Colloquium 2(38)/2020
ISSN 2081-3813, e-ISSN 2658-0365

DOI: http://doi.org.10.34813/12coll2020

WYKORZYSTANIE PRZEZ ROSJĘ CYBERPRZESTRZENI W KONFLIKTACH HYBRYDOWYCH A ROSYJSKA POLITYKA CYBERBEZPIECZEŃSTWA

Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy

Sylwester Gardocki
Uniwersytet Warszawski, Polska
ORCiD: https://orcid.org/0000-0002-1703-0172

Joanna Worona
Uniwersytet w Białymstoku, Polska
ORCID: https://orcid.org/0000-0002-1335-2983

Abstract

Over the last years, an increased activity of the Russian Federation in virtual space has been observed. The article aim is to analyse Russia's use of cyberspace in hybrid conflicts. Although the hypothesis states that the Russian cyber security policy has undergone a gradual evolution, its vital function is still to maintain Russia's role as a global leader. This article identifies examples of the Kremlin's use of cyberspace - cyber-attacks (also on the other countries), participation in information war conducted using propaganda, and manipulation. Russia's activity in cyberspace shows that it is necessary to examine its cyber security policy. The article briefly presents Russian Federation legal acts on cyber security. The article raises the issue of Runet - a project of an internal Russian network, independent from the global Internet. Moreover, the paper also discusses the issue of illegal use of the cyberspace, and international responsibility under international law. The article is based on the descriptive method, as well as analysis of sources, and documents.

Keywords: cyber security, hybrid warfare, Russia, information war.

Badanie nie otrzymało finansowania ze strony instytucji publicznych ani komercyjnych.

Adres do korespondencji: dr Joanna Worona, Uniwersytet w Białymstoku, ul. Świerkowa 20 B, 15-328 Białystok,
e-mail: joannaworona@onet.eu

Streszczenie

W ostatnich latach można zaobserwować wzmożoną aktywność Federacji Rosyjskiej w przestrzeni wirtualnej. W artykule podjęto próbę analizy sposobu wykorzystania przez Rosję cyberprzestrzeni w konfliktach hybrydowych. Przyjęto hipotezę, że rosyjska polityka cyberbezpieczeństwa wprawdzie przechodziła stopniową ewolucję, jednak jej kluczowe założenie sprowadza się do roli wzmocnienia działań na rzecz utrzymania i pogłębiania roli Rosji jako mocarstwa na świecie. Zidentyfikowano przykłady użycia przez Kreml cyberprzestrzeni zarówno poprzez inicjowanie cyberataków (w tym na inne państwa), jak i aktywny udział w wojnie informacyjnej prowadzonej z wykorzystaniem propagandy i manipulacji. Aktywna działalność Rosji spowodowała, że konieczne stało się zbadanie rosyjskiej polityki cyberbezpieczeństwa. W artykule przedstawione zostały pokrótce akty prawne Federacji Rosyjskiej, odnoszące się do bezpieczeństwa przestrzeni wirtualnej. Omówiono ponadto projekt stworzenia wewnętrznej, niezależnej od ogólnoświatowego Internetu, rosyjskiej sieci Runet. Odniesiono się również do kwestii odpowiedzialności międzynarodowej za niezgodne z prawem międzynarodowym wykorzystanie cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, konflikt hybrydowy, Rosja, wojna informacyjna.

Wprowadzenie

Zwiększenie znaczenia przestrzeni wirtualnej i jej wykorzystanie przez podmioty państwowe nadało nowy wymiar pilnej debacie na temat cyberbezpieczeństwa na poziomie państw. Federacja Rosyjska od kilku lat systematycznie jest uznawana za prekursora cyberataków. Zaryzykować można stwierdzenie, że korzenie globalnej potęgi cybernetycznej Rosji wywodzą się z rosyjskich doświadczeń w zakresie gromadzenia danych wywiadowczych oraz polityki wewnętrznej zdobytych w czasach ZSRR. Początkowo Internet był wykorzystywany przez rosyjskie władze jako narzędzie inwigilacji, monitorowania oraz zakłócania aktywizmu opozycjonistów i niezależnych mediów. Obecnie jest wykorzystywany również na arenie międzynarodowej.

Użycie cyberprzestrzeni przez Rosję ma wymiar zarówno aktywnych ataków (prawdopodobne cyberataki na infrastrukturę Gruzji, Estonii czy Ukrainy), jak i niejawnej manipulacji w czasie kampanii wyborczych (np. podejrzenie o ingerencję w trakcie wyborów prezydenckich w USA pomiędzy Donaldem Trumpem a Hilary Clinton w 2016 roku).

Celem niniejszego artykułu jest przedstawienie sposobów wykorzystywania cyberprzestrzeni przez Rosję do realizacji swoich celów politycznych. Analizie poddano rosyjską politykę cyberbezpieczeństwa i jej rozumienie przez rząd rosyjski. W artykule wykorzystano: analizę dokumentów prawnych Federacji Rosyjskich w kontekście opisywanego zagadnienia cyberbezpieczeństwa; następnie metodę porównawczą w aspekcie analizy skoordynowanych ataków skierowanych zagranicę ze strony rosyjskich służb w cyberprzestrzeni. Wykorzystano tu również metodę instytucjonalno-prawną odnoszącą się do wyjaśnienia funkcjonowania i kompetencji działań odpowiednio powołanych do celów bezpieczeństwa cybernetycznego instytucji w państwie rosyjskim.

Hipotezą główną pracy jest założenie, że rosyjska polityka cyberbezpieczeństwa wprawdzie przechodziła stopniową ewolucję, jednak jej kluczowe założenie sprowadza się do roli wzmocnienia działań na rzecz utrzymania i pogłębiania roli Rosji jako światowego mocarstwa.

