Agnieszka BÓGDAŁ-BRZEZIŃSKA
Uniwersytet Warszawski[1]
Wydział Nauk Politycznych i Studiów Międzynarodowych
bogdal@uw.edu.pl
ORCID 0000-0003-0247-1941
Jan A. WENDT
Uniwersytet Gdański
Wydział Oceanografii i Geografii
jan.wendt@ug.edu.pl
ORCID 0000-0003-1712-4926
https://doi.org/10.34739/dsd.2020.02.07

GEOPOLITYCZNY KONTEKST SUWERENNOŚCI INFORMACYJNEJ ROSJI W CYBERPRZESTRZENI I JEJ ZNACZENIE DLA BEZPIECZEŃSTWA MIĘDZYNARODOWEGO

ABSTRAKT: Celem niniejszego artykułu jest wskazanie zależności miedzy geopolityką jako istotnym czynnikiem definiowania polityki Rosji (w zakresie bezpieczeństwa i stosunków z zagranicą), a jej aktywnością na rzecz uznania cyberprzestrzeni za podległą suwerenności państwowej. Definicji podlega pojęcie geopolityki informacyjnej. Podjęto analizę katalogu czynników determinujących nowy wymiar geopolityki rosyjskiej z uwzględnieniem cyberprzestrzeni i polityki informacyjnej. Autorzy zastanawiają się nad rangą czynnika cybernetycznego i udziałem suwerenności informacyjnej w kształtowaniu wizerunku międzynarodowego Federacji Rosyjskiej (FR), by następnie poddać diagnozie ich wpływ na sferę bezpieczeństwa międzynarodowego. W opracowaniu nie zostaną omówione przykłady cyberataków rosyjskich wobec państw trzecich, podjęta zostanie natomiast próba wyjaśnienia uwarunkowań szeroko definiowanej aktywności państwa w geoprzestrzeni informacyjnej.

SŁOWA KLUCZOWE: suwerenność, geopolityka, cyberprzestrzeń, Rosja, polityka informacyjna, bezpieczeństwo międzynarodowe

THE GEOPOLITICAL CONTEXT OF RUSSIA'S INFORMATION SOVEREIGNTY IN CYBERSPACE AND ITS SIGNIFICANCE FOR INTERNATIONAL SECURITY

ABSTRACT: The purpose of this article is to indicate the relationship between geopolitics as an important factor in defining Russia's policy (in terms of security and relations with foreign countries) and its activity for recognizing cyberspace as subject to state sovereignty. The concept of information geopolitics is subject to definition. An analysis of the catalog of factors determining the

[1] The Warsaw University; Poland.

new dimension of Russian geopolitics, including cyberspace and information policy, is undertaken. The authors consider the importance of the cybernetic factor and the participation of information sovereignty in shaping the international image of the Russian Federation, to then diagnose their impact on the sphere of international security. The study will not discuss examples of Russian cyber attacks against third countries, but an attempt will be made to explain the determinants of broadly defined state activity in the information geospatial.

KEYWORDS: sovereignty, geopolitics, cyberspace, Russia, information policy, international security

WPROWADZENIE: NARRACYJNOŚĆ W DOBIE INTERNETU A WIARYGODNOŚĆ PRZEKAZU INFORMACYJNEGO PAŃSTW

Internet jako źródło informacji ujawnia jeden z wielu paradoksów współczesnej rzeczywistości społecznej – jest podstawowym narzędziem umacniania dotychczasowego światopoglądu użytkowników, poszukujących potwierdzenia dla własnych przekonań i opinii. Wrażliwość na ocenę światopoglądu czy prościej punktu widzenia rzeczywistości jest prawdopodobnie o wiele bardziej reprezentatywna dla współczesnych niż dla poprzednich generacji. Jeśli przyjąć, że bezpieczeństwo informacyjne jest wyrazem potrzeb jednostki, to obserwacja opisanego wyżej mechanizmu wskazuje, w jak ścisły sposób wiązać należy tę potrzebę z poczuciem tożsamości (indywidualnej i wspólnotowej). Pierwszym poziomem bezpieczeństwa informacyjnego jednostki jest jej potrzeba wiedzy o sobie i potwierdzenia opowieści na własny temat (autonarracji). Neil Postman traktuje narracje jako opowieści wyjaśniające rzeczywistość w sposób, z którym zgadza się większość ludzi żyjących w danej epoce. Narracja gwarantuje człowiekowi poczucie sensu, a jesteśmy obarczeni takim rodzajem świadomości, który wymaga, abyśmy to poczucie mieli. „Nie ma większego przestępstwa wobec umysłu, jak wyszydzić cudzą narrację. To tak, jakby obrabować ludzi z ich sensu życia" – pisze dobitnie Postman[2].

Dodać należy w tym miejscu, że profilowanie informacji przez wyszukiwarki jest niczym innym jak reakcją na te zachowania. Internet jako produkt ludzkiego doświadczania rzeczywistości nie służy bowiem czystej wiedzy, neutralnej aksjologicznie i emocjonalnie. Jest wykorzystywany jako mapa drogowa wyborów moralnych, poradnia psychologiczna. Przeniesienie do sieci schematów towarzyszących ludzkiemu życiu skutkuje w naturalny sposób wielofunkcyjną replikacją obyczajów i praktyk ze świata rzeczywistego. Całkowicie zrozumiałe jest zatem to, że „polityka międzynarodowa staje się coraz bardziej zawodami o konkurencyjność wiarygodności (*competitive credibility)*. Tak jak kiedyś w rozgrywce międzynarodowej walka toczyła się przede wszystkim o to, czyja gospodarka lub czyj potencjał wojskowy przeważy, tak teraz, w erze informacji, bardziej wyrafinowana gra coraz bardziej toczy się o to, czyja opinia zwycięży"[3]. Szybki rozwój technologii informatycznych prowadzi do tego, że informacja staje się nowym istotnym elementem porządkującym przestrzeń polityczną, a przepływy idei i obrazów inspirują

[2] N. Postman, *W stronę XVIII stulecia*, Warszawa 2001, s. 111.
[3] T.W. Grabowski, *Postprawda a bezpieczeństwo,* [w:] T.W. Grabowski, M. Lakomy, K. Oświecimski, *Bezpieczeństwo informacyjne w dobie postprawdy*, Kraków 2018, s. 13.

weryfikację i metamorfozę struktur politycznych. Dotyczy to zarówno struktur atrybuowanych podmiotowo, takich jak państwo, jak również struktur funkcjonalnych, takich jak ład międzynarodowy.

Badacze zwracają uwagę, że „ilość dostępnej informacji gwałtownie rośnie i niezbędna staje się jej selekcja i ocena pod względem szeroko rozumianej jakości”[4]. Podejmowane są próby porządkowania wiedzy o skutkach nadmiarowości informacji, którą uznaje się za stopniowalną. Ocenie podlegają patologiczne formy tego zjawiska i ich społeczne konsekwencje. „Szum informacyjny” jest nierównowagą między proporcjami informacji wytwarzanej i przetwarzanej. W odniesieniu do jednostek oznacza on niezdolność świadomego śledzenia informacji i skupiania na nich uwagi. W odniesieniu do państw niesie to deficyt instrumentów i struktur wyspecjalizowanych w identyfikacji i zarządzaniu informacją istotną dla bezpieczeństwa narodowego. Z kolei pojęcie „informacyjnej mgły” odnosić należy do dostępności kolosalnej ilości nieustrukturyzowanych, nieuporządkowanych, chaotycznych, niespójnych i rozproszonych informacji. Bezradność jednostek i państw wyraża się w braku naturalnych narzędzi i procedur ich porządkowania, zatem w trudnej sztuce nadawania znaczeń. „Smog informacyjny”, czyli występowanie nadmiaru informacji bezwartościowych, a nawet szkodliwych – jak zaznaczają R. Tadeusiewicz czy M. Szynkiewicz – jest dowodem aktywności osób niekompetentnych „lub użytkowników świadomie generujących przekazy nieprawdziwe czy tendencyjne”[5]. Ci ostatni wpisują się w klasyfikacje destrukcyjnych internautów zwanych trollami, uczestników walki informacyjnej w sieci[6].

