mgr Mikołaj KORGOL-SOWIŃSKI
Wojskowa Akademia Techniczna w Warszawie
u64599@student.wat.edu.pl
ORCID: 0009-0004-0598-8326

CYBERPRZESTRZEŃ JAKO DOMENA WALKI O SUWERENNOŚĆ IDEOLOGICZNĄ W DOKTRYNACH I USTAWODAWSTWIE FEDERACJI ROSYJSKIEJ

CYBERSPACE AS A DOMAIN OF STRUGGLE FOR IDEOLOGICAL SOVEREIGNTY IN THE DOCTRINES AND LEGISLATION OF THE RUSSIAN FEDERATION

Streszczenie

W niniejszym artykule dokonano analizy ewolucji roli cyberprzestrzeni w rosyjskiej myśli strategicznej, ze szczególnym uwzględnieniem koncepcji bezpieczeństwa informacyjnego. W przeciwieństwie do zachodnich definicji cyberbezpieczeństwa, koncentrujących się głównie na ochronie infrastruktury technicznej, rosyjskie podejście, wyrażone m.in. w doktrynie bezpieczeństwa informacyjnego z 2016 r., integruje aspekty techniczne z informacyjno-psychologicznymi. Autor stawia tezę, że dla Federacji Rosyjskiej cyberprzestrzeń jest kluczową domeną walki o suwerenność państwową oraz narzędziem przeciwdziałania zagrożeniom dla stabilności ustrojowej i kulturowej. W pracy omówiono procesy legislacyjne, takie jak ustawa o „suwerennym internecie", oraz metody wykorzystywania technologii cyfrowych do prowadzenia operacji hybrydowych. Przeprowadzona analiza wykazuje, iż rosyjska percepcja cyberprzestrzeni osadzona jest w paradygmacie wojny informacyjnej, co wymusza dążenie do autarkii technologicznej i systemowego uszczelniania kontroli nad krajowym obiegiem danych.

Słowa kluczowe: cyberprzestrzeń, Federacja Rosyjska, wojna hybrydowa, bezpieczeństwo informacyjne

Abstract

This article analyzes the evolution of the role of cyberspace in Russian strategic thought, with a particular focus on the concept of information security. In contrast to Western definitions of cybersecurity, which primarily concentrate on the protection of technical infrastructure, the Russian approach—as expressed, inter alia, in the 2016 Information Security Doctrine—integrates technical aspects with information-psychological ones. The author posits that for the Russian Federation, cyberspace is a key domain in the struggle for state sovereignty and a tool for countering threats to constitutional and

cultural stability. The paper discusses legislative processes, such as the „sovereign internet" law, and methods of utilizing digital technologies to conduct hybrid operations. The conducted analysis demonstrates that the Russian perception of cyberspace is embedded in the information warfare paradigm, which necessitates a drive toward technological autarky and the systematic tightening of control over the national flow of data.

Keywords: cyberspace, Russian Federation, hybrid warfare, information security

Wprowadzenie

Ewolucja globalnej przestrzeni cyfrowej w XXI wieku wymusiła na podmiotach państwowych redefinicję tradycyjnych paradygmatów obronności. W zachodniej myśli strategicznej nadal jednak dominuje technocentryczne ujęcie cyberbezpieczeństwa, koncentrujące się na odporności sieci, kryptografii oraz ochronie zasobów informacyjnych przed nieuprawnioną ingerencją[1]. Tymczasem Federacja Rosyjska wypracowała unikalne, dualistyczne podejście, które fundamentalnie odbiega od standardów euroatlantyckich. Rosyjska myśl wojskowa i polityczna nie uznaje dychotomii między warstwą techniczną a treściową; zamiast tego integruje je w ramach nadrzędnego pojęcia bezpieczeństwa informacyjnego. W tym modelu ochrona procesora i kodu jest nierozerwalnie związana z ochroną ludzkiej psychiki przed wrogą ideologią, co czyni cyberprzestrzeń domeną o charakterze totalnym, gdzie technologia służy jedynie jako medium dla głębszej rywalizacji o charakterze socjopsychologicznym.