Konflikty hybrydowe – zarys problematyki

Zagadnienie wojny hybrydowej zostało spopularyzowane przez Franka Hoffmana, który stwierdził, że: „zagrożeniem hybrydowym jest, gdy jakikolwiek adwersarz używający kombinacji broni konwencjonalnej, nieregularnej taktyki, terroryzmu i przestępczości, w tym samym czasie i na tym samym polu bitwy, celem osiągnięcia celów politycznych" (Hajduk, Stępniewski, 2015, s.136). Tego rodzaju konflikty mogą być prowadzone zarówno przez podmioty państwowe, jak i pozapaństwowe, przez pojedyncze oddziały, jak i złożone formacje. Walka prowadzona jest zaś z wykorzystaniem taktyk partyzanckich połączonych z nowoczesnymi technologiami wojskowymi (Skonieczny, 2015, s.42) Z kolei W.J. Nemeth pojęcie hybrydowości przedstawił w aspekcie funkcjonowania nowoczesnego społeczeństwa w trakcie trwania konfliktu rosyjsko-czeczeńskiego (Nemeth, 2002). W.J. Nemeth, oprócz specyficznej organizacji armii oraz wykorzystania siły militarnej (m.in. taktyk partyzanckich), jako cechę wojny hybrydowej wskazał umiejętność wykorzystania nowoczesnych technologii w działaniach taktycznych i strategicznych (Skonieczny, 2015, ss.41-42). Z kolei M. Wojnowski uznaje, że „główną cechą charakterystyczną wojny hybrydowej jest dążenie do maksymalnej zbieżności i synchronizacji metod, środków oraz sposobów prowadzenia operacji militarnych i pozamilitarnych w celu zwiększenia efektu synergii" (Wojnowski, 2015, s. 9).

W konfliktach hybrydowych niejednokrotnie wykorzystywana jest również walka informacyjna, na potrzeby niniejszego artykułu rozumiana jako działania mające na celu wpłynięcie na przeciwnika, jego zasoby informacyjne, systemy informatyczne i sieci komputerowe. W społeczeństwie informacyjnym opartym na wiedzy niezakłócony dostęp do informacji spełnia szczególną rolę. Znawcy tematu uznają, że „Informacja niszcząca jako narzędzie walki informacyjnej spełnia dwojaką funkcję: po pierwsze osłabia strukturę przeciwnika, przede wszystkim utrudniając przepływy informacji, zwłaszcza między społeczeństwem a wybranym przez nie kierownictwem, czy też decydentami a wykonawcami decyzji; po drugie inspiruje błędne decyzje decydentów i błędne działania wykonawców przez wprowadzenie do ich procesów informacyjnych błędnych algorytmów decyzyjnych i błędnych algorytmów działania, które osłabiają, a w skrajnych wypadkach doprowadzają do samozniszczenia państwa" (Gronowska-Starzeńska, 2017, s. 39).

Wykorzystanie przez Rosję wojny informacyjnej dokonuje się na kilku płaszczyznach – politycznej, wojskowej, dyplomatycznej, ekonomicznej oraz obecnie – w obszarze technologii informacyjnych. Cel jest niezmiennie ten sam – dezinformacja, spowodowanie paraliżu i niemożności obrony przeciwnika. Coraz większe uzależnienie krajów od poprawnego i niezakłóconego działania systemów informatycznych, oparcie infrastruktury krytycznej, komunikacji i innych najistotniejszych obszarów życia na systemach komputerowych sprawiło, iż utworzyła się nowa przestrzeń wpływów. Przestrzeń cyfrowa stała się nowym obszarem nie tylko prowadzenia ruchów wojennych, ale również wywierania wpływu na społeczeństwo.

Szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej Walerij Gierasimow w swoim artykule (Gierasimow, 2013) opisuje metody prowadzenia nowoczesnych wojen. W ocenie Gierasimowa coraz większe znaczenie należy przypisać niemilitarnym środkom działań wojennych, w tym manipulowaniu nastrojami lud-

ności zamieszkującej teren działań wojennych (propaganda). Działania te winny być wspierane przez wojnę informacyjną oraz operacje jednostek specjalnych. Nowoczesne technologie są wykorzystywane nie tylko w celu usprawnienia komunikacji pomiędzy dowództwem i siłami zbrojnymi, ale również do niwelowania potencjału bojowego przeciwnika (Skonieczny, 2015, s. 43). Podkreśla się również wagę działań niemilitarnych (presji ekonomicznej, aktywności służb specjalnych, wielokierunkowych działań dyplomatycznych i, w końcu, działań ofensywnych w cyberprzestrzeni prowadzonych zarówno przez służby specjalne, jak i hackerów) w konfliktach hybrydowych. Według Ł. Skoniecznego działania niemilitarne „mają na celu głównie oddziaływanie na ludność cywilną oraz społeczność międzynarodową. Ich zadaniem jest osłabianie woli oporu, zwiększanie poziomu zniechęcenia oraz niezadowolenia społecznego, co w rezultacie ma doprowadzić do zakończenia konfliktu zgodnie z interesem agresora" (Skonieczny, 2017, s. 47). Szczególną rolę w prowadzeniu konfliktów nabrała przestrzeń wirtualna. Y. Harrel uznaje, że „(…) cyberprzestrzeń pozwala korzystać z relatywnej dyskrecji, umożliwia uderzenie szybkie bądź z opóźnieniem, prowadzenie działań synchronicznych czy też asynchronicznych, osłabiających siły wroga" (Harrel, 2014, s. 149). Przestrzeń wirtualna poprzez swój globalny, transnarodowy i transgraniczny charakter oraz szybkość wymiany informacji w znaczący sposób zmieniła sposób komunikacji społecznej oraz sposób pozyskiwania informacji. Społeczeństwo czerpie informację nie tylko z oficjalnych kanałów komunikacji, takich jak prasa czy radio, lecz coraz częściej z Internetu i portali społecznościowych. Sieć zalewa fala nierzetelnych, niezweryfikowanych informacji, które potrafią być masowo udostępniane przez nieświadomych użytkowników sieci. Rosja wykorzystuje ten potencjał do szerzenia propagandy i dezinformacji, korzystając z faktu, że ustalenie autorów publikowanych treści (bądź ich mocodawców) jest trudne do ustalenia.

Wykorzystanie cyberprzestrzeni przez Rosję

Pierwszym znanym cyberatakiem szpiegowskim przeprowadzonym 10 września 1986 r., wówczas jeszcze przez służby radzieckie, było włamanie do systemu komputerowego obsługującego testy rakietowe sztandarowej obrony strategicznej Ronalda Reagana, nazywanej Gwiezdnymi Wojnami (ang. *Star Wars*) (Popescu, Secrieru, 2018, s. 9). Rosjan można również uznać za pionierów nowoczesnych działań propagandowo-informacyjnych. Ł. Skonieczny wskazuje, że: „Stworzyli oni (…) hierarchicznie zorganizowany system organów państwowych, instytucji naukowych oraz powiązanych z nimi mediów, który jest odpowiedzialny za wypracowywanie strategii, prowadzenie działań w zakresie walki informacyjnej i ich koordynowanie. Jego zadaniem jest zarówno kształtowanie oraz manipulowanie poglądami rosyjskiego społeczeństwa, jak i oddziaływanie na społeczność międzynarodową zgodnie z interesem Moskwy" (Skonieczny, 2015, s. 49). Celem zaś jest budowanie pozytywnego wizerunku Rosji, osłabianie współpracy państw członkowskich UE i NATO oraz zbudowania w społeczeństwie rosyjskim poczucia zagrożenia ze strony państw zachodnich.