Informacja może być traktowana jako zasób: źródło wiedzy albo narzędzie walki. Warto zauważyć, że podmioty polityczne wykorzystujące informację powinny uwzględniać jej parametry jakościowe tj. aktualność, kompletność, istotność, dokładność, zrozumiałość, operatywność, pochodzenie z pewnych źródeł[7]. Niestety wobec osłabienia merytorycznej oceny informacji internetowych „treści pseudonaukowe mogą skutecznie imitować rzetelne i wartościowe poznawczo przekazy naukowe. Negatywne skutki opisywanych procesów mają odzwierciedlenie również w sferach etyki i prawa – dziedzin, których rozwój, […] nie nadąża za postępem, jaki dokonuje się w obrębie nowoczesnych technologii komunikacyjnych”[8].

---

[4] K. Liderman, A. Malik, *Polityka informacyjna a bezpieczeństwo informacyjne*, „Studia Bezpieczeństwa Narodowego” 1 (4)/ 2013, s. 400.

[5] R. Tadeusiewicz, *W dymie i we mgle...*, http://www.solidarnosc.org.pl/ksn/strona-archiwalna/Docs/rystad.pdf, s. 7–8; M. Szynkiewicz, *Metafora smogu informacyjnego a procesy informacyjne*, „Studia Metodologiczne”, nr 32/2014, s. 71: „Rozdrobnienie i brak uporządkowania utrudnia użytkownikom sieci sprawne i efektywne wykorzystywanie zgromadzonych w nich zasobów informacyjnych. Nieuporządkowanie i nieusystematyzowanie stanowi jeden z głównych mankamentów współczesnych, opartych na technologii internetowej, źródeł informacji. Drugim czynnikiem utrudniającym korzystanie z zasobów sieci rozproszonych jest to, co Tadeusiewicz określa mianem dymu. W omawianym modelu symbolizuje on informacje bezwartościowe, a nawet szkodliwe, które umieszczane są w sieci przez osoby nieposiadające odpowiednich kompetencji merytorycznych lub użytkowników świadomie generujących przekazy nieprawdziwe czy tendencyjne”.

[6] J. Darczewska, *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego” t. 10 nr 18, s. 40–67.

[7] T.W. Grabowski, *Postprawda a bezpieczeństwo,* [w:] T.W. Grabowski, M. Lakomy, K. Oświecimski, *Bezpieczeństwo informacyjne w dobie postprawdy*, Kraków 2018, s. 16.

[8] M. Szynkiewicz, *Metafora smogu informacyjnego a procesy informacyjne*, op. cit., s. 72.

Badacze zauważają, że „znane z XX wieku masowe oddziaływanie na świadomość za pomocą jednakowych przekazów informacyjnych szybko odchodzi w przeszłość. Państwa w swojej polityce informacyjnej muszą się koncentrować na informacji precyzyjnej, kierowanej do konkretnego odbiorcy (profilu jednostek, grupy odbiorców, segmentu). Podobnie jak w marketingu, w oddziaływaniu informacyjnym państw odchodzi się od masowości na rzecz podejścia zindywidualizowanego”[9]. W niniejszym opracowaniu zwrócimy uwagę na politykę kształtowania bezpieczeństwa państwa poprzez pogłębianie suwerenności informacyjnej.

Internet służy podmiotom o różnym statusie międzynarodowym, których część, tj. suwerenne państwa, posiada w sensie formalno-prawnym uprawnienia kontrolne i represyjne wobec pozostałych, a przy tym dysponuje środkami do konstruowania rzeczywistości poprzez wywieranie wpływu informacyjnego. „Państwa narodowe reaktywują tę fizyczną emanację cyberprzestrzeni, aby usprawiedliwić rozwój środków działania w tej przestrzeni, która wydaje się wymykać ich jurysdykcji i suwerenności”[10]. Państwa stają się równorzędnymi, ale wtórnie aktywnymi współtwórcami infosfery (wymiar informacyjny cyberprzestrzeni), nabywającymi umiejętności posługiwania się nowymi mediami cyfrowymi od podległych sobie uczestników globalnego obiegu informacji tj. jednostek, korporacji i mediów[11]. O ile te ostatnie typy uczestników są osobowymi, kolektywnymi lub instytucjonalnymi konkurentami państw, o tyle ich przeciwnikami stają się antypaństwowe i anarchiczne ruchy społeczne, ugrupowania terrorystyczne i wreszcie – inne państwa prowadzące dawniej walkę ideologiczną tradycyjnymi metodami. Ponadto „rosnące uzależnienie ludzkości od nowoczesnych technologii, sieci komputerowych i Internetu powoduje, że cyberprzestrzeń odgrywa coraz większą rolę w komunikacji strategicznej w państwie i świecie. Uzależnienie to bardzo szybko rośnie, bowiem cyberprzestrzeń wykorzystywana jest nie tylko do odbierania i przekazywania informacji, ale także do koordynacji naszych działań oraz analizy otoczenia w celu oceny potencjalnych zagrożeń i konfliktów”[12].

GEOPOLITYCZNY KONTEKST POLITYKI ROSJI NA RZECZ SUWERENNOŚCI INFORMACYJNEJ

Mocarstwa prowadzą politykę opartą na kilku tendencjach, wśród których znajdziemy: dążenie do hegemonizacji wpływu (globalnego albo o mniejszym zasięgu), dążenie do równoważenia wpływu rywali, dążenie do tworzenia stref wpływów[13]. Hegemonizm absorpcyjny

[9] T.W. Grabowski, *Postprawda a bezpieczeństwo…*, *op. cit*., s. 14.
[10] A. Desforges, *Les représentations du cyberespace: un outil géopolitique*, „Hérodote”: Cyberespace: enjeux géopolitiques, 2014/1–2 (n° 152–153), s. 75.
[11] M. Rukat, *Polityka informacyjna państw w domenie cyfrowej*, Fundacja Bezpieczeństwa i Rozwoju Stratpoints, 2017; Do walki o świadomość ludzi w wymiarze lokalnym, narodowym i międzynarodowym stają także podmioty pozapaństwowe: organizacje międzynarodowe, NGO’s, korporacje międzynarodowe, różnego rodzaju grupy interesu, sieci medialne, oddolne ruchy społeczne itd. T.W. Grabowski, *Postprawda a bezpieczeństwo…*, *op. cit.*, s. 13-14.
[12] Z. Trejnis, P.Z. Trejnis, *Polityka ochrony cyberprzestrzeni w państwie współczesnym*, „Studia Bobolanum”, 28 nr 3 (2017), s. 25.
[13] Szerzej o mocarstwowości *Cf* np. A. Bógdał-Brzezińska, *Mocarstwowość w teorii stosunków międzynarodowych*, [w:] M. Sułek, J. Symonides (red.), *Państwo w teorii i praktyce stosunków międzynarodowych*, Warszawa 2009; J.

pojawia się w analizach polityki mocarstw jako koncept wyjaśniający tendencję przyłączania przez państwa terenów przyległych i jako opozycja do ekspansjonizmu zamorskiego[14] i w niniejszym opracowaniu będzie postrzegany jako atrybut polityki Rosji wobec tzw. bliskiej zagranicy. J. Potulski zwraca uwagę, że hegemonia międzynarodowa uwzględnia oprócz komponentów materialnych emanację *soft power* państwa w postaci interpretacji rzeczywistości międzynarodowej („wytworzonym, dominującym kolektywnym obrazie porządku światowego, włączając w to wartości, na których opiera się ten porządek"[15]. Przywołani przez Potulskiego A. Gramsci i P. Bourdieu stanowią kapitalny punkt odniesienia w poszukiwaniach wyjaśnień dla specyfiki rosyjskiej koncepcji polityki informacyjnej. W świetle refleksji Bourdieu rosyjska wykładnia rzeczywistości międzynarodowej reprezentuje typowy proces narzucania imperializmu Federacji Rosyjskiej (FR) jako oczywistej i naturalnej obrony przed pochodzącym z Zachodu zagrożeniem dla tożsamości i suwerenności. Tak przedstawiana imperialna aksjologia jest przykładem przemocy symbolicznej tj. „wszelkich procesów wpajania norm i wzorów zachowań kulturowych" […] skutkiem których „pewne konkretne sposoby rozumienia świata stają się oczywiste, czy też naturalne, a inne, alternatywne, zaczyna się postrzegać jako bezsensowne lub absurdalne"[16].

