji

Znaczenie informacji, a w konsekwencji – wojny informacyjnej, jako instrumentu polityki zagranicznej Kremla wynika z założeń formułowanych w dokumentach rządowych, stanowiących trzon polityki zagranicznej realizowanej przez Rosję. Należy więc wymienić chociażby najważniejsze zagadnienia poruszone w *Doktrynie bezpieczeństwa informacyjnego Federacji Rosyjskiej* z 2016 r. W dokumencie zwrócono uwagę na ogromny wzrost roli informacji postrzeganej jako nieodłączny element życia politycznego, społecznego i ekonomicznego państw. Do największych zagrożeń zaliczono z kolei ukazywanie przez media zachodnie w globalnej przestrzeni informacyjnej stronniczych treści na temat polityki zagranicznej Rosji, dyskryminację rosyjskich dziennikarzy oraz negatywne oddziaływanie informacyjne na mieszkańców Rosji (Prezident Rossijskoj Federacii, 2016a). Innym dokumentem wartym przywołania jest *Koncepcja polityki zagranicznej Federacji Rosyjskiej*, również z 2016 r., w której – mając na względzie rzeczone zagrożenia – ujęto wprost cel Rosji polegający na „wzmocnieniu pozycji rosyjskich środków masowego przekazu i masowej komunikacji w globalnej przestrzeni informacyjnej oraz dotarciu do szerokich kręgów społeczności międzynarodowej z rosyjskim punktem widzenia na procesy międzynarodowe" (Prezident Rossijskoj Federacii, 2016b). Ponadto podkreślono znaczenie ideologii rosyjskiego świata, czyli tzw. ruskiego miru[10], który ma stanowić jeden z filarów polityki zagranicznej prowadzonej przez Kreml. Wreszcie

[10] Ideologia ruskiego miru, zwana również ideologią rosyjskiego świata, oznacza restaurację „świadomości mocarstwowej, wyobrażenia o dawnej, świetnej przeszłości, łączącej różne narody wokół kultury rosyjskiej i więzi z Rosją […]. […] *ruski mir* ma zasadniczo obronny charakter, zmierzający do ochrony rosyjskiego interesu narodowego, nieodłącznie związanego przede wszystkim z »bliską granicą« […], pozostając koncepcją zorientowaną na obronę rosyjskiego interesu narodowego. Od czasu do czasu *ruski mir* przyjmuje charakter bardziej ekspansywny (odpowiedź na atak Gruzji w 2008 r., aneksja Krymu, zaangażowanie w konflikt na wschodzie Ukrainy), będąc reakcją na sytuację międzynarodową w najbliższym środowisku geopolitycznym Federacji Rosyjskiej. W rosyjskim rozumieniu jest to wtedy również obrona, ale staje się ona jedynie bardziej aktywna niż ekspansywna" (Wierzbicki, 2015, s. 135–136).

w *Strategii bezpieczeństwa narodowego Federacji Rosyjskiej* z 2021 r. określono główne zagrożenia dla interesów kraju – do istotniejszych zaliczono politykę Zachodu, przede wszystkim USA. W kontekście bezpieczeństwa informacyjnego zauważono, że globalna przestrzeń informacyjna jest zagospodarowywana jako nowa sfera działań wojennych, a „dywersje informacyjne i psychologiczne oraz »westernizacja« kultury zwiększają zagrożenie utraty suwerenności kulturowej przez Federację Rosyjską" (Prezident Rossijskoj Federacii, 2021). W 2022 r. przyjęto wspólną doktrynę wojenną Państwa Związkowego Rosji i Białorusi, zakładającą jeszcze szersze wykorzystanie środków z zakresu wojny informacyjnej wobec wrogich państw (Dyner, 2022).