W 2007 r. po raz pierwszy doszło do zmasowanego cyberataku na suwerenne państwo – Estonię. Pretekstem do ataku było przeniesienie z centrum Tallina pomnika

tzw. Brązowego Żołnierza, upamiętniającego żołnierzy Armii Czerwonej. Decyzja ta spowodowała spór polityczny na linii Tallin – Moskwa. Rosyjscy hackerzy w dniu 27 kwietnia 2007 r. zaatakowali serwery rządu estońskiego za poprzez zablokowanie możliwości dostępu do stron (tzw. atak DoS). Hackerzy przez trzy tygodnie blokowali dostęp do oficjalnych stron internetowych m.in. prezydenta, parlamentu i partii politycznych. Oprócz witryn rządowych zaatakowane zostały również największe banki, policja i niezależne gazety (Lakomy, 2010, s. 61). Podkreślić należy, że Estonia jest jednym z najbardziej zaawansowanych technologicznie krajów w UE. Ponad 95% transakcji odbywa się elektronicznie, dopuszcza się tam również możliwość internetowego głosowania w wyborcach. Z tych też względów atak miał wielką siłę rażenia i uniemożliwił znacznej części społeczeństwa m.in. dostęp do środków pieniężnych zgromadzonych w estońskich bankach. Efekt psychologiczny cyberataku był ogromny nie tylko dla Estończyków, ale również społeczności międzynarodowej. Po raz pierwszy w historii suwerenne państwo zostało ofiarą zmasowanego ataku dokonanego przez Internet. Przeprowadzone śledztwo potwierdziło znaczny stopień zorganizowania ataku, a jego źródła prowadziły do Rosji. Kreml jednakże zaprzeczył jakimkolwiek związkom z incydentem, choć nie ulega wątpliwości, iż był on stroną politycznego konfliktu związanego z przeniesieniem pomnika żołnierzy sowieckich. Konsekwencją niniejszego ataku było podjęcie przez rząd estoński szeregu kroków prawnych i organizacyjnych celem zapobieżenia podobnej sytuacji w przyszłości. Oprócz zmiany ustawodawstwa powołana została jednostka „cyberarmii" zrzeszająca obywateli (głównie informatyków), mająca na celu obronę estońskiej przestrzeni wirtualnej w przypadku wystąpienia kolejnego ataku.

Kolejnym przykładem zmasowanego ataku dokonanego przez powiązanych z rządem rosyjskich hackerów był cyberatak na Gruzję w 2008 r. W okresie tym toczyła się zbrojny konflikt pomiędzy Gruzją a Rosją z udziałem prorosyjskich republik separatystycznych Osetii Południowej i Abchazji. Rosja w czasie wojny w Gruzji obok tradycyjnych działań wojennych na lądzie, wodzie i w powietrzu zaatakowała również gruzińską przestrzeń wirtualną. Wejście rosyjskich wojsk do Osetii Południowej zbiegło się w czasie z hackerskim atakiem na rządowe gruzińskie strony internetowe prezydenta, ministra spraw zagranicznych oraz ministra obrony. Tak jak w przypadku Estonii, zaatakowane zostały również witryny komercyjne i media. Gruzini mieli ograniczony dostęp do Internetu i mediów, a przez to utrudnioną możliwość informowania społeczności międzynarodowej o sytuacji w kraju (Lakomy, 2010, ss. 62-63). Gruziński rząd w obronie przed cyberatakami podjął niekonwencjonalny krok przeniesienia swoich zasobów informatycznych do USA, Estonii i Polski (Korns, Kastenberg, 2008-2009, s. 60). Działania Rosji miały na celu zdobycie przewagi nad przeciwnikiem oraz ograniczenie możliwości przepływu informacji, wobec czego wpisują się w schemat działania w ramach wojny informacyjnej oraz działań hybrydowych.

Od czasu wybuchu proeuropejskiej pomarańczowej rewolucji Rosja podjęła kroki mające na celu zdestabilizowanie politycznie Ukrainy, zatrzymanie integracji z Zachodem i ugruntowanie swojej strefy wpływów w regionie. W 2014 r. w drodze użycia siły zbrojnej doszło do aneksji Krymu przez Rosję. Moskwa zastosowała wiele działań hybrydowych skierowanych przeciw ukraińskiej gospodarce i społe-

czeństwu przy wykorzystaniu działań informacyjnych. Prorosyjskie media stawiały tezy o możliwym bankructwie Ukrainy, korupcji, bezrobociu i załamaniu się ukraińskiego przemysłu. Niejednokrotnie odnoszono się również do teorii spiskowych jakoby za ukraińskim Majdanem stał Zachód czy też faszyści i bojówki banderowców. W wojnie informacyjnej Rosja nie tylko manipuluje obawami społecznymi czy mitami, ale również tworzy nieprawdziwe informacje (tzw. *fake news*), tak jak wówczas gdy „Rossija 1", powołując się na internetowy Cyber – Berkut, podała, że Euromajdan sfinansowany został z pieniędzy USA i oligarchów (Hajduk, Stępniewski, 2015, ss. 139-147). Obecnie Rosja w wojnie hybrydowej wykorzystuje całą gamę działań cybernetycznych – od szpiegostwa, poprzez inwigilację, operacje hackerskie oraz wykorzystanie mediów społecznościowych i działania dyplomatyczne. Twierdzi się nawet, iż działania te sprawiają, że Rosja stanowi większe zagrożenie dla europejskich państw niż jakikolwiek inny cyberprzestępca (Popescu, Secreriu, 2018, s. 10).

