mgr Otylia BIENIEK[1]

CYBERPRZESTRZEŃ W ROSYJSKIEJ PRZESTRZENI INFORMACYJNEJ

Słowa kluczowe: *rewolucja cyfrowa, przestrzeń informacyjna, cyberprzestrzeń, komunikacja strategiczna, Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej, bezpieczeństwo interesów narodowych Federacji Rosyjskiej w cyberprzestrzeni*

STRESZCZENIE

Celem niniejszego opracowania jest interpretacja, na podstawie ogólnej analizy dokumentów strategicznych i doktrynalnych, działań Federacji Rosyjskiej w przestrzeni informacyjnej. Radio, telewizja, prasa, jak i uważany za najistotniejszy element w podsystemie technologicznym internet, stanowią współcześnie narzędzia do obrony i ochrony interesów państwowych. Autor dokona interpretacji działań Federacji Rosyjskiej w jednym z kluczowych dziś obszarów przestrzeni informacyjnej – cyberprzestrzeni oraz unikalnego postrzegania przez Rosjan tego obszaru.

Wstęp

Dzisiejsza aktywność Rosji w przestrzeni informacyjnej stanowi bez wątpienia wyzwanie dla innych decydentów państwowych, co nie oznacza, że jest to zupełnie nowa działalność Rosjan. Posiadają oni największy potencjał operacji psychologiczno-informacyjnych na świecie. Potencjał ten jest budowany w Rosji od lat, dlatego w kontekście zagadnień dotyczących bezpieczeństwa w cyberprzestrzeni znaczenie rzeczywistości kulturowej Rosji nie powinno być pomijane. Rosja jako Federacja jest zwieńczeniem długiej historycznej drogi. Dzisiejsze zachowanie Rosji w przestrzeni informacyjnej są ściśle zależne od wydarzeń takich jak: upadek Rusi Kijowskiej, trzy wieki jarzma mongolskiego, po czym panowania cara Iwana I oraz formowania się niesamowicie trwałych służb wywiadowczych o nazwie Opricznina[2],

[1] Otylia Bieniek jest doktorantem Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

[2] Przyp. wł. Opriczninę uważa się za pierwsze rosyjskie służby wywiadu wewnętrznego oraz prototyp stałych służb wywiadowczych związanych z rosyjską władzą centralną, została zniesiona w 1572 r.

a także ich apogeum w postaci sowieckich służb specjalnych. Warto też odnieść się do Ochrany (skrót terminu „departament gwardii" Охранное отделение), politycznej policji cara, stworzonej w 1881 roku, która określana jest mianem najdoskonalszej policji świata. Jak widać formowanie się współczesnych rosyjskich służb specjalnych XX wieku, tj.: GPU, OGPU, NKWD, NKGB, KGB odbywało się na solidnych podwalinach i bogatej tradycji służb informacyjnych. Zdaniem prof. Harrella mimo, iż zmieniały się nazwy owych komórek, cel pozostawał zawsze ten sam: obrona sowieckiego reżimu. Prof. Harrell twierdzi, iż trudno sobie wyobrazić, że Związek Radziecki mógłby przetrwać bez skrojonych na miarę służb informacyjnych: KGB to Związek Radziecki, a Związek Radziecki to KGB. Nic zatem dziwnego, że w szeregach służb specjalnych odnajdujemy wielu późniejszych przywódców i pierwszoplanowe osobistości Związku Radzieckiego. Wniosek jest jeden – kto kontroluje informację i komunikację, kontroluje społeczeństwo[3].

Celem niniejszej pracy jest zatem interpretacja, na podstawie ogólnej analizy dokumentów strategicznych i doktrynalnych, działań Federacji Rosyjskiej w przestrzeni informacyjnej. Z tego względu, że zarówno radio, telewizja, prasa, jak i uważany za najistotniejszy element w podsystemie technologicznym internet, służą Rosjanom jako narzędzia do obrony i ochrony swoich interesów, zinterpretowane w szczególności zostaną działania Rosji w jednym z kluczowych dziś obszarów przestrzeni informacyjnej – cyberprzestrzeni oraz unikalne podejście Rosjan do tego obszaru.

Niniejsze opracowanie stanowi wstęp do szerszych rozważań na temat defensywnych i ofensywnych zdolności militarnych Federacji Rosyjskiej w cyberprzestrzeni.