Przytoczone wyżej sformułowania potwierdzają istnienie wciąż żywego tzw. syndromu oblężonej twierdzy, który pamięta czasy Związku Socjalistycznych Republik Radzieckich. Syndrom ten, polegający na postrzeganiu otoczenia państwa jako kręgu wrogich podmiotów dążących do jego anihilacji (Ziółkowski, 2016, s. 171; szerzej zob. Ziółkowski, 2019), często przejawia się w wypowiedziach najwyższych władz Kremla. Na przykład Szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej generał Witalij Gierasimow oświadczył, że Zachód prowadzi zmasowaną kampanię oddziaływania informacyjnego przeciwko Rosji, która to kampania zmierza do zakwestionowania wizerunku Federacji jako państwa walczącego z terroryzmem międzynarodowym oraz zaangażowanego w rozwiązywanie sporów międzynarodowych (Modrzejewski, 2018, s. 109). Przywołane sformułowanie Gierasimowa nie jest przypadkowe, albowiem to właśnie on stworzył doktrynę nazwaną jego imieniem, przedstawioną w styczniu 2013 r. na Konferencji Nauk Wojskowych w Moskwie. Doktryna Gierasimowa zakłada podjęcie wszelkich działań zbrojnych dopiero po osłabieniu przeciwnika, głównie w wyniku przeprowadzonych uprzednio, w czasie pokoju, operacji sił specjalnych i zastosowania środków właściwych dla wojny informacyjnej (kampanii oddziaływania informacyjnego oraz cyberataków). Należy zatem wykorzystywać środki informacyjne, psychologiczne, dyplomatyczne i ekonomiczne w celu osłabienia wroga, co z kolei ułatwi agresję zbrojną. Nie bez znaczenia pozostaje tutaj oddziaływanie informacyjne polegające na stosowaniu technik propagandowych i różnych form agitacji (Wojnowski, 2015b, s. 28–31). Omawiana koncepcja bardzo wyraźnie nawiązuje więc do teorii tzw. wojen buntowniczych Messnera. Trzeba dodać, że w literaturze przedmiotu znajdziemy również poglądy, iż „doktryna Gierasimowa" nie jest tak naprawdę nowym zjawiskiem, a sporo obserwatorów i badaczy nadaje jej o wiele wyższą rangę, niż na to zasługuje (szerzej zob. Giles, 2020).

Koncepcje wojen informacyjnych w ujęciu rosyjskim mają także bardzo silne zaplecze teoretyczne w poglądach badaczy, do których czołówki zaliczamy Igora Panarina oraz Aleksandra Dugina. Pierwszy z nich w swojej pracy zatytułowanej *Druga światowa wojna informacyjna – wojna przeciwko Rosji* wskazywał, że wszystkie tzw. kolorowe rewolucje czy też arabska wiosna były

efektem kampanii psychologiczno-informacyjnych przygotowanych i zrealizowanych przez Zachód. Dlatego według niego „narodowy system walki informacyjnej, polegający na jawnym i tajnym sterowaniu procesami komunikacyjnymi, musi być adekwatny do współczesnych realiów globalnych. Oparty na najlepszych doświadczeniach ZSRR, winien być wzbogacony o doświadczenia USA i Chin" (Darczewska, 2014, s. 16). Panarin zauważył również, że na całym świecie trwa konfrontacja informacyjna, i wyróżnił takie jej elementy jak: strategiczna analiza polityczna (uzyskanie informacji), wpływ na informacje (ich blokowanie, przetwarzanie, wymiana i modyfikowanie) i opór informacyjny (obrona przed wrogimi działaniami) (Wrzosek, Markiewicz i Modrzejewski, red., 2019, s. 109).

Z kolei Dugin opracował teorię tzw. wojny sieciowej, czyli zdobywania przewagi w konfrontacji informacyjnej (o której pisał także Panarin) prowadzonej z innymi państwami w globalnej przestrzeni informacyjnej. Aby tego dokonać, konieczne są działania agitacyjno-propagandowe oraz wywiadowczo-organizacyjne, polegające na „tworzeniu, finansowaniu i kierowaniu działalnością różnego rodzaju organizacji i nielegalnych grup opozycyjnych w celu uzyskania wpływu na szerokie sfery działalności politycznej i społecznej w innych państwach. Jest to realizowane m.in. przez jawne lub tajne wykupywanie lokalnych mediów, indoktrynowanie ekspertów, dziennikarzy i przedstawicieli różnych środowisk politycznych, a następnie przekształcanie ich w świadomą lub nieświadomą agenturę wpływu, co odbywa się na prestiżowych konferencjach naukowych" (Wojnowski, 2017, s. 30). Warto przywołać też poglądy jeszcze jednego teoretyka, Siergieja Rastorgujewa[11] z Instytutu Problemów Bezpieczeństwa Informacyjnego Uniwersytetu Łomonosowa w Moskwie, który zrównał kategorię celów osiąganych dzięki wojnom informacyjnym z celami osiąganymi podczas wojen konwencjonalnych. Stwierdził, że wojny konwencjonalne toczą się o zasoby państw, natomiast wojny informacyjne – o zasoby społeczne. Kluczem do ich wygrania są, w jego ocenie, elity polityczne i media przeciwnika, pośród których trzeba mieć dostateczną liczbę agentów wpływu, aby skutecznie realizować wyznaczone zadania (Modrzejewski, 2018, s. 106).