Przeprowadzone po 2016 r. śledztwo wykazało, że prawdopodobnie Rosja chciała również wpłynąć na wynik w wyborach prezydenckich w USA pomiędzy Hilary Clinton a Donaldem Trumpem. Próbowano wywrzeć wpływ na amerykańskich wyborców za pośrednictwem mediów społecznościowych i opłacanych przez Kreml farm trolli (m.in. zlokalizowanej w Sankt Petersburgu rosyjskiej organizacji IRA – Internet Research Agency). Rosjanie wykorzystali platformy społecznościowe (tj. YouTube, Facebook, Twitter, Instagram) do polaryzacji amerykańskiego społeczeństwa na bazie różnic społecznych, ideologicznych i rasowych, publikując wysoce stronnicze, kontrowersyjne treści, m.in. na temat dostępu do broni palnej czy tożsamości płciowej. Celem było faworyzowanie jednego kandydata, by pomóc D. Trumpowi w zwycięstwie. W konsekwencji Komisja ds. Wywiadu Senatu USA opublikowała raport wskazujący na powiązania IRA z rosyjskim rządem i udzielanie przez Kreml wsparcia finansowego w prowadzeniu działań mających na celu wpłynięcie na niezależne wybory prezydenckie. Trudno ocenić, w jakim stopniu działania Rosji przyczyniły się do zmiany decyzji amerykańskich wyborców, jednakże z całą pewnością taka forma wywierania wpływu na demokratyczny proces wyborczy innego państwa jest działaniem bezprecedensowym. W reakcji na incydenty Senat USA zalecił przeprowadzenie audytu rozwiązań prawnych gwarantujących możliwość ustalenia sponsora reklam politycznych czy też funkcjonowania platform społecznościowych w zakresie profilowania ich użytkowników.

Wolność słowa w Rosji, w przeciwieństwie do państw Zachodu, często jest w znacznym stopniu ograniczana przez władze państwowe. Niezależne media krytykujące politykę rządu są atakowane i likwidowane, opozycjoniści, niezależni dziennikarze są szykanowani, zastraszani i nierzadko aresztowani. J. Hajduk i T. Stępniewski stoją na stanowisku, że najważniejsze rosyjskie stacje telewizyjne, radiowe i ogólnokrajowe gazety są podporządkowane interesom Kremla. Rosyjska przestrzeń informacyjna ma za cel sprzyjanie interesom grupy rządzącej. Podkreśla się że: „Wszystkie te media w swojej polityce redakcyjnej kierują się zasadą pozytywnego przedstawienia poczynań rządu i prezydenta Putina. W tym celu stosują znane mechanizmy propagandy, wywodzące się jeszcze ze Związku Radzieckiego, udoskonalają je przez korzystanie z nowych technologii przekazywania informacji. Manipulując symbolami, posługując się półprawdami albo kłamstwami, stawiają

sobie za cel wpływanie na »zbiorowe podstawy«" (Hajduk, Stępniewski, 2015, s. 138). Media rosyjskie kreują wizerunek Rosji jako mocarstwa, a jakakolwiek próba walki przeciwko temu państwu jest z góry skazana na porażkę.

Nie ulega również wątpliwości, iż Kreml w swej polityce korzysta z cyberataków prowadzonych nie tylko przez formacje państwowe. Tajne służby zaczęły zlecać operacje hackerskie i cyberataki grupom nieformalnym – aktywistom, hackerom, grupom przestępczym. Dziennikarskie śledztwa dowiodły tworzenia tzw. farm trolli, którzy z fikcyjnych profili rozpowszechniają nieprawdziwe informacje, tzw. *fake news*. Rosyjscy trolle mają za zadanie wpłynąć na innych internautów poprzez ich ośmieszanie bądź obrażanie, pochwalanie władz kremlowskich i deprecjonowanie opozycji i Zachodu. Trolle działają zazwyczaj w trzyosobowych grupach, dziennie publikując około 130 komentarzy, każdy po 300 znaków zawierających słowa-klucze. W trzyosobowej grupie pojawia się jeden „zły troll", który neguje działania Rosji, oraz dwa dobre trolle, które bronią działań Kremla (Zalewski, 2016, s. 214).

Działania hakerów i internetowych trolli służą do atakowania politycznych oponentów, dezinformacji i zmniejszaniu politycznej mobilizacji przeciwko reżimowi. Działania te pozwoliły obniżyć koszty operacji oraz utrudnić możliwość wyśledzenia prawdziwego zleceniodawcy operacji. Część operacji bezpośrednio wskazywała na rosyjskie tajne służby (tj. podsłuchiwanie opozycji), w innych przypadkach zaś (cyberatak na Estonię w 2007 r., ingerencja w wybory prezydenckie USA w 2016 r.) powiązania z rosyjskimi władzami nie były tak oczywiste (Soldatov, Borogan, 2018, ss. 18-19). Rosyjska cyberstrategia obejmuje ofensywne działania w sieci w celu realizowania wewnętrznej i międzynarodowej polityki Kremla. Klasyczną propagandę zastąpił „trolling", który przez unikanie prawdy oraz wykorzystywanie niejednoznaczności stał się powszechną taktyką polityczną.

Farmy trolli wykorzystane były m.in. po zamordowaniu w lutym 2015 r. przywódcy opozycji Borysa Niemcowa. Powiązanie jego zabójstwa z Kremlem mogłoby poważnie zaszkodzić władzom rosyjskim. W marcu 2015 r. rosyjska niezależna prasa opublikowała listy kont trolli wraz z instrukcją działania. Trolle miały za zadanie rozpowszechnić pogląd, iż władza rosyjska nie mogła zyskać na zabójstwie; popularyzowane miało być stanowisko, że to opozycja będzie czerpać korzyści ze śmierci Niemcowa, w sprawę są zaangażowani obywatele Ukrainy, a zachodni politycy wykorzystują jego śmierć do bezprawnej ingerencji w sprawy wewnętrzne Rosji. Trolle wykorzystując fikcyjne profile prywatne, publikowały treści na internetowych forach, które miały wyglądać na dyskusję zwykłych obywateli. Celem było sianie niezgody, dezinformacji oraz uniemożliwienie rozróżnienie fikcji od prawdy (Kurowska, Reshetnikov, 2018, s. 28). Podobne metody stosowane są poza granicami Rosji dzięki fikcyjnym kontom na Twitterze i Facebooku. Celem wojny informacyjnej jest m.in. indoktrynacja i modelowanie obrazu rzeczywistości zgodnego z interesem Kremla oraz celami politycznymi i wojskowymi, a także wpływanie na procesy decyzyjne innych podmiotów państwowych.

Kreml konsekwentnie zaprzecza używaniu cyberataków do swojej gry politycznej. Skutkiem agresywnej taktyki cybernetycznej jest utrata zaufania do rosyjskich organów ścigania, tajnych służb oraz organów rządowych wśród zachodnich ekspertów do spraw cyberbezpieczeństwa. Jednocześnie Rosja jest postrzegana jako główny

podejrzany w przypadku wystąpienia każdego cyberataku na Zachodzie, co buduje wizerunek agresywnego aktora polityki zagranicznej (Soldatov, Borogan, 2018, s. 22).

