Cybulski, M.A., Maciorowska, M., 2021. *Wykorzystanie cybertechnologii w walce informacyjnej przez Rosję*, Przegląd Geopolityczny, 38, s. 116-131.

Michał A. CYBULSKI
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Martyna MACIOROWSKA
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

WYKORZYSTANIE CYBERTECHNOLOGII W WALCE INFORMACYJNEJ PRZEZ ROSJĘ

Abstrakt:

Rozwój nowoczesnych technologii fundamentalnie zmienił oblicze i postrzeganie walki informacyjnej. Powstanie i rozwijanie cyberprzestrzeni jako platformy szybkiego obiegu informacji dało niezwykłą sposobność do wykorzystania jej w prowadzeniu działań militarnych. Sama walka informacyjna ma przede wszystkim w pożądany przez daną stronę sposób wpływać na przeciwnika, wywoływać u niego oczekiwane przez agresora reakcje. Wykorzystanie środków i sił nowego rodzaju prowadzenia wojny nie skupia się na ich niszczycielskim charakterze, lecz sprowadza się do zakłócania przebiegu informacji, blokowania dostępu do systemów i sieci informacji, w celu pozbawiania przeciwnika kontroli nad własnymi zasobami informacyjnymi. Państwem w szczególny sposób wykorzystującym cybertechnologię jest Federacja Rosyjska. Celem opracowania jest próba sformułowania odpowiedzi na następujące pytania: dlaczego Rosja Władimira Putina rozwija narzędzia wojny informacyjnej? Dlaczego są one warte rozwijania? Jak, w odróżnieniu od państw zachodnich, Rosja pojmuje wojnę informacyjną? Jak Federacja Rosyjska wykorzystuje cybertechnologię do prowadzenia działań operacyjno-strategicznych? Zrozumienie kierunku przeobrażania się współczesnego pola bitwy wskazuje na potrzebę przygotowywania się na mogące wystąpić w przyszłości nowe rodzaje prowadzenia wojny.

Słowa kluczowe: walka informacyjna, cybertechnologia, Federacja Rosyjska, informacja, bezpieczeństwo informacyjne

Wstęp

Federacja Rosyjska w licznych publikacjach naukowych przedstawiana jest jako państwo tak zwanego „miękkiego autorytaryzmu", które aspiruje do przywrócenia systemu totalitarnego. Władze rosyjskie wykorzystują różnego rodzaju psychologiczne metody

wobec własnego narodu, z jednej strony dążąc do odbudowy mocarstwowości oraz zrozumienia takiego stanu rzeczy, natomiast z drugiej budując poczucie stałego zagrożenia, dzięki czemu są w stanie uzasadnić metody i charakter własnych działań. Podtrzymywanie syndromu „oblężonej twierdzy", rozumiane jako przeświadczenie o obecności wroga blisko granicy własnego terytorium i zagrażającego wewnętrznym interesom państwowym, a także wskazywanie ideologicznych zagrożeń z „Zachodu", usprawiedliwia potrzebę kosztownego militaryzowania się i rozbudowy tzw. sektorów siłowych. W celu spełnienia swoich imperialnych aspiracji Federacja Rosyjska stosuje także wyszukane metody walki informacyjnej, oddziałując za ich pomocą na własne społeczeństwo jak i na państwa zachodnie.

Koncepcja walki informacyjnej stała się zagadnieniem intensywnie dyskutowanym w państwach zachodnich od samego początku kryzysu związanego z Rosją i Ukrainą w 2014 roku (Giles 2016). Rosja stara się konkurować z innymi aktorami stosunków międzynarodowych, przez co stale dokonuje ona modyfikacji w sposobach prowadzenia konfliktu oraz przygotowywania się do niego. Sam Władimir Putin przekonuje, że Federacja Rosyjska „*musi brać pod uwagę plany oraz kierunki rozwoju sił zbrojnych innych państw (...). Odpowiedzi muszą być oparte na przewadze intelektualnej, będą asymetryczne i mniej kosztowne*"[1].

W rosyjskiej koncepcji walka informacyjna ma miejsce nie tylko w trakcie trwania wojny. Nie ogranicza się ona także do inicjacyjnej fazy konfliktu jeszcze przed początkiem działań wojennych, kiedy ma miejsce informacyjne przygotowanie zmagań. Jako kontrast do innych metod i form, walka informacyjna toczona jest bezustannie także w czasie pokoju (Slipchenko, Gareev 2007). Wyrażenie *wojna informacyjna,* obecne w słowniku najważniejszych terminów z zakresu bezpieczeństwa sporządzonym przez Akademię Wojskową Sztabu Generalnego Federacji Rosyjskiej, w istotny sposób wskazuje różnice w definiowaniu tegoż pojęcia: rosyjska definicja jest szeroka i w żadnym stopniu nie jest ograniczana do czasu trwania konfliktu zbrojnego, podczas gdy definicje zachodnie traktują ją jako działania wykorzystywane do celów

[1] W. Putin, *Żołnierz to zaszczytny i poważany stopień*, fragment corocznego przemówienia do Zgromadzenia Federalnego Federacji Rosyjskiej z dnia 11.05.2006, http://old.redstar.ru/2006/05/11_05/1_01.html, (dostęp: 20.05.2021).

taktycznych prowadzonych wyłącznie w czasie trwania wojny[2].Walka informacyjna w rozumieniu rosyjskim obejmuje bardzo szeroki zakres różnego rodzaju czynności, a także procesów, które dotyczą: kradzieży, blokowania, manipulowania, edytowania lub całkowitego usuwania informacji. Informację rozumie się przy tym jako narzędzie, określony cel, a także jako domena operacyjna.