Prowadząc wojny informacyjne, Federacja Rosyjska stosuje wiele środków oddziaływania informacyjnego na odbiorców, a ich rodzaj jest determinowany przede wszystkim posiadanymi w tym zakresie możliwościami. Należy tu wyróżnić kilka najczęstszych środków, które zostaną dalej omówione (ich katalog oczywiście nie ma charakteru enumeratywnego): tzw. farmy trolli, fałszywe konta na portalach Facebook i Twitter oraz na komunikatorze Telegram, działalność portali informacyjnych, a także cyberataki.

[11] Siergiej Rastorgujew – rosyjski pułkownik Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej oraz były zastępca naczelnika Instytutu Naukowo-Badawczego Technologii Informacyjnych FSB.

Pierwszy – i być może nawet najbardziej znany – środek rosyjskich kampanii oddziaływania informacyjnego stanowią „farmy trolli". Najpopularniejsze z nich, tzw. Trolle z Olgino[12], są pracownikami Agencji Badań Internetowych z siedzibą w Sankt Petersburgu (Rid, 2022, s. 529–547). Agencja jest silnie powiązana z rosyjskim rządem, a samo przedsiębiorstwo zostało założone w 2013 r. przez Jewgienija Prigożyna, bliskiego współpracownika Władimira Putina. Codzienna działalność „trolli" polega na posługiwaniu się fałszywymi kontami, głównie na portalach społecznościowych, ale również na witrynach internetowych i forach dyskusyjnych, w celu publikowania treści zgodnych z wytycznymi Kremla (Wojnowski, 2019, s. 30). Trolling nie ogranicza się wyłącznie do działań ludzi, lecz obejmuje też wykorzystanie tzw. botów. Są to programy, które przeszukują Internet i w sposób automatyczny odpowiadają na wybrane komentarze czy wiadomości na podstawie wykrytych w nich słów kluczowych (Giles, 2016a, s. 54–60), a także mogą rozpowszechniać sfabrykowane treści (Palczewski, 2019). Max Seddon omówił dzień pracy „rosyjskiego trolla" na przykładzie Agencji Badań Internetowych i wskazał, że ma on za zadanie codziennie opublikować co najmniej 50 artykułów informacyjnych oraz prowadzić 6 kont na Facebooku, gdzie powinien publikować minimum 3 posty i dyskutować w grupach minimum 2 razy w ciągu dnia. Stosując te zasady, przeciętny „troll" do końca pierwszego miesiąca pracy zdobędzie w przybliżeniu 500 subskrybentów i będzie otrzymywał ok. 5 komentarzy dziennie. W przypadku Twittera pracownicy mają administrować maksymalnie 10 kontami, posiadać nie więcej niż 2 tysiące odbiorców i tweetować co najmniej 50 razy na dobę (Seddon, 2014). Jako inny przykład można przywołać relacje Marata Mindijarowa, zatrudnionego w Agencji od listopada 2014 r. do lutego 2015 r., pracującego na 12-godzinnych zmianach i zobowiązanego codziennie do napisania 135 komentarzy po 200 znaków (Rid, 2022, s. 534).

Następnie należy przedstawić zjawisko wykorzystywania kont na portalach Facebook i Twitter oraz na komunikatorze Telegram, przy których tworzeniu podaje się fikcyjne dane użytkowników. Ten typ środka prowadzenia wojen informacyjnych jest bezpośrednio związany z uprzednio omówionym, ponieważ właśnie za pomocą m.in. tych mediów działają „trolle" oraz boty. Warto zauważyć, że w okresie istnienia ZSRR takie instrumenty nie były dostępne, z kolei dziś stanowią niezwykle proste i tanie narzędzie oddziaływania w globalnej przestrzeni informacyjnej (Savranska, 2020, s. 86). O ile w czasach ZSRR służby specjalne z KGB na czele musiały podjąć wiele skomplikowanych działań, by ich propaganda przedostała się do zachodnich mediów, o tyle obecnie dzięki Internetowi zdolności rosyjskie w tym zakresie są w zasadzie wręcz nieograniczone (Weiss i Pomerantsev, 2014, s. 17). Dokładne ustalenie liczby kont

[12] Olgino – przedmieścia Sankt Petersburga (wieś), gdzie znajduje się siedziba Agencji Badań Internetowych.