Rosyjska polityka dotycząca cyberbezpieczeństwa

W tym miejscu należy pokrótce przedstawić podstawy polityki dotyczącej cyberbezpieczeństwa Rosji. W Koncepcji bezpieczeństwa narodowego Federacji Rosyjskiej z 1997 r. określono interesy narodowe istotne do budowy rosyjskiego społeczeństwa informacyjnego. Jednym z punktów był „rozwój nowych technologii informatycznych służących skutecznemu oddziaływaniu na terytoria mające szczególną rangę dla rosyjskich stref wpływów i stref interesów oraz konsolidowania państwa-organizacji wieloetnicznego narodu rosyjskiego. Obowiązek tworzenia nowych kanałów komunikacyjnych z udziałem najnowszej technologii cyfrowej stanowił oś przygotowywanej strategii wojny informacyjnej, dla której prymarnym celem była obrona terytorialności rosyjskich interesów, ochrona dziedzictwa kulturowego" (Zalewski, 2016, s. 208). Dokument ten potwierdzał, że mimo upadku Związku Radzieckiego Rosja nie zamierza rezygnować ze statusu mocarstwa i swojej strefy wpływów. Również w wydanej w 2014 r. Doktrynie wojennej Federacji Rosyjskiej za zagrożenie dla bezpieczeństwa kraju uznano stosowanie przez Zachód wojny hybrydowej oraz ekspansję NATO na rosyjską strefę wpływów. Wobec powyższego podkreślono konieczność opracowania: „nowych, nietradycyjnych metod łączących środki wojskowe i niewojskowe w czterowymiarowej przestrzeni walki" (Żochowski, 2015, s. 76). Do metod tych z całą pewnością należy zaliczyć wykorzystanie cyberprzestrzeni do osiągnięcia założonych celów.

Podłoże rosyjskiej polityki cyberbezpieczeństwa upatruje się w 2000 r. w drugiej wojnie czeczeńskiej. Władimir Putin niepowodzeniem pierwszej wojny czeczeńskiej obwinił niezależne media, zdradzając głęboką nieufność i antagonizm wobec niezależnych mediów. Rosyjskie władze uznały, że wygrana w Czeczeni zależy od ściślejszej kontroli niezależnych mediów, a informacja winna być traktowana jako broń w konflikcie informacyjnym. Wobec nowego podejścia wojna została przemianowana na „operację antyterrorystyczną", zasady akredytacji dla dziennikarzy zostały zaostrzone, ograniczono również dostęp do Czeczenii zagranicznych dziennikarzy. Rosyjskie media, które nie wpisywały się w linię rządową były szykanowane, dziennikarze zwalniani bądź oskarżani o popełnienie przestępstw (Soldatov, Borogan, 2018, ss. 15-16).

W 2000 r. Władimir Putin podpisał dokument o nazwie Doktryna bezpieczeństwa informacji Federacji Rosyjskiej (Doktryna bezpieczeństwa informacji FR, 2000), w którym wyszczególniono listę zagrożeń, tj. osłabienie duchowego, moralnego i twórczego potencjału twórczości rosyjskiej czy też manipulacja informacjami. Rozpowszechnianie informacji niezgodnych z polityką Kremla (w tym przez niezależne media) mogło zostać uznane za zagrożenie dla bezpieczeństwa narodowego Rosji. W 2002 r. dział cyberwywiadu FSB został zmieniony na Centrum Bezpieczeństwa Informacji (ang. Information Security Centre). Z kolei w 2013 r. rosyjskie Ministerstwo Obrony ogłosiło plany utworzenia oddziałów „cyberżołnierzy"(Doktryna Bezpieczeństwa Informacji…, 2000), tj. żołnierzy, którzy mieliby za zadanie odpieranie cyberataków, ale również ich przeprowadzanie.

Nie mniej istotna dla władz na Kremla jest ochrona własnej infrastruktury krytycznej i systemów komputerowych. W dniu 12 grudnia 2014 r. Władimir Putin zatwierdził *Koncepcję państwowego systemu wykrywania, zapobiegania i likwidacji skutków ataków komputerowych na zasoby informacyjne FR*. Zgodnie z niniejszym dokumentem zwalczanie cyberzagrożeń jest jednym z głównych zadań Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej. Kreml wyraził potrzebę stworzenia bezpiecznego systemu informatycznego przeznaczonego wyłącznie dla rosyjskich instytucji państwowych (Żochowski, 2015, s. 79).

Co ciekawe, po uruchomieniu wojskowego Internetu baz niejawnych w 2016 r. rozpoczęła się realizacja projektu stworzenia wewnętrznej rosyjskiej sieci o nazwie Runet odciętej od globalnego Internetu. Ustawa o działaniu Internetu w warunkach izolacji od sieci globalnej została przyjęta w kwietniu 2019 r., a pierwsze testy zostały zaplanowane na listopad 2019 r. Ustawa zakłada, że w razie zagrożenia zarządzanie rosyjską cyberprzestrzenią zostanie przejęte przez Urząd Roskomnadzor, który obecnie jest odpowiedzialny za regulację mediów i Internetu w Rosji. Ponadto w Runecie zostanie utworzone podległe Roskomnadzorowi centrum monitoringu, którego zadaniem będzie zarządzanie siecią wirtualną w sytuacjach kryzysowych. Ustawa zakłada utworzenie wykazu punktów wymiany ruchu internetowego między globalnymi i rosyjskimi sieciami. Całość rosyjskiego ruchu internetowego będzie przechodziła przez wskazane punkty ujawnione w rejestrze, do którego będą należeć wyłącznie te punkty, które spełnią kryteria podane przez FSB. Przewiduje się również stworzenie systemu domen internetowych, niezależnego od światowej organizacji ICANN (Forbes, 2019). W oficjalnych stanowiskach powołanie Runetu miałoby zapewnić bezpieczeństwo rosyjskiej sieci internetowej niepodatnej na ataki z zewnątrz, jednak Runet może prowadzić do całkowitej kontroli przepływu informacji w rosyjskiej cyberprzestrzeni oraz blokowania niechętnych Kremlowi treści, w tym mediów niezależnych. Władze będą również mogły „wyłączyć" jakiś adres IP bez udziału operatora. Podobne rozwiązania przyjęte są obecnie w Chinach (tzw. pakiet ustaw nazywany Great Firewall of China), gdzie władze od lat cenzorują chińskim internautom dostęp do niewygodnych dla siebie treści. Wydaje się, że to prawdziwym celem stworzenia Runetu nie jest ochrona przed cyberatakami, lecz właśnie zdobycie władzy nad treściami publikowanymi w rosyjskiej przestrzeni wirtualnej.