Problematyka

Przełom XX i XXI w pierwszej kolejności kojarzy się z rewolucją cyfrową, którą spowodowało, uwarunkowane ekonomicznie i społecznie dynamiczne tempo przemian. Futurolog A. Tofler nie mylił się, ogłaszając swoją tezę tzw. trzeciej fali, oznaczającą pojawienie się ery wiedzy i informacji. Aktualnie możemy zauważyć, że zgodnie z tą tezą wszelką działalność człowieka cechuje samowystarczalność i realizacja celów w oparciu o nowe technologie, które obsługują ogromne zasoby wiedzy i informacji. Oprócz tego najważniejsze aspekty życia społecznego, gospodarczego oraz militarnego zaczęły przenosić się do wirtualnej przestrzeni – cyberprzestrzeni.

[3] Y. Harrel, *Rosyjska cyberstrategia*, Warszawa 2015, s. 56.

Pojawienie się cyberprzestrzeni uwarunkował nieprzerwany i dynamiczny rozwój technologii. Cyberprzestrzeń stanowią dzisiaj połączone siecią komputery i inne media cyfrowe (telefony, tablety, radio, telewizja), które są między sobą dodatkowo skomunikowane. Nie bez znaczenia są także technologie z zakresu internetu rzeczy (IoT)[4]. Internet rzeczy tworzą urządzenia lub zwykłe przedmioty, które za pomocą podłączenia do sieci są w stanie przesyłać informacje. Analitycy twierdzą zgodnie, że jeśli uda się okiełznać Big Data generowane przez smart-urządzenia, to IoT stanie się jednym z głównych budulców naszej epoki[5].

Bez wątpienia rozwój nowych technologii ma istotny wpływ na charakter prowadzenia współczesnych konfliktów zbrojnych, a także na kształt i obraz samej wojny. Cyberwojna, wojna hybrydowa, wojna niekontaktowa, walka informacyjna, agresja poniżej progu wojny – to najczęściej używane określenia starć, których głównym polem jest cyberprzestrzeń. Współczesne konflikty zbrojne cechuje informacyjny charakter, brak jednoznacznych granic w czasie i w przestrzeni oraz przewaga środków niemilitarnych nad walką zbrojną[6].

Wśród narzędzi współczesnych konfliktów wymienia się zatem: dyplomację, propagandę, kampanie psychologiczne, działania na poziomie wpływania na procesy polityczne lub kulturowe, dezinformację bądź manipulowanie lokalnymi mediami, infiltrację sieci komputerowych i baz danych, wysiłki w zakresie promowania opozycyjnych lub wrogich populacji będących celem grup w sieciach komputerowych[7].

---

[4] IoT czyli Internet of Things – pojęcie sformułowane przez Kevina Ashtona ponad 30 lat temu, oznacza szeroko rozumianą koncepcję bazującą na idei łączności między urządzeniami (M2M – machine to machine). To znaczy, że zakłada ona możliwość komunikacji, wymiany, przetwarzania oraz gromadzenia danych przez urządzenia bez ingerencji człowieka – jedynie za pośrednictwem sieci komputerowej. Więcej na: https://www.csi.pl/consulting-techniczny/230-czym-jest-internet-of-things/ [dostęp: 6.05.2017].

[5] http://www.forbes.pl/czym-jest-internet-rzeczy-,artykuly,195983,1,1.html/ [dostęp: 6.06.2017].

[6] M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-5/1223,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-13-7-2015.html/ [dostęp: 6.06.2017].

[7] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku, Bezpieczeństwo narodowe*, 2011, www.bbn.gov.pl/download/1/7008/1Wojnacybernetyczna.pdf/ [dostęp: 1.06.2017].

Wyżej wymienione narzędzia nie narodziły się wraz z powstaniem internetu. Cyberprzestrzeń dała po prostu nowe, efektywne metody tych działań, które określa się wspólnym mianem walki informacyjnej[8].

Bezpieczeństwo informacyjne w polityce bezpieczeństwa Federacji Rosyjskiej

Bezpieczeństwo informacyjne w głównej mierze rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. W celu eliminacji zagrożeń dla informacji przede wszystkim należy zapewnić jej poufność, integralność i dostępność. Bezpieczeństwo informacyjne stanowi jeden z kryteriów przedmiotowych bezpieczeństwa narodowego obok bezpieczeństwa militarnego, ekonomicznego, politycznego czy społecznego[9].

Rosyjską definicję bezpieczeństwa informacyjnego podaje oficjalnie obowiązujący w Federacji Rosyjskiej słownik wojenno-polityczny: *Wojna i pokój w terminach i definicjach*[10]. Zespołowi redakcyjnemu przewodził Dmitrij Rogozin wicepremier Federacji Rosyjskiej, dlatego słownik ten posiada też istotne znaczenie doktrynalne.