zakładanych na portalach społecznościowych nie jest możliwe, jednakże kilka przykładów dobitnie zobrazuje skalę problemu. Po rozpoczęciu wojny rosyjsko-ukraińskiej Meta poinformowała, że w ciągu 48 godzin zlokalizowano i zlikwidowano sieć złożoną z ok. 40 kont na Facebooku rozsiewających rosyjską propagandę, które miały łącznie ok. 5000 obserwujących, z czego ok. 500 na Instagramie (Collins i Ling Kent, 2022; Gleicher, 2022). Liczba ta może nie robić stosunkowo dużego wrażenia, ale wiadomość o zlikwidowaniu przez Ukrainę „farmy botów" obejmującej ponad milion kont i grup w sieciach społecznościowych z prawie 400 tysiącami odbiorców ukazuje rozmiar zjawiska oraz możliwości rosyjskich służb specjalnych w zakresie kampanii oddziaływania informacyjnego na użytkowników Internetu (Interfax-Ukraine, 2022).

Kolejnym środkiem są portale informacyjne, które publikują sfabrykowane treści w Internecie, i to nie tylko w języku rosyjskim, lecz także po angielsku lub w języku państwa, do którego społeczeństwa kierowany jest dany komunikant. Cel Kremla stanowi dotarcie z rosyjskim punktem widzenia do jak największej grupy odbiorców, a jego osiągnięcie wymaga tworzenia podmiotów medialnych takich jak telewizje czy portale informacyjne (Prezident Rossijskoj Federacii, 2016b) – doskonałymi przykładami mogą być RT[13] czy Sputnik News[14]. Serwis NewsGuard zidentyfikował 645 portali szerzących dezinformację na temat agresji Rosji w Ukrainie, z czego 341 publikuje w języku angielskim, 61 we francuskim, 53 w niemieckim, 45 we włoskim, a 145 w innych językach (NewsGuard, 2024). Z kolei w polskiej przestrzeni informacyjnej portal OKO.press zidentyfikował 43 polskojęzyczne podmioty propagujące rosyjski punkt widzenia na wskazany konflikt, w tym 27 portali informacyjnych, 11 blogów oraz 5 niszowych platform społecznościowych i serwisów (Mierzyńska, 2022). Należy zaznaczyć, że przedstawione dane obejmują tylko wycinek ogromnej machiny medialnej zbudowanej przez służby specjalne Federacji Rosyjskiej.

Dotychczasowe rozważania prowadzą do wniosku, że propaganda odgrywa istotną rolę w rosyjskiej wojnie informacyjnej. Jedną z najbardziej znanych definicji tego terminu zaproponował pionier *public relations* Edward L. Bernays, według którego jest ona „konsekwentnym, trwałym wysiłkiem tworzenia lub kształtowania wydarzeń w celu wpłynięcia na stosunek społeczeństwa do jakiegoś przedsięwzięcia, idei lub grupy" (Bernays, 1928, s. 25). William W. Bidelle natomiast zauważył, że „pod wpływem propagandy każda jednostka zachowuje się tak, jak gdyby jej reakcje były wynikiem jej własnej decyzji. Wiele jednostek można zmusić do takiego samego zachowania, przy czym każdą pozornie kierują jej własne sądy" (Dobek-Ostrowska, 2007, s. 204). Z kolei zdaniem

[13] RT – działająca od 2005 r. ogólnoświatowa wielojęzyczna rosyjska telewizja informacyjna, prowadząca również portal informacyjny pod tą samą nazwą (do 2009 r. pn. Russia Today).

[14] Sputnik News – rosyjska rządowa agencja informacyjna powstała w 2014 r., prowadząca wielojęzyczny portal informacyjny, w tym w języku polskim.

Jacques'a Ellula „propaganda" oznacza „zestaw metod stosowanych przez zorganizowaną grupę chcącą spowodować, by czynny lub bierny udział w jej działaniach wzięły ludzkie masy, wśród których dochodzi do wytworzenia jedności psychicznej wskutek manipulacji i włączenia do organizacji" (Ellul, 1973, s. 61). Po zakończeniu II wojny światowej omawiany termin zaczął być rzadziej używany, również w środowisku naukowym, z uwagi na jego negatywne konotacje – zamiast tego wprowadzono pojęcie „komunikowanie polityczne", które miało bardziej neutralny charakter (Dobek-Ostrowska, Fras i Ociepka, 1997, s. 32). Nie zmienia to jednak faktu, że propaganda, bez względu na nazewnictwo, nadal pozostaje propagandą. Wydaje się, że doskonale rozumieją to Rosjanie, którzy czerpiąc ze swoich bogatych doświadczeń historycznych, wykorzystują ją jako instrument kampanii oddziaływania informacyjnego.