Rosyjska koncepcja wojny informacyjnej: założenia i różnice względem państw Zachodu

Rosyjska koncepcja walki informacyjnej zawiera ogół działań psychologicznych prowadzonych przez wywiad i kontrwywiad z użyciem cybertechnologii w celu uniemożliwienia łączności sił przeciwnika, blokowania nawigacji, zakłócania sprawnego funkcjonowania narzędzi komputerowych, a także wykorzystanie dezinformacji[3]. Wszystkie wymienione elementy mają za zadanie wywieranie wpływu na sposób myślenia i podejmowania decyzji przez adwersarza, obywateli danego kraju lub międzynarodowej społeczności (Zalewski, Dzierżyński, 2019, s. 157-159). Ich wykorzystanie przedstawiane jest w Rosji jako fundamentalny komponent sukcesu w przyszłych wojnach. Wiele wskazuje na to, że konflikty zbrojne będą toczyły się przy użyciu konwencjonalnych sił i środków militarnych, oraz sprawnie zastosowanego potencjału informacyjnego w takich dziedzinach jak cybertechnologia czy ekonomia. Wojna informacyjna nowego wymiaru będzie stanowiła swojego rodzaju punkt wyjściowy wobec każdego nowego typu konfliktu. Dziejąca się na naszych oczach rewolucja w prowadzeniu operacji wojskowych egzemplifikująca się wykorzystywaniem elementów wojny hybrydowej w Gruzji i na Ukrainie każe sądzić, że przyszłe działania wojenne do osiągnięcia określonych celów będą eksploatować m.in. środki masowego przekazu i/lub globalną sieć internetową, w tym media społecznościowe, blogi, video blogi itp. (Banasik, Panek, 2018, s. 187).

Władimir Putin funkcjonujący zarówno jako prezydent, a następnie premier Federacji Rosyjskiej, podkreślał rolę informacji jako jednego z priorytetowych czynników bezpieczeństwa narodowego. Uwidaczniało się to w kontroli sieci komunikacyjnych i medialnych, co

[2] S. Ennis, *Russia in 'information war' with West to win hearts and minds*, BBC, https://www.bbc.com/news/world-europe-34248178, (dostęp: 20.05.2021).
[3] K. Mshvidzobadze, *The Battlefield On Your Laptop*, RadioFreeEurope/RadioLiberty, https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html (dostęp: 20.05.2021).

zaowocowało w późniejszych latach reorganizacją struktur państwowych i dostosowaniem ich do osiągania zamierzonych celów politycznych. W 2003 r. tak zwana FAPSI, czyli Federalna Agencja Łączności i Informacji Rządowej została zlikwidowana, a jej kompetencje rozdzielone pomiędzy takie struktury jak Służbę Wywiadu Wojskowego (SVR), Wywiad Wojskowy (GRU), Federalną Służbę Ochrony (FSO) oraz Federalną Służbę Bezpieczeństwa (FSB). Dwie ostatnie zajmują się badaniem łączności telefonicznej, satelitarnej oraz internetowej. Zdaniem Khatuna Mshvidobadze (ibid.), dostawcy usług internetowych są zobligowani do szkolenia funkcjonariuszy FSB i FSO do użytkowania sprzętu nadzorującego ruch w przestrzeni internetowej w celu szpiegowania osób prywatnych.

Wyraźne różnice w pojmowaniu rozmaitych działań z wykorzystaniem informacji należy dostrzec już u samych podstaw myśli zarówno rosyjskiej jak i państw zachodnich. Przedstawiciele zachodniej myśli dotyczącej bezpieczeństwa cybernetycznego zdają się wyraźnie oddzielać prowadzenie operacji w przestrzeni cybernetycznej od takich, których celem jest atakowanie, edytowanie, przechwytywanie bądź blokowanie dostępu do zasobów informacyjnych. Jak podaje D. J. Smith (2012, s. 8-9), „ataki rozproszonej odmowy usług (DDoS – przyp. autora), zaawansowane techniki eksploatacji oraz telewizja Russia Today są powiązanymi ze sobą elementami wykorzystywanymi do prowadzenia wojny informacyjnej".

Termin *cyberwojna* w literaturze rosyjskiej odnosi się do zagranicznych form i koncepcji wojny informacyjnej, które w swej treści osobno traktują działania informacyjne przy użyciu urządzeń komputerowych i tradycyjnie pojmowane działania polegające na przejęciu kontroli nad zasobami informacji w postaci fizycznych nośników lub urządzeń je zawierających (Giles 2016, s. 8). Konkluzja jest więc taka, że każdorazowe eksplorowanie rosyjskiego piśmiennictwa w poszukiwaniu hasła *cyber* skutkować będzie jedynie odnalezieniem odniesień do zachodnich terminologii, co niesie ze sobą poważne ryzyko pozyskania mylących wyników. Wynika to przede wszystkim z faktu, że Rosjanie traktują działania prowadzone w cyberprzestrzeni łącznie z tymi w rzeczywistości.