Według powyższego słownika bezpieczeństwo informacyjne (*информационная безопасность*) oznacza stan, który zapewnia bezpieczeństwo informacji, nośników informacji, zasobów, systemów informacyjnych przed nieuprawnionym i przypadkowym modyfikowaniem lub niszczeniem informacji, przy jednoczesnym zapewnieniu szybkiego dostępu uprawnionym podmiotom i uniemożliwienie takiego prawa nieuprawnionym podmiotom[11].

Według rosyjskiej myśli doktrynalnej bezpieczeństwo informacji można uzyskać na kilku płaszczyznach: normatywno-prawnej, organizacyjno-proceduralnej, programowo-technicznej, duchowo-psychologicznej[12].

Bezpieczeństwo informacyjne jest aktywnym przeciwdziałaniem państwa, w szczególności takim zagrożeniom, które powstają gdy pod pozorem wolności słowa realizowana jest polityka wprowadzania do umysłów obywateli informacji i norm kulturowych, orientujących i motywujących działania tych obywateli w taki

---

[8] Z. Modrzewski, Sz. Markiewicz, *Współczesna walka informacyjna*, Warszawa 2016, s. 77.

[9] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19.

[10] http://voina-i-mir.ru/ [dostęp: 1.06.2017].

[11] http://voina-i-mir.ru/article/32/ [dostęp: 1.06.2017].

[12] Tamże.

sposób by zastępować tradycyjne wartości duchowe i ostatecznie, prowadzących do degradacji tożsamości narodowej i erozji narodowej suwerenności[13].

Rosjanie za pomocą mediów aktywne wspierają swoich rodaków żyjących w kraju jak i poza granicami Federacji. Wsparcie ludności rosyjskojęzycznej, zamieszkującej republiki poradzieckie postrzega się również jako realizację koncepcji tak zwanego *„rosyjskiego pokoju"* (*русский мир*). Należy dodać, że *„rosyjski pokój"* obejmuje zarówno rosyjską przestrzeń duchową, jak i rosyjską przestrzeń kulturową i przestrzeń rosyjskojęzyczną[14]. Nie jest również nowością, że rosyjskie władze kontrolują media masowe. Umożliwia to utrzymanie w miarę spójnej interpretacji przedstawianych zdarzeń. Za pomocą oddziaływania informacyjnego władze rosyjskie, m.in. kultywują swoistą nostalgię za imperium radzieckim. Rosyjska propaganda działa na odbiorców tak, aby w opinii publicznej Rosja uchodziła, np. za ośrodek „przyciągania" innych państw. Przykład stanowi przeprowadzone w 2014 roku referendum w sprawie statusu Krymu[15]. Zgodnie z oficjalnymi danymi skalę podejmowanych działań w celu obrony rosyjskiej mocarstwowej pozycji w przestrzeni poradzieckiej[16].

Państwowi decydenci aby bronić interesów państwowych oraz zapewnić stabilną pozycję państwa na świecie w sferze bezpieczeństwa informacyjnego podejmują szereg działań legislacyjnych. Wdrażanie czy nowelizacje regulacji prawnych takich jak m.in. strategia bezpieczeństwa informacyjnego oraz doktryny i koncepcje dotyczące cyberbezpieczeństwa to jedne z ważniejszych działań. Warto dodać, że na świecie powołane zostały zespoły reagowania na cyberincydenty (CERT lub CIRT). Nową tendencją stało się także ogłaszanie przez czołowe państwa funkcjonowania w swoich strukturach tak zwanych cyberwojsk[17]. Ważnym krokiem do kontroli regulacji prawnych i teoretycznych mechanizmów cyberbezpieczeństwa stała się działalność międzynarodowych indeksów cyberbezpieczeństwa[18].

---

[13] http://voina-i-mir.ru/article/32

[14] S. Bieleń, *Siła motywacyjna w polityce zagranicznej Federacji Rosyjskiej*, [w:] *Bezpieczeństwo obszaru poradzieckiego*, red. nauk. Bryc A., Legucka A., Włodkowska-Bagan A., Warszawa 2011, s. 69.

[15] https://pl.wikipedia.org/wiki/Referendum_na_Krymie_w_2014_roku/ [dostęp: 1.06.2017].

[16] S. Bieleń, *Siła motywacyjna (…)*, s. 69.

[17] Przyp. wł. Specjalistyczne jednostki zajmujące się cyberbezpieczeństwem w celach militarnych albo wywiadowczych istnieją w Rosji, USA, Chinach, Wielkiej Brytanii, Niemczech, Francji, Korei Północnej; patrz szerzej [w:] http://www.cyberdefence24.pl/578523,niemcy-wzmacniaja-cyberobrone [dostęp: 2.06.2017].