Wreszcie należy omówić ostatni z instrumentów, czyli cyberataki. Ich zasadniczą rolą w kontekście oddziaływania informacyjnego jest wspieranie kampanii prowadzonych przez Kreml. Cyberataki mogą w związku z tym polegać nie tylko na niszczeniu infrastruktury państwa lub podmiotów prywatnych, lecz także na uzyskiwaniu (wykradaniu) informacji, które posłużą do rosyjskich działań dezinformacyjnych bądź propagandowych – ataki takie powinny być więc postrzegane jako ich element uzupełniający czy mający je wzmocnić. W ten sposób Kreml może zdobywać dane wspomagające oddziaływanie informacyjne, wykradać dokumenty w celu ich sfabrykowania oraz rozpowszechniać przekazy propagandowe, jak również dokonywać aktów cyberszpiegostwa (Brangetto i Veenendaal, 2016, s. 121–126). Rosja korzysta głównie z usług profesjonalnych hakerów pracujących na rzecz służb specjalnych zgodnie z polityką zagraniczną prowadzoną przez Federację oraz na zlecenie Kremla. Poza podmiotami państwowymi działają organizacje cyberprzestępcze, wobec których nie wyciąga się konsekwencji, o ile ich działalność jest skierowana wyłącznie przeciw państwom zachodnim (Kozłowski, 2021, s. 99). Co istotne, Kreml zleca też operacje w cyberprzestrzeni mniej lub bardziej sformalizowanym podmiotom zewnętrznym, np. hakerom czy aktywistom (Gardocki i Worona, 2020, s. 39).

Omówione w zarysie środki realizowania wojny informacyjnej w ramach rosyjskiej polityki zagranicznej stanowią jedynie wycinek prowadzonych działań. Ich kompleksowy charakter (Kreml przeznacza na nie duże ilości zasobów zarówno finansowych, jak i organizacyjnych) nakazuje stwierdzić, że nie możemy wykluczyć pojawienia się w przyszłości innych, nowych instrumentów. Ponieważ ich pokaźna część pozostaje niejawna (do pewnego czasu), przypuszczalnie takie środki są już wykorzystywane, a wiedzę o nich uzyskamy *post factum*.

Polska jest celem owej wojny informacyjnej. Odnosząc działania podejmowane przez Rosję do kwestii spornych występujących w stosunkach polsko-rosyjskich, można wskazać, że szczególnie widoczne są tutaj próby ingerencji w wewnętrzną sytuację w kraju, a zwłaszcza podsycanie antagonizmów w konfliktach politycznych i społecznych. W ostatnich latach doszło do wyjątkowego

zintensyfikowania tych działań, przede wszystkim po aneksji Półwyspu Krymskiego przez Rosję w 2014 r. (Aleksandrowicz, 2016, s. 138–139), później w związku z pandemią COVID-19. W polskiej przestrzeni medialnej bardzo szybko zaczęły się pojawiać portale i osoby, które publikowały treści negujące istnienie pandemii, głoszące, że szczepienia są nieskuteczne, a wirus wytworzono jako broń (Służby specjalne, b.d.). Wcześniej powyższe podmioty szerzyły dezinformację dotyczącą rzekomej szkodliwości sieci 5G (Służby specjalne, b.d.), obecnie zaś – w trakcie wojny rosyjsko-ukraińskiej – prowadzą kampanie, które mają z jednej strony usprawiedliwić rosyjskie poczynania w Ukrainie, a z drugiej strony antagonizować Polskę i Ukrainę (Służby specjalne, 2022). Operacje Kremla w polskiej przestrzeni informacyjnej opierają się głównie na sieci portali informacyjnych i społecznościowych. Celem ich działalności jest kreowanie nastrojów antyzachodnich i antynatowskich (obecnie również antyukraińskich), podważanie zaufania do organów państwa polskiego oraz Sił Zbrojnych RP, a ponadto wywoływanie konfliktów na tle historycznym, narodowościowym, rasowym i religijnym (szerzej zob. Bochyńska, 2022; Służby specjalne, b.d.; a także raporty Centrum Analiz Propagandy i Dezinformacji: Kowalska i Marek, 2019; Lelonek, 2017; Wóycicki, Kowalska i Lelonek, 2017). Działalność Rosji obejmuje też ataki w polskiej cyberprzestrzeni, jak wynika z raportów Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego i Zespołu CERT Polska (Ministerstwo Cyfryzacji, 2019). Cyberataki najczęściej towarzyszą największym napięciom występującym w stosunkach dwustronnych, co doskonale obrazują działania podejmowane przez Rosję w Estonii (2007), w Gruzji (2008) oraz w Ukrainie (od 2014 r.) (Kowalewski i Kowalewski, 2017, s. 136).