Pojęcie cyberprzestrzeni w Federacji Rosyjskiej, podobnie jak w wielu innych państwach, traktowane jest jako przestrzeń informacyjna. Vladimir Kvachkov, były oficer wywiadu wojskowego Federacji Rosyjskiej, zwraca uwagę, że rosyjski koncept przestrzeni informacyjnej przejawia się w dwóch domenach zasadniczo odróżniających go od

innych państw: informacyjno-psychologiczny oraz informacyjno-technologiczny. Prowadzenie wojny informacyjno-psychologicznej zakłada wywieranie wpływu na ludność funkcjonującą na danym terenie bądź funkcjonariuszy sił zbrojnych, i prowadzona jest bezustannie, zarówno w czasie pokoju, jak i wojny. Natomiast wykorzystywanie domeny informacyjno-technologicznej ma na celu prowadzenie działań penetrujących systemy techniczne przeciwnika odpowiedzialne za odbieranie, przetwarzanie i wysyłanie informacji. Ta metoda prowadzenia wojny informacyjnej prowadzona jest w czasie trwania konfliktu. Przytoczone wyżej zagadnienia wskazują *informację* jako fundamentalny czynnik w pojmowaniu myśli rosyjskiej traktującej zasoby informacyjne za kluczowe w prowadzeniu działań operacyjnych. W rosyjskich ramach koncepcyjnych informacje te mogą być przechowywane gdziekolwiek i przekazywane w dowolny sposób - tak więc informacje w mediach drukowanych czy w telewizji podlegają tym samym funkcjom, co informacje przechowywane na komputerze lub smartfonie przeciwnika. Podobnie, przekazywanie lub transfer tych informacji może odbywać się w dowolny sposób: tak więc wprowadzenie uszkodzonych danych do komputera przez sieć lub z pendrive'a, nie różni się w głównej mierze od umieszczenia dezinformacji w mediach lub spowodowania jej publicznego powtórzenia przez osobę publiczną mającą duży wpływ na opinię społeczeństwa.

Doktryna Bezpieczeństwa Federacji Rosyjskiej z 2000 r., ogłoszona niecały rok po zaprzysiężeniu Władimira Putina na stanowisko prezydenta, określa trzy główne cele uwzględniające bezpieczeństwo informacji. Podobnie jak większość państw zachodnich, Federacja Rosyjska traktuje informację jako strategicznie istotny element funkcjonowania nowoczesnego państwa i pieczołowicie skupia się na jej ochronie. Następne cele widocznie różnią się od krajów demokratycznych: kolejny z nich jasno określa konieczność ochrony państwa przed informacjami pochodzącymi z zewnątrz. Co więcej, przedstawiane są one jako zagrożenie ciągłości władzy, narodowych interesów, mogą przemycać wrogą ideologię i stawiać w złym świetle panujący aparat władzy. Ostatni cel skupia się na budowaniu w społeczeństwie postaw patriotycznych oraz właściwych wartości moralnych zgodnymi z normami przyjętymi w Rosji (Brangetto, Veenendaal, 2016, s. 116).

Kolejnym bezprecedensowym podejściem do tworzenia sił wojny informacyjnej jest niewątpliwie wykorzystywanie młodzieżowych grup

przestępczych. Wyróżnia się co najmniej dwa powody, które sprzyjają takiej formie prowadzenia działań operacyjnych. Pierwszy to kwestia finansowa; działalność młodzieżowych grup przestępczych jest tańsza do sfinansowania niż szkolenie i utrzymywanie wyspecjalizowanych żołnierzy, a skuteczne i umiejętne wejście w posiadanie zasobów informacyjnych bądź ekonomicznych sprawia, że można dodatkowo się na tym wzbogacić. Drugim powodem jest trudność w zidentyfikowaniu faktycznego sprawcy ataku i ustalenie, jaki cel miał zostać dzięki niemu osiągnięty. Wykorzystywanie przez rząd rosyjski uzdolnionej matematycznie i informatycznie młodzieży stanowi swojego rodzaju zabezpieczenie: trudno oczekiwać, że nawet przy precyzyjnym określeniu sprawcy jakiegokolwiek ataku z wykorzystaniem cybertechnologii, będzie on utożsamiany z aparatem władzy. Oficjalnie taka formacja nie jest częścią Sił Zbrojnych Federacji Rosyjskiej, więc wykazanie korelacji między nimi jest właściwie niemożliwe do ustalenia (Smith, op.cit. s. 11).

W Federacji Rosyjskiej nie ma sztywnego rozróżnienia pomiędzy pokojem a wojną, jak ma to miejsce w amerykańskim myśleniu strategicznym. Wojsko amerykańskie ma pojęcie „fazy zero", czyli etapu poprzedzającego wystąpienie konfliktu zbrojnego. Rosyjskie postrzeganie stałego zagrożenia sprawia, że Rosja każdego dnia przygotowuje się do wojny i wykorzystuje do tego wszystkie instrumenty władzy państwowej w celu zwiększenia swojego bezpieczeństwa i ochrony interesów.

Wojna informacyjna w praktyce

Szeroka koncepcja wojny strategicznej jest nieodłącznym elementem rosyjskiej strategii militarnej. Doktryna wojskowa z 2010 r. wskazuje, że prowadzenie działań przy wykorzystaniu cybertechnologii przeciwko Federacji Rosyjskiej skutkować będzie otwartym wypowiedzeniem wojny. Ów dokument zawiera również koncepcje, według których osiągnięcie celów politycznych przy użyciu informacji jest wysoce pożądane, przy czym wskazuje się, że wykorzystanie konwencjonalnych sił zbrojnych powinno być jak najmniejsze.