[18] Przyp. wł. Do najpopularniejszych cyberindeksów zalicza się: Cyber-Security: the vexed question of global rules (Cyberbezpieczeństwo: dręczący problem globalnych zasad),

Federacja Rosyjska ostatnimi laty podjęła szereg kroków w celu zwiększenia bezpieczeństwa swojej przestrzeni informacyjnej. Pod auspicjami Rady Bezpieczeństwa Federacji Rosyjskiej wprowadzane i na bieżąco uaktualniane są dokumenty strategiczne, doktryny, tzw. cyberstrategie[19]. Do najważniejszych należą:

- **Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej, 2016;** Доктрина информационной безопасности Российской Федерации.
- **Dekret „O strategii rozwoju społeczeństwa informacyjnego w Federacji Rosyjskiej na lata 2017–2030", 2017;** Указ „О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы".
- **Koncepcyjne spojrzenie na aktywność sił zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej, 2011;** Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве.
- **Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku, 2013;** Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.
- **Rosyjska koncepcja Konwencji ONZ „O międzynarodowym bezpieczeństwie informacyjnym" 2012;** Российская концепция конвенции ООН «Об обеспечении международной информационной безопасности».
- **Fragment Koncepcji państwowego systemu wykrywania, uprzedzania i likwidacji skutków ataków komputerowych na zasoby informacyjne Federacji Rosyjskiej, 2014;** ВЫПИСКА ИЗ КОНЦЕПЦИИ государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак[20].

Ogólna analiza powyższych dokumentów dowodzi, że Federacja Rosyjska świadoma zwiększenia się zagrożenia użycia „broni informacyjnej" przeciwko swojej infrastrukturze informacyjnej pracuje nad adekwatną i wyczerpującą odpowiedzią na zagrożenia wynikające z intensywnego wprowadzania zagranicznych technologii informatycznych do sfery działalności jednostki, społeczeństwa i państwa. Zagrożenie według Rosjan tkwi w korzystaniu z systemów technologicznych

---

The Cyber Index: International Security Trends and Realities, Global Cybersecurity Index and Cyberwellness Profiles, EU Cybersecurity Dashboard.

[19] Przyp. wł. W ogólnym rozumieniu dokument cyberstrategii ma za zadanie nakreślić teoretyczne koncepcje działania w przestrzeni wirtualnej danego państwa lub organizacji międzynarodowej.

[20] https://ccdcoe.org/cyber-security-strategy-documents.html/ [dostęp: 1.06.2017].

otwartej informacji oraz integracji krajowych systemów informacji z międzynarodowymi systemami informacji[21].

Należy zaznaczyć, że wcześniejsza doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej z 2000 roku określiła wtedy militarny charakter środowiska informacyjnego. W dokumencie uznano przestrzeń informacyjną za równorzędne pole działań wojennych do tradycyjnej przestrzeni operacyjnej armii lądowej, a broń informacyjna została włączona do defensywnego i ofensywnego katalogu zdolności militarnych Federacji Rosyjskiej[22].

Natomiast warto w tym miejscu zaznaczyć, że jednym z głównych celów strategicznych doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej[23] jest zapewnienie bezpieczeństwa informacyjnego zgodnie z polityką wojskową tego kraju.

Dokument doktryny wojskowej FR, którego nowelizację Prezydent Putin podpisał 26 grudnia 2014 roku[24] uzupełnia szereg zapisów z doktryny z 2010 roku o nowe pojęcia w dziedzinie bezpieczeństwa, uwzględnił przesunięcie zagrożeń i ryzyka wojny w przestrzeń informacyjną i wewnętrzną.

Doktryna wyszczególnia zagrożenia wewnętrzne, poza destabilizacją polityczno-społecznej sytuacji wewnętrznej, zaliczono do nich: ataki na system informacyjny, w tym obiekty militarne oraz infrastrukturę krytyczną państwa, destrukcyjne oddziaływanie informacyjne na społeczeństwo, zwłaszcza młodzież, osłabiające więzi historyczne, duchowe i patriotyczną tradycję w dziedzinie bezpieczeństwa ojczyzny[25].

Doktryna wojskowa określa główne zadania w zakresie zapobiegania i przeciwdziałania konfliktom zbrojnym, tj.: ocenę i prognozowanie rozwoju sytuacji politycznej i wojskowej na szczeblu regionalnym i globalnym, jak też stan militar-

---

[21] Szerzej patrz [w:] R. Szpyra, *Doktrynalne modele i działania państw oraz organizacji pozarządowych w obszarze bezpieczeństwa w cyberprzestrzeni*: [praca naukowo-badawcza] II.1.18.3.0 / Akademia Obrony Narodowej. Wydział Bezpieczeństwa Narodowego, Warszawa 2015.