Podsumowanie

Podsumowując niniejsze rozważania, można wyprowadzić kilka zasadniczych wniosków:

1. **Brak jednolitej definicji.** Istnieją rozbieżności w definicjach wojny informacyjnej między badaczami zachodnimi i rosyjskimi. Zachodnie definicje skupiają się na aspektach militarnych, podczas gdy rosyjskie podejście jest znacznie szersze, obejmuje dodatkowo działania psychologiczne, propagandowe i psychospołeczne.
2. **Ewolucja i adaptacja.** Rosyjskie teorie wojny informacyjnej ewoluują i dostosowują się do zmieniającego się otoczenia międzynarodowego. Kreml wykorzystuje różnorodne metody, od tradycyjnej propagandy po nowoczesne technologie w cyberprzestrzeni, aby wpływać na międzynarodową opinię publiczną i destabilizować inne państwa.

3. **Cel i strategia.** Najważniejsza różnica pomiędzy zachodnim a rosyjskim podejściem do wojny informacyjnej dotyczy celu, jaki ma ona osiągnąć. Podczas gdy Zachód używa informacji głównie do przekonywania i wywierania wpływu, Rosja dąży do dezorganizacji, demoralizacji i destabilizacji przeciwników poprzez szeroko zakrojone kampanie oddziaływania informacyjnego.
4. **Integracja z polityką zagraniczną.** Wojna informacyjna jest integralnym narzędziem polityki zagranicznej Rosji. Dokumenty takie jak *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej* oraz *Koncepcja polityki zagranicznej Federacji Rosyjskiej* jasno wskazują na strategiczne znaczenie informacji w realizacji celów polityki zagranicznej.
5. **Techniki i narzędzia.** Rosja wykorzystuje różnorodne instrumenty, takie jak „farmy trolli", boty internetowe, fałszywe konta w mediach społecznościowych i cyberataki, aby prowadzić wojny informacyjne. Narzędzia te pozwalają skutecznie oddziaływać w globalnej przestrzeni informacyjnej na dużą skalę, często przy minimalnych kosztach.
6. **Kluczowe teorie i koncepcje.** Rosyjskie podejście do wojny informacyjnej opiera się na fundamentach opracowanych przez takich badaczy jak Jewgienij Messner, Igor Panarin i Aleksandr Dugin. Ich teorie zakładają, że kluczem do sukcesu w wojnach informacyjnych jest zdobycie przewagi w sferze świadomości społecznej przeciwnika, a niekoniecznie fizyczne zniszczenie infrastruktury.

Wojna informacyjna w ujęciu rosyjskim stanowi wszechstronne narzędzie polityki zagranicznej, które łączy tradycyjne metody propagandowe ze współczesnymi zdobyczami technologicznymi.

Bibliografia

Aleksandrowicz, T.R. (2016). *Podstawy walki informacyjnej*. Editions Spotkania.

Aleksandrowicz, T.R. (2018). Bezpieczeństwo informacyjne państwa. *Studia Politologiczne*, *49*, 33–50.

Aleksandrowicz, T.R. (2021). *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*. Difin.

Banasik, M. (2021a). *Rywalizacja, presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego*. Difin.

Banasik, M. (2021b). Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską. W: M. Banasik (red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski* (s. 49–65). Difin.

Bebber, R. (2016). Information war and rethinking phase 0. *Journal of Information Warfare, 15*(2), 39–52.

Bernays, E.L. (1928). *Propaganda*. Horace Liveright.