Najnowocześniejsze rozwiązania technologiczne sprawiają, że obraz wojny zmienia się w zastraszającym tempie. Wykorzystywanie cybertechnologii do prowadzenia działań militarnych nie jest już od dawna niczym nowym. Dynamiczny rozwój nowych technologii zmienia nie tylko charakter samego konfliktu, ale i wymiar, w którym ma on miejsce. Federacja Rosyjska, podobnie jak Stany Zjednoczone oraz

Chińska Republika Ludowa, prowadzi badania nad zastosowaniem broni antysatelitarnej. 16 grudnia 2020 r. dowództwo kosmiczne Departamentu Obrony USA wydało oświadczenie, w którym oskarżyło Rosję o przeprowadzenie testu tak zwanej broni orbitalnej. Stoi to w sprzeczności ze stanowiskiem rosyjskich dyplomatów jakoby starali się oni aktywnie zapobiegać transformowaniu przestrzeni okołoziemskiej w nowe pole bitwy pomiędzy globalnymi hegemonami. Pentagon wskazał przy tym, że grudniowy test był trzecim w tym roku tego typu testem nowego rodzaju broni kosmicznej przeprowadzonej przez Kreml. Głównodowodzący Sił Kosmicznych USA, gen. John Raymond, sprecyzował w oświadczeniu, że był to swojego rodzaju pocisk miotany stanowiący realne zagrożenie nie tylko dla możliwych za obranie celów strategicznych, ale i prywatnych podmiotów wykorzystujących sygnał satelitarny do chociażby emisji programów telewizyjnych czy zapewniających łączność internetową[4].

Federacja Rosyjska do tej pory zademonstrowała dwa rodzaje broni kosmicznej: pierwszym są startujące z Ziemi rakiety DA-ASAT, a drugim jest system zainstalowany w przestrzeni okołoziemskiej określany przez Siły Kosmiczne Stanów Zjednoczonych mianem „współorbitalnego ASAT". Warto w tym miejscu zauważyć, że zakłócenie łączności satelitarnej u strony przeciwnej jest traktowane jako kluczowe w osiągnięciu nie tyle przewagi informacyjnej, co zupełnej dominacji. Oparte na kontakcie satelitarnym systemy nawigacyjne okazałyby się całkowicie bezużyteczne, co mogłoby zagwarantować hegemonię w prowadzeniu konwencjonalnych działań operacyjnych. Aktualnie wiodące prym państwa zarządzające informacją, nawigacją, ogółem środków dowodzenia strategicznego i używające systemów teleinformatycznych do kierowania działań, mogą znaleźć się w wysoce niekorzystnym położeniu. Doprowadzenie do zakłócenia bądź kompletnego zniszczenia systemu poprzez użycie sił i środków asymetrycznych drastycznie zmniejsza szanse na prowadzenie jakichkolwiek operacji, a co za tym idzie, odniesienie zwycięstwa na polu walki (House, Seaboyer, Giles 2019, s. 17). Powodem, dla którego Rosjanie prowadzą badania w tym zakresie, są zakończone sukcesami działania wymierzone w cywilną infrastrukturę sieciową i telekomunikacyjną w marcu 2014 r. na Krymie. Potrzeba uzyskiwania

[4] *„Wystrzał z satelity". Pentagon oskarża Kreml o test orbitalnej broni*, space24, 24.07.2020, https://www.space24.pl/wystrzal-z-satelity-pentagon-oskarza-kreml-o-test-orbitalnej-broni, (dostęp:27.05.2021).

przewagi informacyjnej jest istotna w myśl rosyjskich koncepcji wojny informacyjnej, zatem penetrowanie łącz internetowych adwersarza stwarza możliwość przeprowadzania akcji szpiegowskich bądź, co równie istotne, przekazywania dezinformacji.

Zdaje się, że Rosja, w znacznie większym stopniu niż inni aktorzy na arenie międzynarodowej, skompilowała metodę na zaimplementowanie szeregu różnorodnych operacji cybernetycznych do koncepcji umożliwiającej osiągnięcie rezultatów w postaci celów polityczno-strategicznych. Decydenci rosyjscy zdają się być w pełni świadomi faktu, że ich potencjał zbrojny nie może równać się z siłami państw członkowskich Paktu Północnoatlantyckiego, zatem przewaga na polu walki musi zostać zdobyta bez militarnego prowokowania oponentów. Takie ujęcie jest fundamentalnym elementem rosyjskiej polityki bezpieczeństwa. Rosja zakłada, że różnorodne konflikty pomiędzy stronami powinny oscylować poniżej progu konfliktu zbrojnego (Brangetto, Veenendaal, op.cit.).

Determinacja Rosjan jest wyraźnie widoczna w destabilizowaniu sytuacji wewnętrznych byłych państw bloku wschodniego. Rosja, jako spadkobierca Związku Socjalistycznych Republik Radzieckich, dąży do utrzymania swojej strefy wpływów, kontrolowania byłych członków bloku wschodniego i przeciwstawiania się poszerzaniu wpływów państw zachodnich na ich terenach. Polityka zagraniczna mająca tworzyć obraz „my kontra oni" jest wszechobecna w rosyjskiej przestrzeni informacyjnej.

Rosyjskie zmasowane ataki cybernetyczno-kinetyczne skierowane wobec Gruzji wskazywane są jako test nowych środków prowadzenia walki. Ów rodzaj siły militarnej odnosi się do klasy cyberataków, które mogą w sposób pośredni lub bezpośredni spowodować szkody fizyczne, poważne obrażenia lub śmierć wyłącznie poprzez wykorzystanie podatnych na ataki systemów informatycznych. Mimo braku pełnego sukcesu, należy mieć na uwadze fakt, że już samo stworzenie doktryny zakładającej otwarte wykorzystywanie sił wojny informacyjnej wraz z późniejszymi incydentami jasno wskazuje pełne zaangażowanie i potencjał jaki Dowództwo Sił ZbrojnychFederacji Rosyjskiej chce wykorzystywać i rozwijać.