[22] https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/ [dostęp: 1.06.2017].

[23] Oryginalny tekst dokumentu patrz [w:] http://kremlin.ru/acts/news/51129/ [dostęp: 1.06.2017].

[24] Oryginalny tekst dokumentu patrz [w:] static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf/ [dostęp: 1.06.2017].

[25] R. Białoskórski, *Cyberprzestrzenny wymiar polityki bezpieczeństwa i obrony Federacji Rosyjskiej*, https://repozytorium.uph.edu.pl/.../bialoskorski.Cyberprzestrzenny_wymiar_polityki.pdf/ [dostęp: 10.06.2017].

no-politycznych stosunków międzynarodowych z użyciem nowoczesnej techniki i technologii informacyjnych[26].

Dokument zakłada stworzenie warunków ograniczających ryzyko zagrożeń związanych z ryzykiem użycia ICT w celach wojskowo-politycznych, sprzecznych z prawem międzynarodowym, naruszających międzynarodową stabilność terytorialną państw i stanowiących zagrożenie dla pokoju, bezpieczeństwa, w wymiarze regionalnym i globalnym[27].

Priorytetowymi działaniami w zakresie realizacji zadań przez instytucje ministerstwa obrony i siły zbrojne FR są: działania na rzecz poprawy efektywności i bezpieczeństwa systemów informacyjno-komunikacyjnych z wykorzystaniem nowoczesnych technologii i międzynarodowych standardów na szczeblach: strategicznym, operacyjnym i taktycznym[28].

Doktryna bezpieczeństwa informacyjnego wskazuje na zagrożenia wynikające z uzależnienia technologicznego i wzywa wprost do „likwidacji zależności od zagranicznych technologii informacyjnych" oraz zapewnienie bezpieczeństwa środowiska informacyjnego poprzez rozwijanie skutecznych rosyjskich technologii. W doktrynie Rosja przedstawia się jako państwo osaczone, zmuszone do podejmowania działań defensywnych w przestrzeni informacyjnej, podtrzymując narrację konfrontacji „świata zachodu" i „świata rosyjskiego"[29].

Rosyjskie postrzeganie przestrzeni informacyjnej i cyberprzestrzeni

Podejście Rosjan do istoty samej walki informacyjnej wyraża się w posiadaniu odmiennego od „zachodniego" zakresu pojęciowego zjawisk takich jak „cyberwalka", „walka informacyjna" czy „walka sieciowa". Brak w nim przeciwstawienia technologicznego i społecznego wymiaru konfliktów XXI wieku[30]. Rosyjskie definicje

---

[26] Tamże.

[27] Tamże, s. 22.

[28] Tamże.

[29] https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/ [dostęp: 10.06.2017].

[30] Charakter współczesnych konfliktów (zarówno walk jak i wojen) uległ w ciągu ostatnich kilkudziesięciu lat istotnym przeobrażeniom: znacznie wzrosła liczba konfliktów wewnątrzpaństwowych, coraz częściej w miejsce państwa pojawiają się różnego rodzaju podmioty o statusie pozapaństwowym, nowo zaobserwowanym elementem współczesnych konfliktów zbrojnych jest rozmycie granicy pomiędzy żołnierzami a cywilami oraz stanem wojny a stanem pokoju. Szerzej patrz [w:] Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, Przegląd bezpieczeństwa wewnętrznego.

mieszają porządek militarny z pozamilitarnym, a technologiczny (cyberprzestrzeń) ze społecznym (przestrzeń informacyjna). Stany Zjednoczone i Europa Zachodnia w podejściu do walki informacyjnej koncentrują się przede wszystkim na militarnym i wywiadowczym zastosowaniu technologii informatycznych[31].

Oprócz tego Rosjanie nie traktują cyberprzestrzeni jako oddzielnego pola działań wojennych – obok powietrza, morza, lądu czy przestrzeni kosmicznej, tak jak w założeniach NATO z 2016 roku. Zamiast słowa „cyberprzestrzeń" Rosjanie używają sformułowania „przestrzeń informacyjna". Cyberzdolności Rosjan są zatem nowym narzędziem do działań w ramach wojny informacyjnej (wywiadu, kontrwywiadu, dezinformacji, propagandy), wojny elektronicznej, zakłócania komunikacji i nawigacji, wywierania presji psychologicznej oraz niszczenia zasobów informatycznych przeciwnika[32].