Bochyńska, N. (2022). *Rosyjska wojna (dez)informacyjna. Ekspert: Celem Rosjan jest stymulowanie paniki w Polsce* [*wywiad*]. https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjska-wojna-dezinformacyjna-ekspert-celem-rosjan-jest-stymulowanie-paniki-w-polsce-wywiad

Brangetto, P., Veenendaal, M.A. (2016). Influence cyber operations: The use of cyberattacks in support of influence operations. W: *8th International Conference on Cyber Conflict (CyCon)* (s. 113–126). Tallinn. https://doi.org/10.1109/CYCON.2016.7529430

Collins, B., Ling Kent, J. (2022). *Facebook, Twitter remove disinformation accounts targeting Ukrainians*. https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880

Darczewska, J. (2014). *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*. Ośrodek Studiów Wschodnich im. M. Karpia (*Punkt Widzenia*, *42*).

Darczewska, J. (2015). Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?. *Przegląd Bezpieczeństwa Wewnętrznego*, *wyd. specj*., 59–73.

Denning, D.E. (2002). *Wojna informacyjna i bezpieczeństwo informacji*, przeł. J. Bloch. Wydawnictwa Naukowo-Techniczne.

Dobek-Ostrowska, B. (2007). *Komunikowanie polityczne i publiczne. Podręcznik akademicki*. Wydawnictwo Naukowe PWN.

Dobek-Ostrowska, B., Fras, J., Ociepka, B. (1997). *Teoria i praktyka propagandy*. Wydawnictwo Uniwersytetu Wrocławskiego.

Dyner, A.M. (2022). Nowa doktryna wojenna Państwa Związkowego Białorusi i Rosji. *Biuletyn PISM*, *28*, 1–2.

Ellul, J. (1973). *Propaganda: The formation of men's attitudes*. Vintage Books.

Gardocki, S., Worona, J. (2020). Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa. *Colloquium Pedagogika – Nauki o Polityce i Administracji*, *2*(38), 33–46. https://doi.org/10.34813/12coll2020

Gerovitch, S. (2002). *From newspeak to cyberspeak: A history of Soviet cybernetics*. MIT Press.

Giles, K. (2016a). *Handbook of Russian information warfare*. NATO Defense College.

Giles, K. (2016b). *The next phase of Russian information warfare*. NATO Strategic Communications Centre of Excellence.

Giles, K. (2020). *Valery Gerasimov's doctrine*. https://doi.org/10.13140/RG.2.2.10944.35848

Giles, K., Seaboyer, A. (2019). *The Russian information warfare construct*. Defence Research and Development Canada. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf

Gleicher, N. [@ngleicher]. (2022). [Tweet z 28.02]. https://x.com/ngleicher/status/1498180571809280001?s=20&t=PEa6XUCoSC7L6WlyAtwomQ

Harrel, Y. (2015). *Rosyjska cyberstrategia*, przeł. B. Losson. DiG.

Interfax-Ukraine (2022). *SBU liquidates million-strong bot farm destabilizing situation in Ukraine on order of political force*. https://interfax.com.ua/news/general/850029.html

Kiera, J. (2019). Implikacje koncepcji wojen buntowniczych Jewgienija Messnera dla doktryny bezpieczeństwa Federacji Rosyjskiej w XXI wieku. W: M. Banasik i A. Rogozińska (red.), *Perspektywy zagrożeń dla bezpieczeństwa międzynarodowego kreowanych przez Federację Rosyjską* (s. 104–120). Difin.

Kowalewski, J., Kowalewski, M. (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Oficyna Wydawnicza Politechniki Warszawskiej.

Kowalska, M., Marek, M. (2019). *Wizerunek Polski i Polaków w rosyjskiej przestrzeni informacyjnej* [raport]. Centrum Analiz Propagandy i Dezinformacji. https://capd.pl/images/Projekt_MSZ/WIzerunek-Polski-i-Polakw-w-rosyjskiej-przestrzeni-informacyjnej.pdf

Kozłowski, A. (2021). Działalność Rosji w cyberprzestrzeni zagrożeniem dla bezpieczeństwa państw regionu euroatlantyckiego. W: M. Banasik (red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski* (s. 95–115). Difin.

Lelonek, A. (2017). *Wojna informacyjna, operacje informacyjne i psychologiczne* [raport]. Centrum Analiz Propagandy i Dezinformacji. https://capd.pl/pl/analizy/161-wojna-informacyjna-operacje-informacyjne-i-psychologiczne

Libicki, M.C. (1995). *What is information warfare?*. National Defense University.

Lucas, E., Pomeranzev, P. (2016). *Winning the information war: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe* [a report]. Center for European Policy Analysis, Legatum Institute. https://www.lse.ac.uk/iga/assets/documents/arena/archives/winning-the-information-war-full-report-pdf.pdf

Messner, J. (2005). *Хочешь Мира, Победи Мятежевойну!*. Русский Путь.