Rosyjsko-ukraiński konflikt z 2014 r. był kolejnym testem wykorzystywania cybertechnologii do prowadzenia działań zbrojnych. Prasa amerykańska określiła konflikt na Ukrainie mianem laboratorium

dla przyszłych działań wojennych XXI wieku[5]. Rosja i asystowane przez nią bojówki niszczyły systemy nawigacyjne i naprowadzania pocisków rakietowych przy użyciu wysoce skutecznej technologii ataku elektronicznego, w tym tak zwanego spoofingu sygnałów GPS, polegającego na oszukaniu odbiornika sygnału GPS przeciwnika, utrudniając przeprowadzenie precyzyjnego ataku rakietowego bądź przy użyciu drona bojowego. Według dziennikarzy *The Christian Science Monitor*, dzięki tej technice udało się zmienić trajektorię lotu drona bojowego Lockheed RQ-170 i zmusić go do lądowania na terenie Iranu gdzie został przechwycony, zamiast jego bazy zlokalizowanej na terenie Afganistanu[6].

Działania rosyjskie w Syrii również dowodzą skuteczności prowadzenia wojny informacyjnej. Opisy operacji wojskowych jasno wskazują, że używanie siły militarnej może w niedalekiej przyszłości zejść na dalszy plan i ustąpić miejsca inny elementom potencjału zbrojnego. Walerij Gerasimow, obecny szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej i członek Rady Bezpieczeństwa Federacji Rosyjskiej, wskazuje, że we współczesnych konfliktach zbrojnych konieczne jest stosowanie środków pozamilitarnych jak chociażby polityczne, informacyjne czy ekonomiczne. Co więcej, owe siły i środki należy prowadzić mając wsparcie konwencjonalnych sił wojskowych. Gerasimow dodaje także, że zminimalizowanie sił i środków jest możliwe dzięki stosowaniu walki informacyjno-psychologicznej, wspieraniu lokalnej opozycji oraz skutecznemu ograniczaniu potencjału militarnego przeciwnika. Słowa te w pewien sposób potwierdzają trend widoczny już w Gruzji i na Ukrainie: odchodzenie od jawnych form interwencji zbrojnej, a intensyfikowanie działań ukrytych (za: House i inni, op.cit. s. 17, 19-21).

Wciąż trwający spór o Krym i toczące się walki na wschodzie Ukrainy świadczą o bezwzględnym działaniu Federacji Rosyjskiej. 22 lutego 2021 r. Ukraina oświadczyła, że po raz kolejny jest obiektem zmasowanych cyberataków. Oskarżyła o to bliżej nieokreślonych sprawców posługujących się rosyjskimi sieciami informacyjnymi. Oficjalne oświadczenie ukraińskiej Rady Bezpieczeństwa Narodowego i

[5] G. Warwick, *Assisting The Human Central to Pentagon's Third Offset*, „Aviation Week" 2016, https://aviationweek.com/defense-space/assisting-human-central-pentagons-third-offset, (dostęp: 27.05.2021).

[6] *Exclusive: Iran hijacked US drone, says Iranian engineer*, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer, (dostęp 10.07.2021).

Obrony wskazuje, że obiektem ataków były strony należące do Służb Bezpieczeństwa, sama Rada Bezpieczeństwa oraz kilka instytucji i organizacji państwowych. W oświadczeniu podano, że atak miał zainfekować serwery wirusem, który sprawiłby, że dana sieć sama dokonałaby ataków na kolejne zasoby rządowe[7]. Seria ataków powtórzyła się również w marcu, tym razem miała na celu wejście w posiadanie i przejęcie niejawnych danych najwyższych instytucji władzy państwowej Ukrainy[8].

Dwaj rosyjscy eksperci w dziedzinie nauk o bezpieczeństwie, S. G. Chekinov oraz A. Bogdanov (2019, s. 23-25) wskazują, że tam, gdzie fizyczny dostęp do określonych obiektów nie jest dostępny, istotną rolę odgrywają tak zwane siły wojsk elektronicznych, które mają za zadanie blokować dostęp do informacji, ludność cywilną oraz media tradycyjne i internetowe. Badacze podkreślają też fakt, że wojsko elektroniczne stanowi nowy rodzaj siły militarnej Federacji Rosyjskiej, odpowiedzialnej za branie udziału w inauguracyjnej fazie konfliktu.

Wojska elektroniczne Federacji Rosyjskiej: rozwój, implementacja, perspektywy na przyszłość

Definicja podana w encyklopedycznym słowniku wojskowym wskazuje, że wojna elektroniczna jest jednym z metod prowadzenia walki zbrojnej, która wykorzystuje wszelkiego rodzaju siły i środki elektroniczne wymierzone we wrogie tak zwane C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – z ang. dowództwo, kontrola, łączność, komputery, wywiad, obserwacja i rozpoznanie). Celem jest spowodowanie zmian lub zmniejszenia formatu danej informacji bądź doprowadzenie do przeobrażenia określonych warunków środowiska operacyjnego[9].