Działania Rosji w cyberprzestrzeni to w głównej mierze działania „obronne". Walkę informacyjną Rosjanie w głównej mierze definiują jako oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych. Należy dodać, że aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomika danego państwa również stanowią cele hakerów lub tzw. trolli internetowych[33].

Rosyjska definicja wojny informacyjnej (*информационная война*) zamieszczona w rosyjskim słowniku wojenno-politycznym: *Wojna i pokój w terminach i definicjach*[34] określa intensywną rywalizację w przestrzeni informacyjnej w celu uzyskania informacyjnej, psychologicznej i ideologicznej przewagi, niszczenia informacyjnych systemów, procesów i zasobów oraz krytycznie ważnych struktur i środków komunikacji (informacyjno-techniczna, sieciocentryczna i cyberwojna) rozkładu systemów politycznych i społecznych a także masowej psychologicznej obróbki stanu osobowego wojsk i ludności (*информационно-психологическая война* – wojna informacyjno-psychologiczna)[35].

---

[31] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014, s. 11–12.

[32] http://geopolityka.org/analizy/andrzej-kozlowski-cyberwojownicy-kremla/ [dostęp: 1.06.2017].

[33] http://geopolityka.org/analizy/andrzej-kozlowski-cyberwojownicy-kremla/ [dostęp: 1.06.2017].

[34] http://voina-i-mir.ru/ [dostęp: 1.06.2017].

[35] http://voina-i-mir.ru/article/106/, szerzej patrz [w:] Szpyra R., *Doktrynalne modele i działania państw oraz organizacji pozarządowych w obszarze bezpieczeństwa w cyberprzestrzeni* (…).

Wojna informacyjna w wojenno-politycznej kategorii definiowana jest jako zbiór metod wpływania na świadomość wszystkich grup społecznych państwa przeciwnika dla wypaczania lub zmieniania wiedzy o podstawowych zjawiskach społecznych i przyrodniczych i w konsekwencji do osłabiania lub niszczenia fundamentów społeczeństwa, co stwarza warunki do dezorganizacji przedsięwzięć podejmowanych dla przeciwdziałania agresji[36].

Natomiast zgodnie z raportem przygotowanym przez Centrum Eksperckie NATO ds. Komunikacji Strategicznej dotyczącym działań komunikacyjnych podejmowanych przez Rosję, kraj ten dzięki użyciu medialnej ofensywy używa zarówno tradycyjnych, jak i zupełnie nowych form propagandy, by wpoić lokalnym i zagranicznym społeczeństwom swoje cele. Raport stanowi swoistą analizę działań rosyjskich decydentów w ramach rosyjskiej wojny informacyjnej, która opiewa „o wojnę o rząd dusz i umysłów obywateli w kraju i za granicą". Era cyfrowa stanowi zatem doskonałą okazję dla Rosjan do obrony i ochrony swoich interesów w wymiarze globalnym[37].

Wyżej wspomniany raport potwierdza nasze wcześniejsze rozważania dotyczące różnic w podejściu Rosji i krajów szeroko rozumianego Zachodu do zjawiska walki informacyjnej w obszarze cyberprzestrzeni. Zgodnie z tym, co starają się podkreślić autorzy raportu, Rosjanie posiadają pełne sprzeczności podejście do komunikacji strategicznej w porównaniu do krajów natowskich. Przykładem jest zdefiniowanie rosyjskiej wojny informacyjnej w dokumencie z 2011 roku – Koncepcyjne spojrzenie na aktywność sił zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej (*Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*). Rosyjska wojna informacyjna według powyższego dokumentu (przyjęta przez autorów raportu jako odpowiednik natowskiego terminu komunikacji strategicznej) to jedna z wielu możliwości podkopywania systemów politycznych, ekonomicznych i społecznych; zastosowanie masowej kampanii psychologicznej przeciwko obywatelom kraju, by zdestabilizować jego rząd i społeczeństw; oraz zmuszenie państwa do podejmowania decyzji zgodnych z interesem przeciwników[38].

Jednakże komunikacja strategiczna zdefiniowana przez NATO stanowi skoordynowane i właściwe użycie kanałów komunikacyjnych. Definicja ta nie zawiera sformułowań, które określałyby zamierzone i agresywne działania destabilizujące inne państwa[39].

---

[36] Tamże.

[37] Wojna%20informacyjna%20Rosji%20w%20XXI%20wieku.htm

[38] Wojna%20informacyjna%20Rosji%20w%20XXI%20wieku.htm

[39] Tamże.