W dniu 5 grudnia 2016 r. dekretem prezydenta Rosji nr 646 ustanowiono Doktrynę bezpieczeństwa informacyjnego Federacji Rosyjskiej (Doctrine of Information Security of the Russian Federation, 2016). Doktryna określa strategiczne cele i kluczowe obszary bezpieczeństwa informacji, uwzględniając strategiczne priorytety narodowe Federacji Rosyjskiej oraz stanowi podstawę opracowania środków mających na celu poprawę bezpieczeństwa informacji. W rozdziale III Doktryny, wskazującym na najważniejsze zagrożenia informatyczne bezpieczeństwa Rosji, wskazano, że technologie informacyjne przyczyniają się do wzrostu gospodarczego, lecz równocześnie transgraniczny przepływ informacji jest wykorzystywany do celów geopolitycznych, terrorystycznych, eksternistycznych i przestępczych. Stwierdzono, że część państw buduje potencjał informatyczny w celu wpłynięcia na infrastrukturę informacyjną oraz rosyjskie organy rządowe i rosyjski przemysł. W pkt. 12 odnotowano, że zagraniczne media coraz częściej publikują stronnicze materiały o polityce Rosji, rosyjskie media spotykają się z dyskryminacją za granicą, a rosyjskim dziennikarzom uniemożliwia się

wykonywanie swoich obowiązków. W pkt. 13 dokumentu zwrócono uwagę na wykorzystanie cyberprzestrzeni do wywierania wpływu na społeczeństwo w celu rozbudzenia napięć międzyetnicznych, społecznych oraz religijnych, jednakże winą obarczono jedynie organizacje terrorystyczne i ekstremistyczne. Bezpieczeństwo informacji w dziedzinie obrony narodowej charakteryzuje się rosnącym wykorzystaniem przez niektóre państwa i organizacje technologii informatycznych do celów wojskowych i politycznych, w tym do działań niezgodnych z prawem międzynarodowym i mających na celu podważenie suwerenności, stabilności politycznej i społecznej oraz terytorialnej integralność Federacji Rosyjskiej i jej sojuszników. Podkreślono, że zwiększa się liczba cyberataków, w tym na infrastrukturę krytyczną, a działalności wywiadów obcych państw w Rosji zwiększa ryzyko wykorzystania technologii informacyjnych do naruszenia suwerenności, integralności terytorialnej lub stabilności politycznej i społecznej Federacji Rosyjskiej. Jako zagrożenie wskazano również uzależnienie się od zagranicznych technologii (komputerów, oprogramowania itp.) oraz brak konkurencyjności rodzimych rozwiązań.

W rozdziale IV Doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej wskazano cele strategiczne i kluczowe obszary zapewnienia bezpieczeństwa informacji. Głównym celem jest zapewnienie bezpieczeństwa informacji przed zagrożeniami związanymi z wykorzystaniem technologii do celów wojskowych i politycznych, w tym ataków podważających suwerenność i integralność terytorialną państw. W pkt. 21 opisano politykę wojskową Rosji, określającą kluczowe obszary zapewniające bezpieczeństwo informacji w dziedzinie obrony narodowej:

a) zapewnienie strategicznego odstraszania i zapobieganie konfliktom zbrojnym, które mogą wynikać z zastosowania technologii informatycznych;
b) modernizacja systemu bezpieczeństwa informacji Sił Zbrojnych, innych żołnierzy, formacji i organów wojskowych, w tym sił i środków służących do konfrontacji informacji;
c) prognozowanie, identyfikowanie i ocena zagrożeń informacyjnych, w tym zagrożeń dla sił zbrojnych Rosji,
d) promowanie interesów sojuszników Federacji Rosyjskiej w sferze informacyjnej;
e) informacje równoważące i działania psychologiczne, w tym mające na celu podważenie historycznych podstaw i patriotycznych tradycji związanych z obroną ojczyzny.

Jako główne cele w pkt. 24 wymieniono powstrzymanie szkodliwej działalności zagranicznych służb i osób fizycznych korzystających z technologii informacyjnych, zwiększenie ochrony i bezpieczeństwa działania infrastruktury krytycznej, sprzętu wojskowego, systemów kontroli. Jako jeden z celów wymieniono ponadto poprawę bezpiecznego działania obiektów infrastruktury informacyjnej, w tym w celu zapewnienia stabilnej interakcji między organami rządowymi, zapobiegania zagranicznej kontroli nad tymi obiektami oraz zapewnienia integralności, płynnego działania i bezpieczeństwa zunifikowanej sieci telekomunikacyjnej Federacji Rosyjskiej, jak i zapewnienie bezpieczeństwa informacji przesyłanych przez tę sieć i przetwarzanych w ramach systemów informatycznych na terytorium Federacji Rosyjskiej. Istotnym stała się też ochrona „rosyjskiego punktu widzenia" poprzez neutralizowanie

wpływu informacji mających na celu zniszczenie tradycyjnych rosyjskich wartości. W pkt. 25 uznano również, że konieczne jest opracowanie konkurencyjnej bazy krajowych rozwiązań technologicznych, produktów IT i promowanie ich na rynku globalnym.

Odpowiedzialność za wykorzystanie cyberprzestrzeni

Prawo międzynarodowe publiczne nie reguluje kwestii konfliktu czy wojny hybrydowej, wobec czego brak jest odpowiednich mechanizmów reagowania społeczności międzynarodowej. Przypisanie odpowiedzialności za cyberatak jest niezmiernie problematyczne. By obciążyć państwowy podmiot odpowiedzialnością za postępowanie niezgodne z zobowiązaniami międzynarodowymi, spełnione muszą być dwa warunki: po pierwsze konieczne jest uznanie, iż akt bezprawny stanowi naruszenie międzynarodowych zobowiązań państwa, po drugie niezbędna jest możliwość przypisania działania państwu. Przypisanie takiej odpowiedzialności może być stosowane w przypadku wystąpienia konfliktów zbrojnych i jest uważane za jeden z wymogów prawnych możliwości zastosowania prawa do samoobrony opisanej w art. 51 Karty Narodów Zjednoczonych (Dz.U. 1947 nr 23 poz. 90). Wszelkie działania państwowe odnoszące się do tego artykułu muszą być uzasadnione wiarygodną identyfikacją źródła ataku. Tylko w razie dostarczenia takich dowodów uznaje się, że państwa mają niepozbywalne prawo do samoobrony indywidualnej lub zbiorowej, a zatem mogą podjąć kroki w kierunku odpowiedniej reakcji na zagrożenia (Herpig, Reinhold, 2018, s. 34).