Mierzyńska, A. (2022). *43 portale nadają codziennie antyukraińską propagandę po polsku* [*raport z sieci*]. https://oko.press/antyukrainska-propaganda-po-polsku-raport-z-sieci/

Ministerstwo Cyfryzacji (2019). *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)*. https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt

Modrzejewski, Z. (2018). Dezinformacja w służbie walki informacyjnej. W: T.W. Grabowski, M. Lakomy i K. Oświecimski (red.), *Bezpieczeństwo informacyjne w dobie postprawdy* (s. 91–117). Wydawnictwo Naukowe Akademii Ignatianum.

NewsGuard (2024). *Russia-Ukraine Disinformation Tracking Center: 645 websites spreading war disinformation and the top myths they publish*. https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/

Palczewski, S. (2019). *Strategia rosyjskich botów w sieci – uderzyć w NATO i Polskę*. https://cyberdefence24.pl/polityka-i-prawo/strategia-rosyjskich-botow-w-sieciuderzyc-w-nato-i-polske

Prezident Rossijskoj Federacii. (2016a). *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii*. http://kremlin.ru/acts/bank/41460

Prezident Rossijskoj Federacii. (2016b). *Koncepcija vnešnej politiki Rossijskoj Federacii*. http://static.kremlin.ru/media/acts/files/0001201612010045.pdf

Prezident Rossijskoj Federacii. (2021). *Strategija nacional'noj bezopasnosti Rossijskoj Federacii*. http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf

Rid, T. (2022). *Wojna informacyjna*, przeł. F. Tryl. Bellona.

River, C.H. (2020). *Yuri Bezmenov: The life and legacy of the influential KGB informant who defected to the West*. Charles River Editors.

Savranska, K. (2020). *Problematyka walki informacyjnej w relacjach Rosji z wybranymi państwami europejskimi. Perspektywa medioznawcza*. Instytut Mediów, Dziennikarstwa i Komunikacji Społecznej Uniwersytetu Gdańskiego.

Seddon, M. (2014). *Documents show how Russia's troll army hit America*. https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america

Służby specjalne. (2022). *Operacja informacyjna przeciwko Polsce*. https://www.gov.pl/web/sluzby-specjalne/klamstwa-rosyjskiej-propagandy2

Służby specjalne. (b.d.). *Polska na celowniku dezinformacji*. Pobrane 20 września 2023 z: https://www.gov.pl/web/sluzby-specjalne/polska-na-celowniku-dezinformacji

Sun Tzu. (1994). *Sztuka wojny*, przeł. K.A.M. Przedświt.

Ventre, D. (2016). *Information warfare* (2nd ed.). John Wiley & Sons.

Volkoff, V. (2022). *Krótka historia dezinformacji: Od konia trojańskiego do Internetu*, przeł. M. Miszalski. Wektory.

Weiss, M., Pomerantsev, P. (2014). *The menace of unreality: How the Kremlin weaponizes information, culture and money. A Special Report presented by The Interpreter, a project of the Institute of Modern Russia*. Institute of Modern Russia. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

Wierzbicki, A. (2015). Russkij mir jako projekt restauracyjny imperium. W: S. Bieleń i A. Skrzypek (red.), *Rosja. Rozważania imperiologiczne* (s. 101–136). Oficyna Wydawnicza ASPRA.

Wojnowski, M. (2015a). Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej. *Przegląd Bezpieczeństwa Wewnętrznego*, *7*(13), 13–39.

Wojnowski, M. (2015b). Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku. *Przegląd Bezpieczeństwa Wewnętrznego*, *wyd. specj*., 7–38.

Wojnowski, M. (2017). Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej. *Przegląd Bezpieczeństwa Wewnętrznego*, *9*(16), 11–37.

Wojnowski, M. (2019). Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI w. *Przegląd Bezpieczeństwa Wewnętrznego*, *21*, 13–43.

Wóycicki, K., Kowalska, M., Lelonek, A. (2017). *Rosyjska wojna dezinformacyjna przeciwko Polsce* [raport]. Centrum Analiz Propagandy i Dezinformacji.

https://pulaski.pl/wp-content/uploads/2015/02/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf

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

Ziółkowski, J. (2016). Zarządzanie syndromem oblężenia w demokracji liberalnej. *Studia Politologiczne*, *41*, 170–197.

Ziółkowski, J. (2019). *Syndrom oblężonej twierdzy*. Elipsa.