Kontrola i zarządzanie przekazem medialnym ma na celu ugruntowanie oraz utrzymanie pozycji i siły Rosji na arenie międzynarodowej. Natowski raport wymienia i opisuje stosowane przez Rosjan zabiegi w celu ochrony i obrony swoich interesów. Działania te oprócz użycia narzędzi takich jak radio, telewizja i prasa coraz częściej przenoszone są do przestrzeni wirtualnej z zastosowaniem cyfrowej techniki, np.: oszustwo (trolle internetowe), własne koncepcje (kontrola odbita – reflexive control, broń poznawcza), tworzenie alternatywnej rzeczywistości (w telewizji i wirtualnych wiadomościach) oraz otwarte kłamstwa (nie ma rosyjskich sił na Ukrainie) czy też reakcje na zagrożenie własnego bezpieczeństwa (przejawiające się w teoriach spiskowych, ostrzeżeniach przed kolorowymi rewolucjami i oświadczeniach o byciu otoczoną ofiarą)[40].

W związku z powyższym w czasie pokoju wojnę informacyjną prowadzi się w formie informacyjnej konfrontacji we wszystkich sferach życia społecznego: w ekonomii, polityce, stosunkach społecznych, w życiu duchowym a zwłaszcza w ideologii[41].

Podstawowymi narzędziami prowadzenia wojny informacyjnej są operacje informacyjne i psychologiczne[42].

Operacje informacyjne stanowią kompleksowy termin, który łączy koncepcje wojny elektronicznej, operacji w sieciach komputerowych, operacji psychologicznych, dezinformacji wojskowej prowadzonej w celu wpływania dla naruszenia normalnej aktywności, uszkadzanie lub zajmowanie narzędzi wspierających podejmowanie decyzji dowódcy przeciwnika, a także środki mające na celu podniesienie obronności w stosunku do podobnych działań przeciwnika[43].

W związku z tym najważniejszym elementem rosyjskich operacji informacyjnych są operacje psychologiczne, które rosyjski słownik określa jako 1) działania informacyjne sił zbrojnych prowadzące do demoralizacji i dezorganizacji wroga; 2) w najszerszym znaczeniu – wszelkie celowe działania instytucji rządowych i pozarządowych w czasie pokoju, w okresie zagrożenia i wojny, która ma na celu zmianę postaw przeciwnika, sprzymierzeńca lub neutralnej publiczności, przedstawicieli sił zbrojnych lub cywilów, w wygodnym dla prowadzącego te operacje kierunku[44].

---

[40] Tamże.

[41] http://voina-i-mir.ru/article/106/, szerzej patrz [w:] R. Szpyra, *Doktrynalne modele i działania państw oraz organizacji pozarządowych w obszarze bezpieczeństwa w cyberprzestrzeni* (…).

[42] Tamże.

[43] http://voina-i-mir.ru/article/108

[44] http://voina-i-mir.ru/article/109, szerzej patrz [w:] Szpyra R., *Doktrynalne modele i działania państw oraz organizacji pozarządowych w obszarze bezpieczeństwa w cyberprzestrzeni* (…).

Powyższa analiza głównych pojęć związanych z rosyjską walką informacyjną dowodzi, że konflikty z udziałem tego państwa wyróżniają się celowym ograniczeniem skali prowadzonych operacji zbrojnych, po to aby uniemożliwić określenie w sposób jednoznaczny stanu wojny oraz agresora, a tym samym zapobiec reakcji społeczności międzynarodowej.

W związku z powyższym Rosjanie w swoim podejściu do przestrzeni informacyjnej i cyberprzestrzeni skupiają się przede wszystkim na ochronie integralności politycznej, społecznej, kulturowej i kultowej państwa, poszanowaniu integralności terytorialnej oraz innych zbiorowości wchodzących w skład populacji tego kraju[45].

Podsumowanie

Powyższe rozważania posłużą nam do podjęcia próby analizy defensywnych i ofensywnych zdolności Federacji Rosyjskiej w przestrzeni informacyjnej i stworzenia w tym celu oddzielnej publikacji. Podstawą tej analizy będzie teoria walki informacyjnej i posłużenie się obszerną publikacją na ten temat prof. Dorothy E. Denning. Denning w sposób kompleksowy opisuje są metody i narzędzia walki informacyjnej, wyszczególniając defensywne i ofensywne operacje państw w tej materii. Według Denning operacje te są jednymi z ważniejszych ogniw walki informacyjnej obok elementów takich jak zasoby informacyjne oraz gracze defensywni i ofensywni. Denning twierdzi, że wojnę prowadzi się dlatego, że zasoby informacyjne mają dla ludzi wartość. Ofensywa ma zatem na celu zwiększenie tej wartości dla strony atakującej i zmniejszenie jej dla strony atakowanej, defensywa zaś ma na celu zapobiec potencjalnej utracie wartości[46].