Z punktu widzenia geopolityki informacja nie tylko może być, ale wręcz jest traktowana jako narzędzie w walce o osiągnięcie wyznaczonych celów polityki zagranicznej i polityki bezpieczeństwa. Dla geopolitycznego kontekstu polityki Rosji w jej przestrzeni informacyjnej, przy obecnym bardzo dużym zainteresowaniu geopolityką w wydaniu zarówno naukowym, jak i popularnym, celowe wydaje się określenie rozumienia geopolityki w niniejszym tekście. Dla uniknięcia pojęciowych pułapek[17] i wymagającej osobnego tekstu dyskusji, za Merriam Webster przyjęto, iż geopolityka rozumiana będzie po pierwsze jako badanie wpływu takich czynników jak geografia, ekonomia i demografia na politykę, a zwłaszcza na politykę zagraniczną państwa, a po drugie jako polityka rządu kierowana przez geopolitykę. Przy tak zdefiniowanym rozumieniu geopolityki, jej kontekstowe ujęcie suwerenności informacyjnej Rosji obejmuje czynniki istotne, przede wszystkim z punktu widzenia geografii politycznej, a szerzej antropogeografii, oddziaływujące na rosyjską politykę zarówno wewnętrzną, jak i zagraniczną, gdyż w Rosji są one ze sobą ściśle powiązane. Przyjęta definicja narzuca jednocześnie wskazanie geopolitycznych uwarunkowań rosyjskiej polityki.

Bryła, *Strefy wpływów w stosunkach międzynarodowych*, Poznań 2002; S. Bieleń, *Strefy wpływów w stosunkach międzynarodowych*, [w:] *Filozofia, polityka, stosunki międzynarodowe*, Warszawa 1995.

[14] J. Kukułka, *Zaspokajanie potrzeb i rozwiązywanie konfliktów*, [w:] E. Haliżak, R. Kuźniar (red.), *Stosunki międzynarodowe. Geneza, struktura, dynamika*, Warszawa 2006, s. 261–263.

[15] J. Potulski, *Geopolityka w świecie ponowoczesnym*, Częstochowa 2010, s. 141.

[16] *Ibidem*.

[17] Szerzej o problemach badań i terminologii *Cf* np. J. Wendt, *Geopolityczne aspekty tranzytu w Europie Środkowej*, „Geopolitical Studies", no. 6, Warszawa 1999; J. Wendt, *Problemy badań w geostrategii i geopolityce* [w:] H. Rogacki (red.), *Możliwości i ograniczenia zastosowań metod badawczych w geografii społeczno-ekonomicznej i gospodarce przestrzennej*, Poznań 2002, s. 259–266; J. Wendt, *Model dyfuzji innowacji i inne problemy badań w geopolityce i geostrategii*, [w:] Z. Lach, J. Wendt (red.), *Geopolityka. Elementy teorii, wybrane metody i badania*, Częstochowa 2010, s. 86.

Wyzwaniem tego państwa o największym na świecie terytorium jest obecnie zmniejszająca się populacja i niedorozwój ekonomiczny przy niezmiennej konieczności ochrony granic, problemie bardziej dotkliwym w porównaniu z państwami mniejszymi w sensie geoprzestrzennym. W pierwszym z podanych powyżej zagadnień, wśród szeroko rozumianych czynników geograficznych w zakresie wewnętrznych problemów Rosji, na czoło wysuwa się kwestia demografii. Od początku lat 90. XX wieku Rosję w nowych granicach[18], w których nigdy wcześniej nie funkcjonowała, na olbrzymim, lecz słabo zaludnionym terytorium, cechuje prawie stale ujemny przyrost naturalny, którego skutki w pewnym stopniu łagodzi imigracja głównie z państw postradzieckich, jednak średni spadek liczby obywateli Federacji Rosyjskiej pomimo migracji sięga około 200 tys. rocznie. Aby w jakimś zakresie przeciwdziałać negatywnym skutkom tego procesu, Rosja w zakresie polityki wewnętrznej promuje i premiuje wzrost dzietności, a w polityce zewnętrznej prowadzi działania na rzecz inkorporacji ziem, określanych lub uznawanych za rosyjskie, przykładem jest Krym wraz ze wschodnią Ukrainą, jak i prowadzona przez Rosję polityka wobec Białorusi.

Wsparcie i utrzymanie wpływów rosyjskich widoczne jest również w państwach sukcesorach ZSRR o znaczącym udziale mniejszości rosyjskiej. Rosja prowadziła lub prowadzi w obronie praw i pozycji mniejszości rosyjskiej wojnę informacyjną w Estonii, na Litwie, w Gruzji i na Ukrainie. Rosyjskojęzyczne media obecne są w Azji Środkowej, a w Kazachstanie i Kirgistanie język rosyjski jest drugim językiem urzędowym, co ułatwia prowadzenie polityki informacyjnej przy udziale tradycyjnych mediów. Ważny jest również wpływ i rola rosyjskiej cerkwi prawosławnej[19] w utrzymaniu wpływów rosyjskich wśród mniejszości prawosławnej w Kazachstanie, na Białorusi, a do ostatniej decyzji o autokefalii lokalnej cerkwi także na Ukrainie.

Pod względem ekonomicznym Rosja nadal jest krajem, którego gospodarka zależna jest od globalnych zmian cen surowców na światowych rynkach. W swoim bliskim sąsiedztwie, „wyparta z Europy" Rosja[20] tworzy alternatywne struktury pod swoją egidą – Euroazjatycka Unia Celna (2010) wraz z Euroazjatycką Unią Gospodarczą (2014) petryfikują gospodarcze relacje Armenii, Białorusi, Kazachstanu i Kirgistanu z Rosją. Prowadzona przez Rosję polityka obejmująca budowę gazociągów oraz zróżnicowanie zgodnie z istniejącymi relacjami politycznymi cen eksportowanych przez Rosję surowców energetycznych skutecznie osłabia prowadzenie wspólnej polityki zapewniającej bezpieczeństwo energetyczne przez państwa UE czy Grupy Wyszehradzkiej.

Tak zakreślone czynniki wpływające na politykę Rosji realizowane są w jej sąsiedztwie. Rosja od powstania Federacji prawie nieustannie prowadzi działania wojenne realizując swoją

[18] J. Zupančič, J.A. Wendt, A. Ilieș, A*n outline of border changes in the area between the Baltic and the Mediterranean: their geopolitical implications and classification*, „Geographia Polonica", 91 (1)/ 2018, s. 33–46.
[19] K. Świder, *Geopolityka jako światopogląd władzy w Rosji*, „Teka Kom. Politol. Stos. Międzynar.", OL PAN, 2016, 11 (3), 35–58, s. 54.
[20] *Vide*: J. Potulski*, „Rosja wyparta z Europy" – konsekwencje dla porządku międzynarodowego na progu XXI w.*, „Środkowoeuropejskie Studia Polityczne", nr 1/2010, s. 97–110.

neoimperialną politykę[21]. Regiony konfliktów, co nie dziwi znając przedmiotowe traktowanie wspieranych mniejszości, to od 1991 r. kolejno Gruzja, Abchazja, Transistria, Północna Osetia, Czeczenia, Dagestan, Południowa Osetia, Półwysep Krymski, regiony Doniecka i Ługańska, a w ostatnich latach także Syria, gdzie Federacja Rosyjska występuje jako silny gracz powracający na arenę działań międzynarodowych. Hegemon zmierza do legitymizacji siłowych praktyk w środowisku międzynarodowym, a roszczeniowość Rosji jest wzmacniana przez ideologię imperialną, uzupełnioną oskarżeniami wobec Zachodu o imperializm moralny. „Rosja przekształciła realny konflikt ukraińsko-rosyjski i interwencję zbrojną na Ukrainie w wirtualny konflikt Rosji z Zachodem"[22], co tłumaczy opisany w dalszej części artykułu proces osiągania pogłębionej suwerenności FR w Internecie.