Fundamentem rosyjskiego postrzegania cyberprzestrzeni jest przekonanie, że nie stanowi ona neutralnego środowiska wymiany danych, lecz jest kluczowym polem bitwy o suwerenność informacyjną. Dla decydentów na Kremlu kontrola nad sferą idei w internecie jest równie istotna, co fizyczna kontrola nad terytorium państwa. W tej optyce informacja jest traktowana jako specyficzny rodzaj oręża, zdolnego do destabilizacji nastrojów społecznych, erozji tradycyjnych wartości oraz podważania autorytetu władzy państwowej. To sprawia, że rosyjska aktywność w sieci – od operacji hakerskich po kampanie dezinformacyjne – nie jest zbiorem odizolowanych incydentów, lecz spójnym elementem strategii geopolitycznej, nakierowanej na zabezpieczenie własnej strefy wpływów oraz projekcję siły w skali globalnej. Swobodny przepływ informacji, definiowany na Zachodzie jako fundament demokracji, w rosyjskiej doktrynie figuruje często jako narzędzie „wojny informacyjnej", wymierzonej w bezpieczeństwo narodowe (Budzisz, 2021).

1 Przykładem takich działań jest projekt „Cyber Shield 2025", który zakłada stworzenie wspólnego systemu szybkiego reagowania na cyberataki z centralnym centrum dowodzenia, automatyczną analizą zagrożeń i wsparciem AI. Zob. więcej: S. Hircock, *Cyber Shield 2025*, [dostęp 31.01.2026] https://www.army.mil/article/286378/cyber_shield_2025

Pełne zrozumienie specyfiki tego podejścia wymaga rzetelnej analizy dokumentów strategicznych, które na przestrzeni ostatnich dwóch dekad krystalizowały rosyjską myśl obronną. Szczególne znaczenie mają tutaj Doktryny Bezpieczeństwa Informacyjnego z 2000 oraz 2016 roku. Pierwsza z nich, ogłoszona u progu prezydentury Władimira Putina, stanowiła reakcję na technologiczne zacofanie kraju i rodzące się zagrożenia ery globalizacji. Druga, z roku 2016, jest już dokumentem dojrzałym, odzwierciedlającym konfrontacyjny kurs w relacjach z Zachodem oraz adaptację państwa do realiów wojny hybrydowej. Porównanie tych aktów pozwala nie tylko zidentyfikować ewolucję katalogu zagrożeń postrzeganych przez Moskwę, ale także ukazuje proces instytucjonalizacji kontroli nad przestrzenią cyfrową jako nieodzowny element utrzymania stabilności politycznej Federacji Rosyjskiej w warunkach permanentnego konfliktu informacyjnego.

Specyfika rosyjskiej siatki pojęciowej w sferze walki informacyjnej

Aby zdefiniować pojęcie bezpieczeństwa informacyjnego w kontekście Rosji, istnieje potrzeba wskazania kluczowego terminu, którym posługuje się Rosja, tj. bezpieczeństwo informacji (*informacionnaja biezopasnost'*) vs zachodnie bezpieczeństwo teleinformatyczne (*cybersecurity*). Rosja celowo unika przedrostka „cyber", ponieważ sugeruje on tylko technikę, a „informacja" obejmuje też treść (ideologię). Jak podkreśla J. Darczewska, rosyjska koncepcja prowadzenia zmagań w sferze informacji opiera się na specyficznej siatce pojęciowej, która znacząco odbiega od standardów przyjętych w państwach zachodnich. W przeciwieństwie do USA czy Europy, Rosja nie rozgranicza technologicznego i społecznego wymiaru współczesnych konfliktów. Tamtejsze definicje „cyberwalki" czy „walki sieciowej" w sposób celowy zacierają różnice między sferą militarną a cywilną oraz między infrastrukturą techniczną a oddziaływaniem na świadomość odbiorców. Podczas gdy kraje Zachodu postrzegają walkę informacyjną głównie przez pryzmat wykorzystania narzędzi informatycznych w celach wojskowych i wywiadowczych, podejście rosyjskie traktuje te obszary jako nierozerwalną całość. Zaktualizowane założenia polityki Kremla potwierdzają, że Rosja odrzuca zachodni model ochrony praw człowieka w sieci na rzecz pełnej suwerenizacji przestrzeni cyfrowej. Głównym celem jest tutaj wprowadzenie państwowej kontroli nad przepływem danych i przekazem medialnym, co ma chronić reżim przed wpływem niezależnych treści[2]. W 2019 r. badacze z Ośrodka Studiów Wschodnich zauważyli, że: w warunkach stagnacji gospodarczej, zachodnich sankcji ekonomicznych oraz pogarszającej się sytuacji materialnej obywateli i spadającego poparcia społecznego dla władz Kreml – w obawie przed wybuchem protestów społecznych