Możliwości Federacji Rosyjskiej w zakresie prowadzenia wojny elektronicznej w ostatnich dwóch dekadach zmieniły się. Wojska sił elektronicznych stały się jednym z kluczowych atutów wspierających

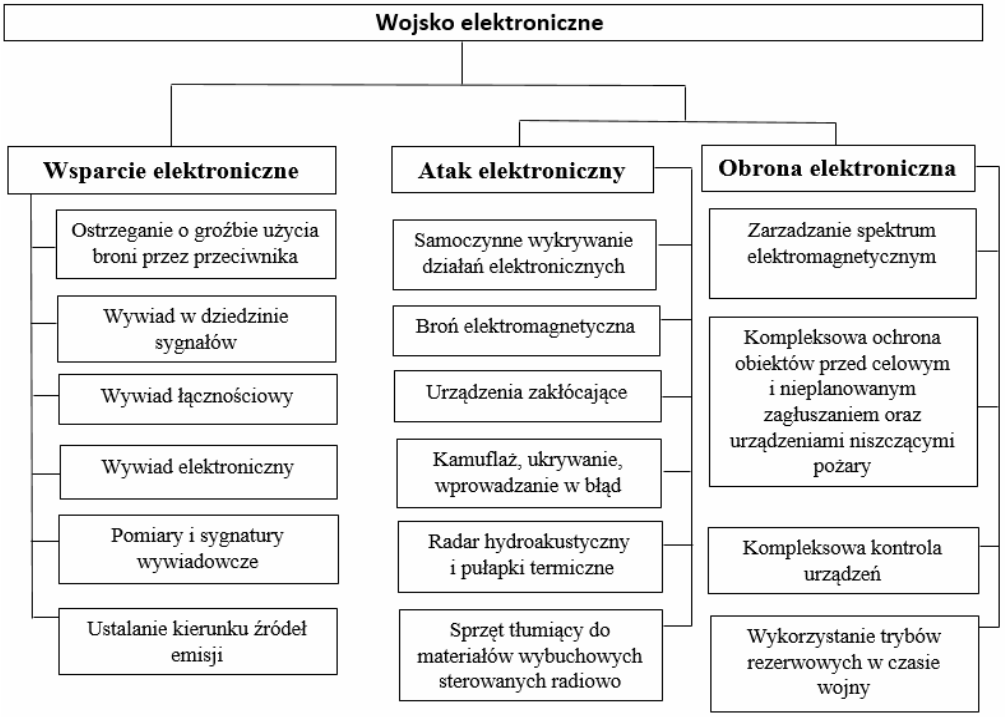
[7] P. Polityuk, *Ukraine accuses Russian networks of new massive cyberattacks*, https://www.nasdaq.com/articles/ukraine-accuses-russian-networks-of-new-massive-cyber-attacks-2021-02-22, (dostęp: 27.05.2021).

[8] *Ukraine Accuses Russia of Fresh Cyberattack*, RadioFreeEurope/RadioLiberty, https://www.rferl.org/a/ukraine-accuses-russia-of-fresh-cyberattack/31153635.html, (dostęp: 27.05.2021).

[9] M. Dura, *Walka radioelektroniczna rosyjską odpowiedzią na przewagę NATO? [ANALIZA]*, 2017, https://www.defence24.pl/walka-radioelektroniczna-rosyjska-odpowiedzia-na-przewage-nato-analiza, (dostęp: 28.05.2021).

konwencjonalne siły zbrojne. Aby w pełni zrozumieć ten stan rzeczy, należy dokonać obserwacji, jak rozwój cybertechnologii i jej zastosowania na polu walki wpisuje się w rosyjską koncepcję prowadzenia działań oraz jaki potencjał mogą stanowić wojska elektroniczne w przyszłości. Analiza treści rosyjskich i zachodnich mediów w połączeniu z reformami strukturalnymi rosyjskich Sił Zbrojnych każe sądzić, iż wojsko elektroniczne dzieli się na trzy główne płaszczyzny operacyjne: wsparcie elektroniczne mające za zadanie współpracować z innymi rodzajami wojsk, zapewniając im informacje i aktywnie wspomagać je w prowadzeniu działań militarnych, siły odpowiedzialne za prowadzenie ataków elektronicznych, a także jednostkio przeznaczeniu obronnym własnych systemów oraz zasobów informacyjnych (Ryc. 1).

Ryc. 1. Podział wojsk elektronicznych Federacji Rosyjskiej



Źródło: Opracowane na podstawie: M. Shepovalenko, Boevyelazerybudushchikhvoyn (Combat lasers of futurewars), „Voyenno-PromyshlennyyKuryer" 2013, http://www.vpk-news.ru/articles/16579, (dostęp: 28.05.2021).

Głównodowodzący rosyjskich wojsk często otwarcie informują o skuteczności wykorzystywanej przez nich cybertechnologii. Minister

Obrony Federacji Rosyjskiej Sergei Shoigu w 2019 r. dla portalu *zvezdaweekly.ru* wyrażał swoje stale rosnące zaufanie do działań wojsk elektronicznych. Wskazywał on, iż komponenty cyberwojsk są w stanie m.in. stwarzać zagrożenie dla sygnałów GPS, blokować możliwość prawidłowego działania systemów nawigacyjnych wrogich sił czy też bezpośrednio powodować niszczenie amerykańskich rakiet zmieniając ich trajektorię lotu. Shoigu miał także wprost stwierdzić przed kolegium Ministerstwa Obrony, iż rosyjskie systemy wchodzące w skład wojsk elektronicznych przewyższają potencjał zagranicznych konkurentów oraz podkreślił fakt, że sprawdziły się one podczas operacji militarnych w Syrii.Za przykład może posłużyć obrona rosyjskiej bazy w Cheimim, gdzie 5 stycznia 2018 r. systemy wojsk elektronicznych odparły atak bezzałogowych statków powietrznych. Według doniesień prasy rosyjskiej, aż 6 z 13 dronów bojowych zostało zniszczonych przez siły wojsk elektronicznych. Niemniej jednak, mimo oczywistego potencjału zastosowania tejże technologii, rosyjscy decydenci zgodnie uważają, że na ten moment nie jest to wystarczająca ochrona i dla pełnego bezpieczeństwa należy zaopatrzyć bazy rosyjskie w miniaturowe pociski tzw. *hit-to-kill*, używane m.in. przez Amerykanów[10].