Jednak słabość gospodarczo-technologiczna, przy problemach demograficznych, olbrzymim terytorium nie pozwala Rosji, pomimo zamierzeń części rosyjskich elit[23], na pozycjonowanie się w roli mocarstwa światowego. Co prowadzi z jednej strony politykę Federacji Rosyjskiej do uznania albo świata wielobiegunowego, albo chociaż do walki o powrót „koncertu mocarstw" w Euroazjatyckiej przestrzeni. Narzędziami prowadzącymi do realizacji tego celu jest destabilizacja bliskiej zagranicy (Estonia, Ukraina czy Gruzja), realizacja unii z Białorusią, wzmocnienie wpływów w Euroazjatyckiej unii celnej i gospodarczej oraz osłabienie wszystkich potencjalnych przeciwników restytucji rosyjskiej przewagi w Euroazji. Z Chinami lub przeciw Chinom, co w zasadzie zależy od polityki USA, EU i Chin. Brutalnie pisząc, „kto da Rosji więcej", osłabiając jedynie świat zachodni przez prowadzenie skutecznej polityki informacyjnej i wojny w cyberprzestrzeni, gdyż Chiny nie są na takie osłabiające działania wrażliwe. To ostatnie z omówionych działań przynosi Rosji doraźne efekty pozytywne w postaci dezorganizacji życia społeczno-politycznego w krajach-adresatach działań ofensywnych w cyberprzestrzeni, a długofalowo – jest elementem odstraszania rywali Rosji lub drogą do naśladownictwa państw autorytarnych o podobnym poziomie rozwoju ICT. Jednak w kategoriach długoterminowych działania cyberofensywne wymagają od Federacji pogłębionej kontroli rosyjskiego Internetu (Runetu) i uznania całej globalnej sieci za przestrzeń geopolityczną.

GEOPOLITYKA CYBERPRZESTRZENI A GEOPOLITYKA INFORMACYJNA

Pojęcie geopolityki cyberprzestrzeni zostało upowszechnione we francuskim dyskursie naukowym, na łamach czasopisma „Herodote", które już w 1997 r. zwiastowało „internetyzację geopolityki". Wskazywano, że „Internet zwielokrotni konflikty o naturze geopolitycznej, prowadząc do strategii dominacji z udziałem państw o rozbieżnych interesach. Jest to broń

[21] K.A. Kowalczyk, *Geopolityczne dążenia współczesnej Rosji*, „Przegląd Geopolityczny", 2019, 27, s. 84.
[22] J. Darczewska, *Rosja zbroi się do wojny informacyjnej z zachodem*, „Biuletyn Rządowego Centrum Bezpieczeństwa" 22.12. 2014, s. 4.
[23] R. Ištok, D. Plavčanová, *Russian geopolitics and geopolitics of Russia: phenomenon of space*, „European Journal of Geopolitics", 2013, 1, s. 61.

o znaczeniu strategicznym dla bezpieczeństwa państw”[24]. Po ponad 15 latach od pierwszych publikacji poświęconych zagadnieniu ukazał się numer tematyczny czasopisma potwierdzający aktualność założeń omawianego konstruktu pojęciowego[25]. Diagnozowano, że „sieć [Internet] sama jest zagrożona wieloma konfliktami geopolitycznymi, które prowadzą do strategii dominacji narodów o rozbieżnych interesach, które starają się kontrolować jej zawartość, funkcjonowanie i rozwój gospodarczy. Jest to wysoce strategiczna broń dla bezpieczeństwa narodów, [...] a przede wszystkim niezwykle potężny instrument w rywalizacji o władzę między grupami, mniejszościami, siłami politycznymi, religijnymi, gospodarczymi, zarówno na poziomie lokalnym, jak i światowym”[26]. Choć geopolitycy uznają za niemożliwe wyznaczenie w cyberprzestrzeni lokalizacji tradycyjnie postrzeganych pojęć (Heartlandu, Rimmlandu), to jednak istnieje ogólna zgoda, że znajdujemy się w początkowej fazie sukcesywnego wzrostu znaczenia cyberprzestrzeni dla sfery stosunków międzynarodowych, a awet, że będzie to epoka cybernetyzacji stosunków międzynarodowych[27].

W dyskursie badawczym o suwerenności w cyberprzestrzeni stosowane jest określenie „cyberwestfalia”[28], które możemy odnaleźć w opracowaniach prawników międzynarodowych, politologów i specjalistów od bezpieczeństwa. Z kolei geografowie stosują określenie „bałkanizacji Internetu” (cyberbałkanizacji), w którym streszcza się „tendencja do odtwarzania fizycznych granic pomiędzy państwami w przypadku funkcjonowania Internetu i sieci WWW”[29] albo szerzej – ogół zjawisk prowadzących do rozgraniczenia globalnej sieci, wzrostu kontroli nad treściami internetowymi oraz nad infrastrukturą sieciową. O pozycji międzynarodowej państwa ma świadczyć zdolność zachowania pełnej suwerenności cybernetycznej, rozumianej jako efektywny system cyberobrony celów infrastruktury krytycznej i cyberataków jako rodzaju retorsji. Przypuszczalnie w dłuższym czasie należy się spodziewać przeniesienia do cyberprzestrzeni wszystkich atrybutów suwerennego państwa, przy czym za „państwa cyber-upadłe” będą uznawane te, które nie zdołają wykonywać kompetencji w sferach społecznej, gospodarczej i obronnej z udziałem narzędzi ICT.

Zarówno terminologia zachodnia (geopolityka cyberprzestrzeni), jak i rosyjska (geopolityka informacyjna) legitymizują traktowanie Internetu jako sfery komplementarnej do przestrzeni terytorialnej współczesnych państw. W rosyjskiej doktrynie bezpieczeństwa informacyjnego znajduje rezonans idea ładu cyberwestwalskiego, która wyrasta z odtwarzania

[24] F. Douzet, *Internet géopolitise le monde*, „Hérodote” 1997, 1 (86–87), s. 222–233.
[25] „Hérodote”: *Cyberespace: enjeux géopolitiques*, 2014/1–2 (152–153).
[26] F. Douzet, *La géopolitique pour comprendre le cyberespace*, „Hérodote”2014/1–2 (152-153), s. 3.
[27] J.F. Popa, *Cyber Geopolitics And Sovereignty. An Introductory Overview*, Paper Conference, Conference: 5th International scientific conference „National and International Security” At: Armed Forces Academy of General Milan Rastislav Štefánik, October 2014, s. 2. (31.12.2019).
[28] Por. np. C. Demchak, P. Dombrowski, *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*, „Georgetown Journal of International Affairs, International Engagement on Cyber III: State Building on a New Frontier”, 2013, s. 29–38.
[29] K. Janc, *Geografia Internetu*, Wrocław 2017, s. 91.

przez decydentów politycznych zwierzchności i kontroli tradycyjnie odnoszonej do terytoriów państwowych. Rywalizacja w globalnej infosferze to walka o rewizję porządku globalnego.