2 J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej, Operacja krymska – studium przypadku*, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2014, s. 11–12.

na znacznie większą niż dotąd skalę – będzie próbował udoskonalać mechanizmy prewencji i represji. Podobnie jak wiele innych ustaw przepisy o „suwerennym Runecie" mogą długo pozostać „uśpione", zwłaszcza jeśli sytuacja polityczna pozostanie stabilna. Należy jednak zakładać, że testy z zakresu udoskonalania mechanizmów blokad oraz filtrowania zawartości stron internetowych i korespondencji elektronicznej będą w najbliższych latach kontynuowane[3].

Rosyjska doktryna różni się od podejścia NATO również w kwestii klasyfikacji teatru działań. Podczas gdy Sojusz Północnoatlantycki od 2016 r. uznaje cyberprzestrzeń za odrębny i samodzielny obszar prowadzenia wojen – obok lądu, morza, powietrza i kosmosu – Rosja unika takiego podziału. Zamiast tego posługuje się szerokim terminem „przestrzeń informacyjna". W tym modelu narzędzia cyfrowe nie stanowią osobnej dziedziny, lecz są nowoczesnym instrumentem służącym do prowadzenia kompleksowej wojny informacyjnej. Obejmuje ona zarówno szpiegostwo i dezinformację, jak i walkę elektroniczną, destabilizację psychologiczną czy fizyczne niszczenie systemów informatycznych wroga. W rosyjskiej narracji operacje w sieci są przedstawiane przede wszystkim jako działania o charakterze obronnym. Sama walka informacyjna jest tam rozumiana jako element szerokiej rywalizacji cywilizacyjnej, mającej na celu wpływanie na nastroje i świadomość masową. Co istotne, rosyjska strategia nie ogranicza się do celów militarnych – obiektem ataków hakerskich oraz działań dezinformacyjnych (prowadzonych m.in. przez tzw. trolle) staje się cała struktura państwa, od administracji i gospodarki, aż po świat nauki i kultury[4].

W obliczu globalnego wzrostu tendencji autorytarnych rosyjska wizja kontrolowanego Internetu zyskuje zwolenników w ONZ oraz organizacjach regionalnych, głównie wśród państw azjatyckich i afrykańskich. Choć Moskwie nie udało się jeszcze przeforsować wiążącej konwencji międzynarodowej, konsekwentnie buduje ona koalicję państw dążących do zwiększenia odgórnych regulacji[5]. Rosja traktuje sferę informacyjną jako pełnoprawne pole bitwy, na którym może dojść do regularnego konfliktu międzypaństwowego. Mimo oficjalnych deklaracji o chęci utrzymania pokoju, Moskwa stale rozwija potencjał technologiczny do celów polityczno-militarnych, czego dowodem są trwające od 2014 r. operacje hybrydowe przeciwko Ukrainie oraz próby destabilizacji państw Unii Europejskiej. Działania te, wymierzone w zaufanie obywateli do własnych rządów, nabierają szczególnego znaczenia w okresach