Wojska elektroniczne to nie tylko technologia i sprzęt, ale również, a może przede wszystkim, ludzie. Narodowy przemysł obronny niezmiennie dostarcza Siłom Zbrojnym coraz to nowszy i udoskonalany system wspierający prowadzenie działań strategicznych, lecz na tym się modernizacja nie kończy. Samo doposażanie wojsk wymaga także szkoleń teoretycznych i praktycznych. W samym 2018 r. miało miejsce nieco ponad 200 ćwiczeń specjalnych zawierających w swej treści szkolenia taktyczne oraz dowódczo-sztabowe. Przeprowadzono również 15 szkoleń brygadowych. Sierpień 2020 r. pokazał jeszcze większe pod względem liczebności ćwiczenia wojsk elektronicznych. Celem tychże manewrów było testowanie potencjału wojsk elektronicznych w przeciwstawianiu się masowym atakom rakietowym i penetrowaniu systemów obrony powietrznej wrogich sił[11].

Od kiedy Kreml zainicjował reformę oraz modernizację sił zbrojnych w 2008 r., niektórzy rosyjscy stratedzy wojskowi zwrócili

[10]R. McDermott, *Russia's Electronic Warfare Capabilities as a Threat to GPS*, 2021, https://jamestown.org/program/russias-electronic-warfare-capabilities-as-a-threat-to-gps/, (dostęp:28.05.2021).

[11] P. Smith, *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*, American Security Project, 2020, s. 4-5, https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf (dostęp: 28.05.2021).

uwagę na potrzebę rozwoju sił i środków odpowiedzialnych za prowadzenie wojny sieciocentrycznej, która określana była mianem „mnożnika sił" i sposobem na przeprowadzenie daleko idących i fundamentalnych zmian w funkcjonowaniu wojska. Za szczególnie istotne uznano przekształcenie struktur dowodzenia i kontroli w taki sposób, aby zostały one zautomatyzowane we wszystkich rodzajach Sił Zbrojnych Federacji Rosyjskiej. Co więcej, rząd w Moskwie dążył do zmian w samym prowadzeniu wojny. Decyzje spowodowały później szereg zmian w strukturach wojskowych i politycznych, a także podjęto działania zmierzające do bardziej otwartego patrzenia na zupełnie nowe, alternatywne koncepcje wykorzystania cyberprzestrzeni oraz informacji do realizacji zamierzonych celów[12].

Rosyjscy politycy i wysoko postawieni dowódcy podkreślają, że samo użycie i inwestowanie w potencjał wojsk elektronicznych nie powinno nikogo dziwić, gdyż jest on relatywnie tanim oraz zaskakująco łatwym sposobem na paraliżowanie funkcjonowania chociażby radarów, systemów nawigacyjnych czy ogromu innych wrogich systemów, ale przede wszystkim są doskonałym środkiem do obrony własnych identycznych systemów przed kontratakami. Podkreślić również należy szereg innych okoliczności, które sprzyjają zastosowaniu tego typu działań: wykorzystywanie sił i środków walki elektronicznej, jako narzędzia arsenału asymetrycznego, daje w prosty sposób możliwość zniwelowania przewagi wroga wynikającej z posiadania wysoce zaawansowanej technologii oraz systemów komputerowych. Prowadzi to do prostej konkluzji, że rozwój wojsk elektronicznych jest jednym z priorytetów dla strony rosyjskiej i spodziewać się należy, iż będą one finansowane i rozwijane w przyszłości[13].

Konkluzje

Federacja Rosyjska poczyniła nadzwyczajne postępy we wdrażaniu nowych form prowadzenia działań wojennych w ostatnich latach. Eksperymentowanie z potencjałem sieciocentrycznym i

[12] R. N. McDermott, *Report: Russia's Electromagnetic Warfare Capabilities to 2025. Chellenging NATO in the Electromagnetic Spectrum*, 2017, s. 3-4, https://euagenda.eu/upload/publications/untitled-135826-ea.pdf (dostęp: 28.05.2021).

[13] O. Bozhyeva, , *"Festival' 'novayavoyna'" (Festival "New War"), Moskovskiy Komsomolets*, 2009, http://www.mk.ru/editions/daily/article/2009/10/08/364473-festival-novaya-voyna.html, tł. za: R. N. McDermott, *Russian Perspective on Network-Centric Warfare: The Key Aims of Serdyukov's Reform*, 2018, s. 13, https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/252646.

elektronicznym, wykorzystywanie cybertechnologii do przejmowania kontroli nad zasobami informacyjnymi czy destabilizowanie działalności operacyjno-strategicznej przeciwnika to tylko niektóre z nowotworzonego arsenału rosyjskiego. Udoskonalanie zdolności wojsk elektronicznych jest stale obserwowane i należy spodziewać się, że ta tendencja pozostanie niezmienna w najbliższych latach, głównie dlatego, iż odgrywają one ważną rolę w ustanawianiu „wzmacniacza" i „mnożnika siły". Dowód tego stanowią doświadczenia wojsk rosyjskich na Ukrainie i w Syrii w ciągu ostatnich kilku lat, gdzie siły i środki wojsk elektronicznych zdają się być nieodzowne w prowadzeniu konfliktów zbrojnych. Kreml postrzega informacyjny wymiar walki jako słabość wrogich państw (np. USA) i sojuszy (jak chociażby NATO).Działalność putinowskiej Rosji w domenie informacyjnej nie jest stała lecz zmienna i sprawnie się rozwijająca. Imperializm rosyjski wymaga stworzenia środków pozwalających Rosji konkurować z innymi światowymi hegemonami. Zdecydowanie się na stosowanie narzędzi wojny informacyjnej wynika ze słabego względem innych podmiotów międzynarodowych potencjału sił konwencjonalnych. Aktywność i dominacja Rosjan w tej sferze nie daje jednak podstaw by sądzić, iż obecnie jest to filar arsenału zbrojnego Federacji Rosyjskiej. Sukcesywne rozwijanie cybertechnologii może sprawić, iż ideologiczny spadkobierca ZSRR będzie w przyszłości stanowił poważne zagrożenie dla innych państw.