Geopolityka informacyjna jest przedstawiana w dyskursie rosyjskim jako gałąź nauki i jako swoista praktyka polityczna. W pierwszym ujęciu bada zależność życia społeczno-politycznego od „zwirtualizowanej" zagregowanej przestrzeni życiowej tj. globalnej infosfery integrującej technologie informacyjne, systemy informacyjne i telekomunikacyjne oraz informacje – treść. Z tej perspektywy wojna informacyjno-psychologiczna, ze względu na duże zagrożenie społeczne, jest najważniejszym czynnikiem determinującym cele, zadania i główne kierunki polityki informacyjnej państwa. Rosyjska polityka informacyjna podporządkowana jest w ścisły sposób polityce bezpieczeństwa informacyjnego i wynika z przedstawionego powyżej interpretowania geopolityki informacyjnej. W ostatnich latach pojawiają się liczniejsze komentarze uzasadniające nacjonalizację polityki informacyjnej FR, którym towarzyszy duch legalizmu, a nawet dziejowej konieczności[30]. „O tej sferze działalności państwa decydują interesy narodowe mające na celu wzmocnienie suwerenności informacyjnej, zapewnienie bezpieczeństwa informacji, integralności krajowej przestrzeni informacyjnej, jej adekwatnej integracji z globalną przestrzenią informacyjną"[31]. Pojawiają się również przestrogi przed niedoszacowaniem roli informacji dla funkcjonowania państwa: „odrzucenie krajowej suwerenności informacyjnej, zaniedbanie w jakiejkolwiek formie wymogu drobiazgowego przestrzegania krajowych interesów w sferze informacyjnej nieuchronnie doprowadzi do utraty kontroli nad suwerennością państwa jako całością"[32]. Głównym doktrynerem rosyjskiej koncepcji suwerenności cyfrowej jest I. Ashmanov, definiujący ją jako prawo i zdolność rządu krajowego do niezależnego określania geopolitycznych interesów narodowych w cyberprzestrzeni[33]. Przestrzeń Internetu jest uznawana za terytorium geopolityczne (lub „geodigitalne"), a intencją jest wyznaczenie jego „granic cyfrowych", które wymaga określania i ochrony granic rosyjskiej „przestrzeni informacyjnej".

ROSYJSKA WIZJA SUWERENNOŚCI W INTERNECIE – CENZURA TREŚCI I KONTROLA INFRASTRUKTURY TECHNICZNEJ

Lata 90. XX wieku były okresem ustrojowej niestabilności rozpadającego się ZSRR i przejmującej po nim sukcesję Federacji Rosyjskiej. Zastrzeżenia adresowane wówczas do władz rosyjskich przez państwa szeroko pojętego Zachodu obejmowały m.in. przekonania, że: rosyjska demokracja nie spełnia zachodnich standardów, Rosja wciąż jest daleka od

[30] П.В. Меньшиков *Эволюция государственной информационной политики в России*, „Журнал Международные коммуникации" 2017 (4): „pełne zaangażowanie państwa w regulacje polityki informacyjnej jest historycznie logiczne, zgodne z prawem i konieczne dla rozwoju pełnoprawnej otwartej informacyjnej przestrzeni narodowej" (20.12.2019).
[31] *Ibidem*.
[32] *Ibidem*.
[33] M. Ristolainen, *Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West*, „Journal of Information Warfare", 16, 4 (Fall 2017), s. 117.

zachodniego ideału otwartej gospodarki ze stabilnymi przepisami, atrakcyjnym systemem podatkowym i rozwiniętą infrastrukturą; Rosja arogancko sprzeciwia się Zachodowi, nie rezygnując z pomocy gospodarczej, a społeczeństwo rosyjskie jest głęboko skryminalizowane i skorumpowane. Wydawało się, że państwo pogrąży się w chaosie wewnętrznym, podsycanym toczonymi wojnami w obszarze „bliskiej zagranicy".

Nowe millenium przyniosło fundamentalną zmianę polityczną związaną z objęciem urzędu prezydenta Rosji przez Władimira Putina, który już w pierwszych miesiącach urzędowania zadekretował dwa kluczowe dokumenty dla rozwoju polityki informacyjnej państwa, tj. Strategię e-Rosja, poświęconą społeczeństwu informacyjnemu i Doktrynę bezpieczeństwa informacyjnego. Dokumenty te stanowiły odpowiedź na oczekiwania społeczne, wyrażane nawet w niezależnym dyskursie medialnym. W roku 2000 np. A. Kokoszkin w artykule pt. „Nowy kontekst międzynarodowy. Interesy bezpieczeństwa narodowego Rosji w warunkach globalizacji", zamieszczonym na łamach „Niezawisimoj Gazety", przedstawił znaczenie sektora informacyjnego dla bezpieczeństwa państwa. W opinii dziennikarza stopień wykorzystania Internetu przez rząd jest asymetryczny w stosunku do globalnych aspiracji państwa i nie odpowiada ani statusowi wielkiego mocarstwa, ani poziomowi naukowo-technicznemu Rosji, ani jej potencjałowi kulturalno-cywilizacyjnemu. Publicysta podkreślał, że w polityce informacyjnej Rosja nie może naśladować żadnego państwa, wspólnoty (UE) ani organizacji międzynarodowej. Jej przygotowanie musi zostać połączone z ogólną koncepcją bezpieczeństwa FR. Doktrynę bezpieczeństwa informacyjnego należy stworzyć w takiej formie, by objęła swym oddziaływaniem byłe republiki ZSRR (bliska zagranica bezpieczeństwa informacyjnego). Powinna zyskać charakter otwartej oferty współpracy z innymi państwami, być skorelowana z koncepcją europejskiego społeczeństwa informacyjnego, kompatybilna z doktrynami informacyjnymi Chin i Indii oraz innych krajów Azji. Wszystko po to, by koncepcja rosyjska służyła za pomost między koncepcjami krajów Europy i Azji[34]. Te ostatnie założenia nawiązywały do najpopularniejszej geopolitycznej koncepcji rosyjskiej autorstwa A. Dugina, spopularyzowanej na przełomie wieków, która również obecnie ma wpływ na praktykę rosyjskiej walki informacyjnej[35].

Ośrodki analityczne na Zachodzie odnotowały zmianę w rozumieniu przez nowe władze Federacji polityki informacyjnej w sieci, aczkolwiek pierwotnie nie doceniano konsekwencji działań kontrolnych i centralizacyjnych Internetu[36]. Tymczasem obowiązująca od 2000 do 2016 r. włącznie pierwsza z dwóch dotąd przyjętych doktryn informacyjnych FR wskazywała wyraźnie na intencję suwerenizacji przestrzeni informacyjnej zarówno wirtualnej, jak i rzeczywistej[37].

[34] A. Bógdał-Brzezińska, *Rosja, Ukraina i Białoruś: koncepcje społeczeństwa informacyjnego i gospodarki opartej na wiedzy*, „Stosunki Międzynarodowe", t. 30/2004, s. 169–189.
[35] M. Wojnowski, *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" t. 17 (9)/2017.
[36] J.R. Azrael, D.J. Peterson, *Russia and the Information Revolution*, „RAND Issue Paper", IP-229-CRE (2002), s. 9.
[37] Por. R. Białoskórski, *Cyberprzestrzenny wymiar polityki bezpieczeństwa i obrony Federacji Rosyjskiej*, [w:] M. Minkina, M. Kaszuba (red.), *Polska - Rosja: polityka bezpieczeństwa Federacji Rosyjskiej. Kontynuacja i zmiana*, Siedlce 2016, s. 7–8; A. Bógdał-Brzezińska, *Rosja, Ukraina i Białoruś…*, *op. cit.*

Konsekwencją jest inne w stosunku do USA czy NATO nadawanie Internetowi znaczenia strategicznego, gdyż Rosjanie nie uważali do 2017 r. cyberprzestrzeni za odrębny obszar działań wojennych – obok powietrza, morza, lądu czy przestrzeni kosmicznej[38].

Doktryna z 2000 r. (DBI 2000) stanowi zapowiedź powrotu Rosji do ofensywnej propagandy imperialnej, ograniczającej wedle kryterium nadrzędności bezpieczeństwa narodowego nad wolnością mediów czy wolnością obrotu gospodarczego czy wolnością wypowiedzi obywateli. W związku ze wzrostem roli informacji bezpieczeństwo narodowe uzależnione jest coraz bardziej od postępu w kontroli sektora informacyjnego. Wśród obszarów profilujących politykę informacyjną za istotne uznaje się zagraniczną propagandę państwową, pogłębienie kontroli nad modernizacją systemów informacyjnych, ukierunkowanych na tworzenie pozytywnego wizerunku zewnętrznego państwa w kraju i zagranicą. Główne zagrożenia wskazane w dokumencie to: działalność wywiadów i grup informacyjnych państw trzecich, dążenie innych państw do ograniczenia interesów Rosji w światowym obrocie informacyjnym, zawężenie jej aktywności na informacyjnych rynkach wewnętrznych i zagranicznych, uzupełnianie doktryn wojennych innych państw elementami koncepcji walki informacyjnej, działalność cyberterrorystyczna[39].

Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej z 2016 r. (DBI 2016) rozwija i uzupełnia treści pierwszego z dokumentów, wskazując na informację jako kluczowy komponent sfery politycznej[40]. Wyraża potrzebę większej wiarygodności informacji o polityce narodowej oraz pozycji geopolitycznej Rosji, wskazuje na współuczestnictwo w tworzeniu światowego systemu bezpieczeństwa informacyjnego. Pojawia się obawa przed wrogimi wpływami informacyjnymi, zwiększeniem się aktywności wywiadowczej wymierzonej w Rosję, dyskryminacją mediów rosyjskich przez zagranicę. Za główne zagrożenia dla bezpieczeństwa informacyjnego uznaje instytucje i służby specjalne innych państw w zakresie cyberataków na infrastrukturę krytyczną Federacji, organizacje i instytucje rozpowszechniające fałszywe informacje o Rosji, dążenie wrogich państw do dominacji w sferze informacyjnej Rosji. Z dokumentu wynika diagnoza, że niski poziom rozwoju ICT jest skutkiem uzależnienia Federacji od zagranicznych firm. W DBI 2016 stwierdza się ponadto, że źródłem zagrożeń dla interesów państwa w sferze informacyjnej są: instytucje i służby specjalne innych państw rozwijające ICT niebezpieczne dla infrastruktury krytycznej FR; organizacje i instytucje rozpowszechniające fałszywe informacji o Rosji; ofensywna polityka niektórych państw prowadząca do dominacji w sferze informacyjnej Rosji; niski poziom rozwoju ICT jako następstwo uzależnienia od zagranicznych firm; zwiększenie się aktywności wywiadowczej wymierzonej w Rosję; dyskryminacja mediów rosyjskich zagranicą.

[38] A. Kozłowski, *Cyberwojownicy Kremla*, „Biuletyn OPINIE FAE", nr 6/2014, s. 2.
[39] Por. A. Bógdał-Brzezińska, *Rosja, Ukraina i Białoruś…*, op. cit.
[40] Por. K. Basaj, *Analiza nowej doktryny informacyjnej Rosji*, 30.12.2016; A. Kuczyńska-Zonik, *Strategia bezpieczeństwa informacyjnego Federacji Rosyjskiej*, [w:] J. Trubalska, Ł. Wojciechowski (red.), *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017.

W DBI 2016 stwierdza się ponadto, że źródłem zagrożeń dla interesów państwa w sferze informacyjnej są: instytucje i służby specjalne innych państw rozwijające ICT niebezpieczne dla infrastruktury krytycznej FR; organizacje i instytucje rozpowszechniające fałszywe informacji o Rosji; ofensywna polityka niektórych państw prowadząca do dominacji w sferze informacyjnej Rosji; niski poziom rozwoju ICT jako następstwo uzależnienia od zagranicznych firm; zwiększenie się aktywności wywiadowczej wymierzonej w Rosję; dyskryminacja mediów rosyjskich zagranicą.

Rosyjskie władze konsekwentnie rozwijają ideę suwerenności cyfrowej, poczynając od kwestii semantycznych: pojęcie cyberprzestrzeni kojarzone z globalnym wpływem korporacji technologicznych jako narzędziem państw zachodnich zastępowane jest określeniem „przestrzeń informacyjna". Jak pisze K. Limonier, „rosyjskie myślenie strategiczne nie uznaje istnienia cyberprzestrzeni, która byłaby obiektem szczególnego rodzaju, i który wymagałby własnych zasad zarządzania. Przeciwnie, uważa się, że sieci cyfrowe, takie jak Internet, podobne są do innych mediów, do których państwo zwykle ma prawo regulacyjne"[41]. W 2012 r. w Rijadzie podczas szczytu Międzynarodowego Związku Telekomunikacyjnego (ITU) delegacja rosyjska postulowała przeniesienie praw do nadawania adresów IP z prywatnej w istocie organizacji pozarządowej ICANN z siedzibą w USA na uzgodnioną agendę ONZ, której kompetencje byłyby mniej dyskusyjne niż obecnie[42]. W konsekwencji rosyjski Internet (Runet) ilustruje ugruntowaną doktrynalnie regułę kontroli państwa ponad wszelkimi przejawami aktywności obywatelskiej. Rok miniony był dla władz rosyjskich czasem poświęconym udokumentowaniu suwerenności w cyberprzestrzeni. W związku z pracami nad ustawą „Narodowy Program Gospodarki Cyfrowej" do kwietnia przyjęto decyzję o przeprowadzeniu testów zamknięcia ruchu między Runetem a Internetem zewnętrznym w sytuacji zagrożenia. Od 2017 r. trwały prace w kierunku ochrony zasobów internetowych, których częścią jest tworzenie kopii adresów domen internetowych[43]. W kwietniu 2019 r. przyjęto ustawodawstwo legalizujące odłączenie Runetu od globalnej sieci w obliczu zdefiniowanych dyskrecjonalnie zagrożeń bezpieczeństwa państwa. „Ustawa przewiduje też, że w Rosji powstanie w najbliższych latach narodowy system nazw domenowych, niezależny od obecnego systemu DNS nadzorowanego przez organizację ICANN. Ponadto do 2021 roku rosyjskie organy państwowe będą musiały przejść całkowicie na krajowe systemy szyfrowania" (koszty około 30 mld rubli, ponad 467 mln USD)[44]. Informację o technicznych przygotowaniach do odcięcia Runetu od sieci globalnej, poprzez wyposażenie providerów w narzędzia blokujące swobodę przepływu danych, podano we wrześniu[45].

[41] K. Limonier, *La Russie dans le cyberespace: représentations et enjeux*, „Hérodote": *Cyberespace: enjeux géopolitiques*, 2014/1–2 (n° 152–153), s. 143.
[42] *Ibidem*, s.144.
[43] S. Palczewski, *Rosja odłączona od globalnej sieci. Wielki test Moskwy*, CyberDefence 24, 11.02.2019.
[44] *Rosja przyjęła ustawę w sprawie Runetu. Internet w izolacji od globalnej sieci*, 24.04.2019.
[45] S. Palczewski, *„Wszystko idzie zgodnie z planem" – Rosja odcina się od globalnej sieci*, CyberDefence 24, 25.09.2019.

Z danych międzynarodowych wynika znaczący udział Rosji w procesach cenzury Internetu, który nasila się od dłuższego czasu. K. Janc, przywołując raport *Freedom of the Net 2016,* wskazuje na zajmowanie przez Rosję pozycji państwa zniewolonego (tj. o bardzo zaostrzonej cenzurze sieci), skutkiem zaś sprawowania silnej kontroli nad Internetem przez państwo jest stosunkowo słaby poziom rozwoju podstaw funkcjonowania społeczeństwa informacyjnego[46] (korelacja ujemna). Z drugiej strony warto zauważyć, że Rosja zajmuje wysokie miejsca w rankingach liczby i intensywności wykorzystania tzw. sieci rozproszonych, których celem jest unikanie przez użytkowników mechanizmów cenzury. 5% tych sieci i 13% ich użytkowników pochodziło z Rosji[47], co wskazuje, że rosyjscy internauci szukają sposobów uczestnictwa w nieograniczonym obiegu informacyjnym.

Wszelako warto zauważyć, że z Runetu korzysta ok. 105 mln, czyli 73% Rosjan. Rosjanie preferują własną wyszukiwarkę Yandex (rosyjski Google) oraz rodzimy odpowiednik Facebooka – serwis społecznościowy Vkontakte (VK.com). Runet jest pośrednim narzędziem wspierającym trendy integracyjne z udziałem Rosji w strefie bliskiej zagranicy, znakiem odrodzenia imperialnego potencjału. Runet obejmuje użytkowników, którzy posługują się językiem rosyjskim jako podstawowym dla pozyskiwania informacji w sieci. Należą do nich oprócz mieszkańców Federacji oraz transkontynentalnej diaspory rosyjskiej również internauci z Białorusi czy republik Azji Środkowej, słowem – staje się przestrzenią dodatkową scalającą WNP. Słuszne wydaje się zatem stwierdzenie o Runecie jako przestrzeni dodatkowej suwerenności Rosji, większej od jej granic fizycznych[48]. Język rosyjski jest fundamentalnym warunkiem sukcesu idei Runetu jako extraterritorium, stąd tak intensywnie rozwijane media tradycyjne z telewizją Russia Today (obecnie RT) jako głównym narzędziem propagandowym adresowanym do średniego i starszego pokolenia byłych mieszkańców ZSRR i diaspory rosyjskiej na całym świecie. Runet ma być petryfikatorem nawiązań do radzieckiej tradycji epatowania poczuciem zagrożenia i do neozimnowojennej retoryki.