Przyznanie odpowiedzialności międzynarodowej za cyberatak konkretnemu państwu może być żmudnym, problematycznym procesem. Wiąże się to z koniecznością przedstawienia konkretnych danych wywiadowczych i technicznych celem ich przedstawiania na arenie międzynarodowej. Dopiero publicznie ujawnienie wiarygodnych informacji i uzyskanie poparcia sojuszników umożliwia rządowi podjęcie takich kroków prawnych jak wydalenie dyplomatów czy wprowadzenie sankcji gospodarczych (Herpig, Reinhold, 2018, s. 34). Gromadzenie dowodów dokonania cyberataku może być niezwykle trudne, nie tylko pod względem technicznym, jak i prawnym. Brak jest bowiem międzynarodowych rozwiązań legislacyjnych dotyczących cyberataków oraz zabezpieczania cyfrowych śladów. Najważniejszym aktem międzynarodowym odnoszącym się do przestępstw dokonanych w cyberprzestrzeni jest *Konwencja o cyberprzestępczości* z 23 listopada 2001 r. (Dz.U. 2015 poz. 728). Ten akt prawny odnosi się głównie do przestępstw pospolitych, nie poruszając kwestii szpiegostwa czy cybernetycznej działalności wojskowej.

Wobec zwiększającej się liczby cyberataków na infrastrukturę krytyczną państw, w trakcie odbywającego się w Warszawie szczytu NATO w 2016 r. uznano, że cyberatak na państwo członka Sojuszu może być uznane za naruszenie art. 5 traktatu północnoatlantyckiego (Dz.U. 2000 nr 87 poz. 970) stanowiącego, iż atak na jedno państwo członkowskie jest agresją wymierzoną w cały Sojusz (zasada *casus foederis*). Cyberprzestrzeń została uznana za obszar działań zbrojnych, a w konsekwencji podkreślono konieczność wzmocnienia cyberobrony sieci krajowych oraz infrastruktury krytycznej. Polityka NATO dotycząca przestrzeni wirtualnej opiera się na założeniu, że tylko ścisła współpraca Sojuszu i dzielenie się wiedzą pozwoli na zabezpieczenie cyberprzestrzeni państw członkowskich i bezpieczeństwo całego Sojuszu.

W przypisaniu odpowiedzialności za cyberatak, oprócz danych wywiadowczych i aspektów technicznych, może również pomóc geopolityka (choć oczywiście nie zastąpi ona rzetelnych dowodów). Po wystąpieniu ataku należy również zadać sobie pytanie, kto na nim skorzysta – analiza taka winna uwzględniać aspekt polityczny, trwające konflikty, negocjacje oraz bieżące wydarzenia. Rosja jest wskazywana jako inicjator cyberataków właśnie z tego powodu, że zyskuje ona na większości z nich. Celem Kremla jest destabilizacja zachodnich demokracji i odwrócenie uwagi od sytuacji politycznej w kraju. Innym aspektem oceny geopolitycznej jest ustalenie, czy nie mamy do czynienia z „fałszywą banderą", tj. sytuacją, gdy atakujący podszywa się pod inny podmiot. Wówczas konieczne jest ustalenie, kto skorzysta z cyberataku, w przypadku gdy inny, najbardziej oczywisty aktor zostanie obwiniony za atak. Znawcy tematu wskazują, iż dość łatwo można zmanipulować pewne aspekty techniczne (znaczniki czasu, konfiguracje języka, kody, komentarze) tak, by wskazywały na inny podmiot. Jako przykład takiego działania przypisywanego Rosji można wskazać operację Olimpic Destroyer, mającą na celu zakłócenie otwarcia Zimowych Igrzysk Olimpijskich w Korei Południowej. W trakcie operacji hackerzy prawdopodobnie wykorzystali podobne aspekty techniczne do tych zastosowanych przez Koreę Północną w poprzednich cyberatakach, dzięki czemu winą za atak można było obarczyć Pjongjang. Jeżeli faktycznie moglibyśmy przypisać niniejszy atak Rosji to zastosowanie „fałszywej bandery" było sprytnym posunięciem mającym na celu zaognienie konfliktu między Koreami, a w konsekwencji skupienie uwagi USA właśnie na tym regionie świata (zamiast Rosji) (Herpig, Rheinhold, 2018, ss. 39-40).

Przez ostatnią dekadę Rosja była wielokrotnie uznawana za agresora w cyberprzestrzeni. Przypisanie odpowiedzialności Kremlowi oznacza nie tylko zebranie technicznych dowodów oraz danych wywiadowczych, ale również przekonanie społeczności międzynarodowej. Przypisanie odpowiedzialności za tradycyjny atak zbrojny jest stosunkowo łatwe, w przypadku zaś wykorzystania cyberprzestrzeni bardzo utrudnione, czasami zaś niewykonalne. Przestrzeń wirtualna oferuje agresorom możliwość zacierania śladów i wykorzystywania infrastruktury informatycznej podmiotu trzeciego. Państwa obwiniane za atak często dystansują się od grupy hackerskiej, która przeprowadziła operację, zaprzeczając jakimkolwiek powiązaniom.

Podsumowanie

Rosyjska polityka w cyberprzestrzeni początkowa miała na celu gromadzenie informacji, obecnie stanowi filar polityki wewnętrznej i zewnętrznej Federacji Rosyjskiej. Na arenie międzynarodowej przestrzeń wirtualna wykorzystywana jest do ingerencji w fundamenty polityczne adwersarzy, w polityce wewnętrznej zaś do budowania pozytywnego wizerunku Kremla i walki z opozycją. Używanie przestrzeni wirtualnej w konfliktach hybrydowych skutecznie zmierza do osiągnięcia zamierzonych celów przy wielokrotnie mniejszych kosztach politycznych, ekonomicznych i wizerunkowych. Cyberataki zaś pozwalają na bardzo szeroki zakres oddziaływania przy małych kosztach. Nie mniej istotne jest to, że anonimowość sieci powoduje ukrycie zleceniodawców ataku, co oczywiście ułatwia utrzymanie odpowiedniego wizerunku na arenie międzynarodowej.

Rosjanie są gotowi poddać się wielu wyrzeczeniom, byleby zachować status mocarstwa. Rosyjskie społeczeństwo stosunkowo łatwo ulega propagandzie, zwłaszcza że część mediów jest kontrolowana przez Kreml. Szeroko zakrojona propaganda i ograniczony dostęp do niezależnych mediów kreuje rosyjską rzeczywistość na tyle, że 65-70% Rosjan zaprzecza udziałowi Rosji w konflikcie na Ukrainie (Darczewska, 2015, s. 60). Internet jest wykorzystywany nie tylko do przeprowadzania cyberataków, ale również do kształtowania nowej rzeczywistości.