Rosjanie bez wątpienia dysponują szeregiem sił i środków do tego, aby konsekwentnie utrzymywać silną pozycję znaczącego gracza na arenie międzynarodowej w przestrzeni informacyjnej. Niniejsze rozważania dowiodły o asymetrycznym charakterze współczesnych konfliktów zbrojnych oraz o szczególnej aktywności Federacji Rosyjskiej w cyberprzestrzeni jako prekursorki operacji psychologiczno-informacyjnych. Nie mniej ważny w tym kontekście okazał się także aspekt kulturowy i cywilizacyjny.

Ponadto interpretacja działań Rosji w przestrzeni informacyjnej dała świadectwo temu, że z jednej strony Rosjanie posiadają szeroki potencjał w prowadzeniu kampanii psychologiczno-informacyjnych w ramach aktywności w cyberprzestrzeni, z drugiej zaś borykają się z problemami dotyczącymi rozwoju wysokich technolo-

[45] Y. Harrell, *Rosyjska cyberstrategia*, Warszawa 2015, s. 23.

[46] E.D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 23.

gii, reorganizacją przemysłu oraz niską współpracą międzynarodową w obszarze systemów teleinformatycznych.

Bibliografia

Opracowania

1. Bieleń S., *Siła motywacyjna w polityce zagranicznej Federacji Rosyjskiej*, [w:] *Bezpieczeństwo obszaru poradzieckiego*, red. nauk. Bryc A., Legucka A., Włodkowska-Bagan A., Warszawa 2011.
2. Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
3. Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa 2014.
4. Harrel Yannick, *Rosyjska Cyberstrategia*, Warszawa 2015.
5. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008.
6. Modrzewski Z., Markiewicz Sz., *Współczesna walka informacyjna*, AON, Warszawa 2016.
7. Szpyra R., *Doktrynalne modele i działania państw oraz organizacji pozarządowych w obszarze bezpieczeństwa w cyberprzestrzeni*: [praca naukowo-badawcza] II.1.18.3.0 / Akademia Obrony Narodowej. Wydział Bezpieczeństwa Narodowego, AON, Warszawa 2015.

Źródła internetowe

1. Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, [w:] http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-Wydanie-specjalne.html
2. Wojnowski M., *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, [w:] https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-5/1223,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-13-7-2015.html
3. https://ccdcoe.org/cyber-security-strategy-documents.html
4. https://www.csi.pl/consulting-techniczny/230-czym-jest-internet-of-things/
5. https://arstechnica.com/security/2017/05/radio-controlled-pacemakers-arent-as-hard-to-hack-as-you-may-think/
6. http://www.heritage.org/homeland-security/report/10-conservative-principles-cybersecurity-policy
7. https://militaryarms.ru/voennye-konflikty/kiberneticheskaya-vojna/
8. http://voina-i-mir.ru/
9. http://www.forbes.pl/czym-jest-internet-rzeczy-,artykuly,195983,1,1.html/
10. https://pl.wikipedia.org/wiki/Referendum_na_Krymie_w_2014_roku

11. http://geopolityka.org/analizy/andrzej-kozlowski-cyberwojownicy-kremla/
12. https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/
13. http://www.cyberdefence24.pl
14. https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/

Źródła elektroniczne

1. Białoskórski R., *Cyberprzestrzenny wymiar polityki bezpieczeństwa i obrony Federacji Rosyjskiej*, [w:] https://repozytorium.uph.edu.pl/../bialoskorski.Cyberprzestrzenny_wymiar_polityki.pdf
2. Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku,* Bezpieczeństwo narodowe, 2011, [w:] www.bbn.gov.pl/download/1/7008/1Wojnacybernetyczna.pdf
3. http://kremlin.ru/acts/news/51129
4. static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf
5. Wojna%20informacyjna%20Rosji%20w%20XXI%20wieku.htm

Keywords: *digital revolution, information space, cyberspace, strategic communication, the information security doctrine of the Russian Federation, security of national interests of the Russian Federation in cyberspace*

SUMMARY

The purpose of this paper is the portrayal of the activities of the Russian Federation in the information space. Author's analysis focuses on the basis strategic and doctrinal documents. Radio, television, the press, and considered as the most important element in the technological subsystem – the Internet, they are tools of defense and protection of the main interests of the states. The author will interpret the actions of the Russian Federation in one of key areas of the cyberspace. Also, the article contains analysis of the unique Russian perception of this area.