W opracowaniach odnoszących się do zagadnień suwerenności państw w cyberprzestrzeni pojawiają się i takie, które wydają się usprawiedliwiać działania na rzecz cenzury Internetu, propagandy elektronicznej, walki informacyjnej. Są one utożsamiane z realizacją tradycyjnych funkcji państwa w zakresie polityki zagranicznej z wykorzystaniem nowoczesnych technologii informacyjnych. Spotyka się nawet pojęcie cyberdyplomacji, definiowanej „jako dyplomacja w domenie cybernetycznej lub, innymi słowy, wykorzystanie zasobów dyplomatycznych i wykonywanie funkcji dyplomatycznych w celu zabezpieczenia interesy narodowe w odniesieniu do cyberprzestrzeni”[49].

[46] K. Janc, *Geografia Internetu,* op. cit., s. 236.
[47] *Ibidem*, s. 246–247.
[48] B. Gołąbek, *Runet jako extra territorium byłego ZSRR – wokół rosyjskiej cybergeopolityki,* [w:] L. Sykulski (red.), *Studia nad rosyjską geopolityką,* Polskie Towarzystwo Geopolityczne, Częstochowa 2014.
[49] A. Barrinha, T. Renard, *Cyber-diplomacy: the making of an international society in the digital age*, „Global Affairs”, 2017, 3:4–5, s. 355.

Zdaniem ekspertów zachodnich odłączenie Runetu od globalnej sieci miałaby następstwa dla bezpieczeństwa międzynarodowego: pogłębiłoby rolę informacji jako narzędzia walki, przyczyniłoby się do uznania fragmentacji globalnego Internetu za dopuszczalne i naturalne zjawisko oraz utrwaliłoby nawyki państw w zakresie cyberodstraszania[50].

PODSUMOWANIE

Zgodnie z przedstawionym we wstępie celem pracy, na podstawie przeprowadzonej analizy można z dużym prawdopodobieństwem uznać za pozytywnie zweryfikowane tezy o podjęciu przez Rosję jako aktora na międzynarodowej scenie politycznej szeroko zakrojonych działań dezinformacyjnych w cyberprzestrzeni zgodnie z determinującymi jej położenie czynnikami geopolitycznymi. W sferze polityki zewnętrznej informacja zarówno przekazywana przez media tradycyjne, jak i w Internecie lub przez instytucje zależnie od państwa rosyjskiego (cerkiew, organizacje państw postradzieckich) służy klasycznej, lecz prowadzonej wielotorowo walce o utrzymanie raczej deklarowanej niż realnej globalnej potęgi Federacji Rosyjskiej. Co ważne, w większości przypadków obrona „ruskiego miru" ma raczej na celu potwierdzenie pozycji władz i kraju na użytek wewnętrzny dla utrzymania władzy przez obecne elity i pacyfikacji demokratyzującego się, o ironio także dzięki Internetowi, społeczeństwa rosyjskiego, niż uzyskanie realnej przewagi na „wielkiej szachownicy". Nie należy jednak lekceważyć oddziaływania rosyjskich działań w cyberprzestrzeni, czego przykładem jest szeroko dyskutowany w mediach zachodnich wpływ rosyjskich trolli na wybory np. w USA czy wsparcie działań części brytyjskiego establishmentu w zakresie Brexitu. Nie tyle chodzi tu o podanie udanych przykładów rosyjskich akcji w cyberprzestrzeni, a o podkreślenie wykorzystania działań informacyjnych dla realizacji stałych w polityce rosyjskiej celów geopolitycznych lub przeciwdziałanie zagrożeniom, realnym czy jedynie wyimaginowanym.

Podobnie ocenić można prowadzenie działań informacyjnych z wykorzystaniem cyberprzestrzeni w zakresie polityki wewnętrznej. Runet, którego wprowadzenie przegłosowano w 2019 r., w teorii ma zabezpieczyć Rosję przed potencjalnymi, jednak nieokreślonymi na razie zagrożeniami związanymi z globalną siecią. W przypadku takich zagrożeń scentralizowane zarządzanie siecią przejąć może Roskomnadzor, obecnie regulujący funkcje informacyjne mediów i Internetu w Rosji. Podporządkowanie sieci, w dowolnej, zależnej od władzy instytucji ma swoje ewidentne plusy w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni, równocześnie jednak kusi możliwością ograniczenia wewnętrznego przepływu informacji, a projektowane centrum monitoringu wraz z określeniem limitowanej liczby punktów dostępu sieci rosyjskich do sieci globalnej skutecznie pozwoli kontrować obieg informacji w wewnętrznym systemie rosyjskiego Internetu, co wprost prowadzić może do jego pełnej kontroli, cenzury, a w efekcie końcowym do ograniczenia dostępu do informacji krążącej wewnątrz systemu i do jej przekazywania do sieci globalnej. Jest to jednak w pełni zgodne z dotychczasową polityką wewnętrzną prowadzoną przez

[50] M. Ristolainen, *Should…*, *op. cit.*, s. 124.

Federację Rosyjską, a dodatkowo w pełni sprzyja realizacji celów politycznych obecnej władzy. W końcu w dobie Internetu truizmem jest stwierdzenie, iż wiedza oznacza władzę, której przede wszystkim zależy na zapewnieniu bezpieczeństwa, w pierwszej kolejności sobie, w drugiej bezpieczeństwa zewnętrznego, co przy słabości ekonomicznej Rosji coraz bardziej skłania do wojny informacyjnej w cyberprzestrzeni, w miejsce kosztownych zbrojeń i wyścigów ekonomicznych, a wreszcie w trudnym do określenia stopniu służyć może także zapewnieniu pierwotnego i marketingowego w polityce celu – bezpieczeństwa obywateli, przy ewidentnym ograniczeniu dostępu do informacji.

BIBLIOGRAFIA

Azrael Jeremy R., Peterson Donald J. 2002. Russia and the Information Revolution, "RAND Issue Paper", IP-229-CRE.

Barrinha Andre, Renard Thomas. 2017. "Cyber-diplomacy: the making of an international society in the digital age". Global Affairs Vol. 3 (4-5) : 353-364.

Basaj Kamil. 2018. Rosyjska ofensywa propagandowa w cyberprzestrzeni oraz inicjatywy podejmowane przez NATO i UE w celu przeciwdziałania temu zjawisku. Nowy Biuletyn RCB, Marzec. W http://rcb.gov.pl/rosyjska-ofensywa-propagandowa-w-cyberprzestrzeni-oraz-inicjatywy-podejmowane-przez-nato-i-ue-w-celu-przeciwdzialania-temu-zjawisku.

Basaj Kamil. 2016. Analiza nowej doktryny informacyjnej Rosji. W https://www.cybsecurity.org/pl/analiza-nowej-doktryny-informacyjnej-rosji/.

Białoskórski Robert. 2016. Cyberprzestrzenny wymiar polityki bezpieczeństwa i obrony Federacji Rosyjskiej. W M. Minkina, M. Kaszuba (red.) Polska – Rosja: polityka bezpieczeństwa Federacji Rosyjskiej. Kontynuacja i zmiana, 13–30. Siedlce: Wydawnictwo UHP.

Bieleń Stanisław. 1995. Strefy wpływów w stosunkach międzynarodowych, W Filozofia, polityka, stosunki międzynarodowe, Warszawa: Wydawnictwo Naukowe Scholar.

Bógdał-Brzezińska Agnieszka. 2009. Mocarstwowość w teorii stosunków międzynarodowych. W M. Sułek, J. Symonides (red.) Państwo w teorii i praktyce stosunków międzynarodowych, 89–114. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.