Dezinformacja w znaczny sposób destabilizuje sytuację w atakowanych państwach i negatywnie wpływa na procesy decyzyjne na najwyższych szczeblach władzy. Szerzenie dezinformacji za pomocą cyberprzestrzeni, szczególnie z udziałem mediów społecznościowych, pozwala na manipulowanie społeczeństwem na masową skalę. Tym, co wyróżnia Rosję na tle innych państw, jest wykorzystanie w realizacji swojej polityki hackerów oraz farm trolli. Agresywna działalność Rosji w przestrzeni wirtualnej bez wątpienia negatywnie wpływa na stabilność sytuacji międzynarodowej oraz bezpieczeństwo międzynarodowe. Działalność ta będzie prawdopodobnie dalej kontynuowana. Polityka Putina jawi się bowiem jako geopolityczna, euroazjatycka, nastawiona na konfrontację z Zachodem i umacnianie rosyjskiej strefy wpływów. To z kolei będzie wymuszać na adwersarzach Rosji zwiększenie cyberbezpieczeństwa państw i wprowadzenie polityk mających na celu niwelowanie skutków ataku.

BIBLIOGRAFIA

1. Darczewska, J. (2015). Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie? *Przegląd Bezpieczeństwa Wewnętrznego Wydanie specjalne – Wojna hybrydowa*, 59-73.
2. *Doctrine of Information Security of the Russian Federation* December 2016 (2016). Pobrane z: http://www.scrf.gov.ru/security/information/DIB_engl/
3. *Doktryna bezpieczeństwa informacji Federacji Rosyjskiej* (zatwierdzony przez Prezydenta Federacji Rosyjskiej w dniu 9 września 2000 r. N Pr-1895) (2019) Pobrane z: http://base.garant.ru/182535/
4. *Rosja będzie mieć własny Internet*. (2019, April 22). Forbes Pobrane z: https://www.forbes.pl/technologie/rosja-wprowadzi-runet-czyli-internet-dzialajacy-w-izolacji/v3tk1sh
5. Gierasmow, W. (Герасимов, В)., *Cennost' nauki v predvidenii, „Voenno-promyšlennyj kur'er" (Ценность науки в предвидении, „Военно-промышленный курьер")* z 27.02.2013 r., Pobrane z: http://www.vpk-news.ru/articles/14632, (2019) Tłumaczenie na język angielski podane z https://inmoscowsshadows. wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
6. Gronowska-Starzeńska, A. (2017). Walka informacyjna – wybrane problemy w ujęciu cybernetycznym. *Zeszyty Naukowe ASzWoj*, 4(109), 36-45.
7. Hajduk, J., Stępniewski, T. (2015). Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty. *Studia Europejskie*, 4(76), 135-151.
8. Harrel, Y. (2014). *Rosyjska cyberstrategia*. Warszawa: Wydawnictwo DiG.
9. Herpig, S., Reinhold, T. (2018). Spotting the bear: credible attribution and Russian operations in cyberspace, W: N. Popescu, S. Secrieru (Eds.), *Hacks, Leaks and Disruption Russian Cyber Strategies* (33-43), Chaillot Papers No 148. European Union Institute for Security Studies.

10. Hoffman, F. (2014). On Not-So-New Warfare: Political Warfare vs. Hybrid Threats, *War on the Rocks*, 28 July 2014, Pobrane z: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/
11. *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* Dz.U. 1947 nr 23 poz. 90.
12. *Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie z dnia 23 listopada 2001 r.* Dz.U. 2015 poz. 728
13. Korns, S. W., Kastenberg, J. E., (2009). Georgia's Cyber Left Hook, *Parameters*, Winter 2008-2009, XXXVIII(4), 60-76.
14. Kossecki, J. (1997). *Totalna wojna informacyjna XX wieku a II RP*. Kielce: Wydział Zarządzania i Administracji Wyższej Szkoły Pedagogicznej im. J. Kochanowskiego w Kielcach.
15. Kurowska, X., Reshetnikov, A. (2018) Russia's trolling complex at home and abroad. W: N., Popescu, S., Secrieru (Eds.), *Hacks, Leaks and Disruption Russian Cyber Strategies* (25-32), Chaillot Papers No 148. European Union Institute for Security Studies.
16. Lakomy, M. (2010). Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku. *Stosunki Międzynarodowe*, 3-4(42), 55-71.
17. Nemeth, W.J. (2002). *Future war and Chechnya: A case for hybrid warfare*. Pobrane z: http:// calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1
18. Popescu, N., Secrieru, S. (2018). Introduction: Russia's cyber prowess – where, how and what for? W: N. Popescu, S. Secrieru (Eds.), *Hacks, Leaks and Disruption Russian Cyber Strategies* (9-14), Chaillot Papers No 148. European Union Institute for Security Studies.
19. Skonieczny, Ł. (2015). Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia. *Przegląd Bezpieczeństwa Wewnętrznego Wydanie specjalne – Wojna hybrydowa*. 39-50. http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,PrzegladBezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html
20. Soldatov, A., Borogan, I. (2018) Russia's approach to cyber: the best defence is a good offence, W: N. Popescu, S. Secrieru (Eds.), *Hacks, Leaks and Disruption Russian Cyber Strategies* (15-24), Chaillot Papers No 148. European Union Institute for Security Studies.
21. *Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r.* Dz.U. 2000 nr 87 poz. 970.
22. *Wojennaja Doktrina Rossijskoj Federacji (Военная доктрина Российской Федерации)*. Pobrane z: http://www.rg.ru/2014/12/30/doktrina-dok.html
23. Wojnowski, M. (2015). Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku. *Przegląd Bezpieczeństwa Wewnętrznego Wydanie specjalne – Wojna hybrydowa*. 7-38. http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,PrzegladBezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html
24. Zalewski, J. (2016), Intoksykacja psychologiczno-informacyjna z elementem wojny informacyjnej prowadzona przez Federację Rosyjską. *Studia Bezpieczeństwa Narodowego*, VI(9), 201-220.
25. Żochowski, P. (2015). Rosyjska „niewypowiedziana wojna" – konsekwencje dla sektora siłowego FR, *Przegląd Bezpieczeństwa Wewnętrznego Wydanie specjalne – Wojna hybrydowa*. 74-84. http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,PrzegladBezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html