Rosja włączyła ataki cybernetyczne i operacje informacyjne do sfery wojny informacyjnej. Wojna nowego typu nabiera coraz to większego znaczenia jako strategia wygrywania konfliktu, która pozwala uniknąć bezpośredniego oskarżenia o prowadzenie działań zbrojnych przez organizacje ponadnarodowe, skutecznie powstrzymując przeciwnika przed prowadzeniem własnych działań oraz minimalizując wydatki, co jest kluczowe z perspektywy Rosji. Politycy rosyjscy zdają się dostrzegać mnogość korzyści płynących z prowadzenia operacji asymetrycznych. Działania te jawią się jako reakcja na wojnę polityczną i informacyjną prowadzoną przeciwko Federacji Rosyjskiej.

Same instrumenty wykorzystywane przez Rosjan nie są nowe, lecz co warto podkreślić, ich kombinacja i metoda wykorzystania w znaczący sposób odbiega od zachodniego myślenia i praktyki. Rosyjska strategia i operacje w dziedzinie wojny informacyjnej i cybernetycznej nadal wprawiają w zakłopotanie zachodnie rządy i opinię publiczną, która nie opracowała jeszcze strategii, za pomocą której mogłaby przeciwstawić się Rosji. Ale

ponieważ Rosja już zaangażowała swoich przeciwników w wojnę informacyjną, muszą oni starać się ją zrozumieć dla dobra własnego bezpieczeństwa.

Literatura

Banasik, M., Panek, B., 2018. *Zagrożenia dla bezpieczeństwa euroatlantyckiego płynące ze strony Federacji Rosyjskiej (cz. I),* Bezpieczeństwo zintegrowane współczesnej Polski, A. Stępień, R. Stawicki (red.), Przedsiębiorczość i Zarządzanie, Łódź-Warszawa.

Brangetto, P., Veenendaal, M. A., 2016. *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*, NATO CCD COE Publications, Tallin.

Chekinov, S.G., Bogdanov, S.A., 2015. *Прогнози рование характера и содержания войнбудущего: проблемы и суждения" (Forecasting the nature and content of wars of the future: problems and assessments),* Voennaya Mysl, nr 10.

Giles, K., 2016. *Handbook of Russian Information Warfare*, NATO Defense College, Rome.

House, C., Seaboyer, A., Giles, K., 2019. *The Russian Information Warfare Construct*, Royal Military College of Canada.

Protasowicki, I., 2018. *Rola szkodliwego oprogramowania w geopolityce*, Przegląd Geopolityczny, 26, s. 85-94.

Slipchenko, V., Gareev, M., 2007. *Future War*, Foreign Military Studies Office.

Smith, D.J., 2012. *How Russia Harnesses Cyberwarfare*, Defense Dossier. American Foreign Policy Council, 4.

Soroka, P., 2016. *Rola nowoczesnych technologii w wyścigu zbrojeń*, Przegląd Geopolityczny, 16, s. 77-86.

Sykulski, L., 2019. *Diffused war as a kind of non-linear war*, Przegląd Geopolityczny, 29, s. 137-146.

Sykulski, L., 2021. *Teoria gier refleksyjnych jako metoda analizy walki informacyjnej*, Przegląd Geopolityczny, 37, s. 58-74.

Świątkowska, J., 2017. *Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem*, Przegląd Geopolityczny, 20, s. 162-177.

Wilczyński, P.L., 2013. *Sektor zbrojeniowy jako czynnik rozwoju gospodarki opartej na wiedzy*, Prace Komisji Geografii Przemysłu Polskiego Towarzystwa Geograficznego, 21, s. 133-156.

Zalewski, J., Dzierżyński, D.G., 2019. *Wojna informacyjna w odbudowie rosyjskiej mocarstwowości*, Wojskowa Akademia Techniczna, Warszawa.

Use of cybertechnology by Russia in information warfare

The development of modern technologies has fundamentally changed the face and perception of information warfare. The emergence and development of cyberspace as a platform for the rapid circulation of information has provided an extraordinary opportunity to use it in the conduct of military operations. The information warfare itself is primarily intended to influence the opponent in a way desired by a given side, to induce in him the reactions expected by the aggressor. The use of means and forces of the new kind of warfare is not focused on their destructive nature, but comes down to disrupting the flow of information, blocking access to information systems and networks in order to deprive the enemy of control over its own information resources. A state in a particular way using cybertechnology is the Russian Federation. The purpose of the study is an attempt to formulate answers to the following questions: why is Vladimir Putin's Russia developing tools of information warfare? Why are they worth developing? How, unlike Western countries, does Russia understand information warfare? How does the Russian Federation use cybertechnology to conduct operational and strategic activities? Understanding the direction of transformation of the modern battlefield indicates the need to anticipate and prepare for new types of warfare that may occur in the future.

Key words: information warfare, cyber technology, Russian Federation, information, information security.