Bógdał-Brzezińska Agnieszka. 2004. „Rosja, Ukraina i Białoruś: koncepcje społeczeństwa informacyjnego i gospodarki opartej na wiedzy". Stosunki Międzynarodowe t. 30: 169–189.

Bryła Jolanta. 2002. Strefy wpływów w stosunkach międzynarodowych, Poznań: Wydawnictwo Naukowe INPiD UAM.

Darczewska Jolanta. 2014. „Rosja zbroi się do wojny informacyjnej z zachodem". Biuletyn Rządowego Centrum Bezpieczeństwa nr 9: 3–8.

Darczewska Jolanta. 2015. Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji. Punkt widzenia nr 50: 1–39.

Darczewska, Jolanta. 2017. Dezinformacja – rosyjska broń strategiczna. W http://rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/.

Darczewska, Jolanta. 2018. „Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy". Przegląd Bezpieczeństwa Wewnętrznego t. 10 nr 18: 40–67.

Demchak Chris C., Dombrowski Peter. 2013. „Cyber Westphalia: Asserting State Prerogatives in Cyberspace", Georgetown Journal of International Affairs, „International Engagement on Cyber III: State Building on a New Frontier" (December), s. 29–38.

Douzet Frederick. 1997. „Internet géopolitise le monde". Hérodote Vol 1 (86-87): 222–233.

Douzet Frederick. 2014. „La géopolitique pour comprendre le cyberspace". Hérodote Vol 1-2 (152-153): 161–173.

Gawkowski Krzysztof. 2018. Cyberkolonializm, Poznaj świat cyfrowych przyjaciół i wrogów. Gliwice: Wydawnictwo Helion.

Gołąbek Bartosz. 2014. Runet jako extra territorium byłego ZSRR – wokół rosyjskiej cybergeopolityki, W L. Sykulski (red.) Studia nad rosyjską geopolityką, 69–100. Częstochowa: Polskie Towarzystwo Geopolityczne.

Grabowski Tomasz W., Lakomy Mirosław, Oświecimski Konrad. 2018. Bezpieczeństwo informacyjne w dobie postprawdy, Kraków : WAM

Кефели Игорь Федорович, Ипатов Олег Сергеевич, Левкин Игорь Михайлович. 2016. „Информационная геополитика на службе российского государства", Геополитика и безопасность Но. 2 (34): 25–34 [Kefeli Igor' Fedorovich, Ipatov Oleg Sergeevich, Levkin Igor' Mikhaylovich. 2016. „Informatsyonnaja geopolitika na sluzhbe rossijskogo gosudarstva", Geopolitika i bezopasnost' No. 2(34): 25-34].

Ištok Robert, Plavčanová Dominika. 2013. „Russian geopolitics and geopolitics of Russia: phenomenon of space". European Journal of Geopolitics Vol. 1: 61–94.

Janc Krzysztof. 2017. Geografia Internetu. Wrocław: Wydawnictwo I–BiS.

Kowalczyk Krzysztof A. 2019. „Geopolityczne dążenia współczesnej Rosji". Przegląd Geopolityczny nr 27: 78–92.

Kozłowski Andrzej. 2014. „Cyberwojownicy Kremla". Biuletyn OPINIE FAE nr 6: 1–11.

Kuczyńska-Zonik Anna. 2017. Strategia bezpieczeństwa informacyjnego Federacji Rosyjskiej. W J. Trubalska, Ł. Wojciechowski (red.) Bezpieczeństwo państwa w cyberprzestrzeni, 97–105. Lublin: Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji.

Kukułka Józef. 2006. Zaspokajanie potrzeb i rozwiązywanie konfliktów. W E. Haliżak, R. Kuźniar (red.), Stosunki międzynarodowe. Geneza, struktura, dynamika, 252-268. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.

Liderman Krzysztof, Malik Andrzej. 2013. „Polityka informacyjna a bezpieczeństwo informacyjne". Studia Bezpieczeństwa Narodowego t. 1 (4): 399–411.

Limonier Kevin. 2014. „La Russie dans le cyberespace : représentations et enjeux". Hérodote Vol 1-2 (152-153): 140–160.

Łuniewski Marcin. 2017. „Rosja szkoli cybernetyczną armię. Cyberżołnierze są na skinienie Kremla". Rzeczpospolita Plus-Minus 31.08.2017.

Меньшиков Петр Витальевич. 2017. „Эволюция государственной информационной политики в России". Журнал Международные коммуникации (4). W http://www.intcom-mgimo.ru/2017-04/state-information-policy-of-russia
[Men'shikov Petr Vital'evich. 2017. „Evolyutsiya gosudarstvennoj informatsionnoy polityki v Rossii". Zhurnal Mezhdunarodnye kommunikatsii (4). V http://www.intcom-mgimo.ru/2017-04/state-information-policy-of-russia].

Nieto Gómez Rodrigo. 2014. „Cybergéopolitique: de l'utilité des cybermenaces", Hérodote Vol. 1–2 (152–153): 98–122.

O'Hara Kieron, Hall Wendy. 2018. Four Internets: The Geopolitics of Digital Governance. CIGI Papers No. 206: 1–16.

Pigman Lincoln. 2019. „Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion". Journal of Cyber Policy Vol. 4 (1): 22–34.

Popa Julian F. 2014. Cyber Geopolitics And Sovereignty. An Introductory Overview. In Proceedings of the 5th International scientific conference „National and International Security", Armed Forces Academy of General Milan Rastislav Štefánik, 413-417. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2520421.

Potulski Jakub. 2010. „Rosja wyparta z Europy" – konsekwencje dla porządku międzynarodowego na progu XXI w." Środkowoeuropejskie Studia Polityczne nr 1: 97–110.

Potulski Jakub. 2010. Geopolityka w świecie ponowoczesnym. Częstochowa: Instytut Geopolityki.

Rosyjska wojna dezinformacyjna przeciwko Polsce. 2017. Warszawa: Fundacja Puławskiego.

Ristolainen Mari. 2017. „Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West". Journal of Information Warfare 16, 4 (Fall): 113–131.

Rukat Mariusz. 2017. Polityka informacyjna państw w domenie cyfrowej. Fundacja Bezpieczeństwa i Rozwoju Stratpoints. W http://www.stratpoints.eu/wp-content/uploads/2017/11/Polityka-Informacyjna-Pw-domenie-Cyfr_M_RUKAT_.pdf.

Świder Konrad. 2016. „Geopolityka jako światopogląd władzy w Rosji". Teka Komisji Politologii i Stosunków Międzynarodowych, 11 (3): 35–58.

Szynkiewicz Mariusz. 2014. „Metafora smogu informacyjnego a procesy informacyjne". Studia Metodologiczne nr 32: 65–77.

Trejnis Zenon, Trejnis Przemysław Z. 2017. „Polityka ochrony cyberprzestrzeni w państwie współczesnym". Studia Bobolanum t. 28 (3): 21–40.

Wendt Jan. 1999. Geopolityczne aspekty tranzytu w Europie Środkowej, Warszawa: IG i PZ PAN.

Wendt Jan. 2002. Problemy badań w geostrategii i geopolityce. W H. Rogacki (red.) Możliwości i ograniczenia zastosowań metod badawczych w geografii społeczno-ekonomicznej i gospodarce przestrzennej, 259–266. Poznań: Bogucki Wydawnictwo Naukowe.

Wendt Jan. 2010. Model dyfuzji innowacji i inne problemy badań w geopolityce i geostrategii. W Z. Lach, J. Wendt (red.) Geopolityka. Elementy teorii, wybrane metody i badania, 81-91. Częstochowa: Instytut Geopolityki.

Wojnowski Michał. 2017. „Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej". Przegląd Bezpieczeństwa Wewnętrznego t. 17 (9):11–37.

Woolley Samuel C., Howard Philip N. 2017. "Computational Propaganda Worldwide: Executive Summary". Working Paper no. 11. Oxford Internet Institute. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Zupančič Jernej, J.A. Wendt Jan A., Ilieş Alexandru. 2018. „An outline of border changes in the area between the Baltic and the Mediterranean: their geopolitical implications and classification". Geographia Polonica t. 91 (1): 33-46.