3 M. Domańska, *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu,* Komentarze OSW 2019, [dostęp 31.01.2026]. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2019-12-04/zakneblowac-runet-uciszyc-spoleczenstwo-kremlowskie-ambicjech

4 A. Kozłowski, *Cyberwojownicy Kremla*, „Biuletyn OPINIE FAE", 6/2014, s. 2-3, [dostęp 15.01.2026] https://www.researchgate.net/publication/345906006_Cyberwojownicy_Kremla/link/5fb17d0545851518fda9b7a0/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

5 Władimir Putin przypomniał, że „Rosja była jednym z pierwszych państw, które zaapelowały do społeczności globalnej o połączenie sił i współpracę w nowym obszarze cywilizacji, kiedy w 1998 r. z jej inicjatywy przyjęto stosowną rezolucję Zgromadzenia Ogólnego ONZ. W istocie był to apel o jak najszerszą współpracę w zwalczaniu wspólnych zagrożeń w sferze informacyjnej, przede wszystkim prób wykorzystywania najnowszych technologii ze szkodą dla międzynarodowego pokoju i stabilności" – stwierdził prezydent. „Co więcej, to w dużej mierze dzięki naszym wysiłkom temat bezpieczeństwa informacyjnego na stałe zagościł w agendzie Zgromadzenia Ogólnego ONZ, a przyjęcie stosownej rezolucji stało się wydarzeniem corocznym" – podkreśliła głowa państwa. Polowninko A., *Internet zamieniat sriedoj oborota dostowiernoj informacyi* „Novaja Gazieta", wyd. 6.07.2021, [dostęp: 08.02.2026] https://novayagazeta.ru/articles/2021/07/06/internet-zameniat-sredoi-oborota-dostovernoi-informatsii

wyborczych. Dla państw, takich jak Polska, perspektywa fragmentacji globalnej sieci jest wyzwaniem, gdyż utrudnia kontakt ze społeczeństwami na Wschodzie.

Powyższa analiza wskazuje, że podejście Rosjan do istoty samej walki informacyjnej wyraża się w posiadaniu odmiennego od „zachodniego" zakresu pojęciowego zjawisk takich jak „cyberwalka", „walka informacyjna" czy „walka sieciowa". Brak w nim przeciwstawienia technologicznego i społecznego wymiaru konfliktów XXI wieku. Rosyjskie definicje mieszają porządek militarny z pozamilitarnym, a technologiczny (cyberprzestrzeń) ze społecznym (przestrzeń informacyjna). Stany Zjednoczone i Europa Zachodnia w podejściu do walki informacyjnej koncentrują się przede wszystkim na militarnym i wywiadowczym zastosowaniu technologii informatycznych. Należy zauważyć, że rosyjska interpretacja bezpieczeństwa informacyjnego ma charakter totalny. Podczas gdy dokumenty NATO (np. Strategia Cyberbezpieczeństwa) skupiają się na odporności systemów, rosyjska Doktryna Bezpieczeństwa Informacyjnego kładzie nacisk na suwerenność duchowo-moralną i ochronę przed destrukcyjnym wpływem ideologicznym.

Legislacyjne podstawy kontroli rosyjskiej cyberprzestrzeni (2012–2019)

Władze na Kremlu tworzą podwaliny pod ograniczanie swobody korzystania z Internetu już od kilkudziesięciu lat. W 2012 r. znowelizowano Ustawę o informacji, technologiach informacyjnych i ochronie informacji. Nowe przepisy wyposażyły Roskomnadzor w narzędzia do natychmiastowego blokowania witryn szerzących pornografię dziecięcą, narkotyki czy namawiających do samobójstw – bez czekania na decyzję sądu. W efekcie stworzono rejestr stron zakazanych, które dostawcy Internetu muszą odcinać od sieci. Nieco inaczej wygląda procedura w przypadku treści ekstremistycznych: tutaj wpisanie na „czarną listę" wciąż wymaga uzyskania oficjalnego wyroku. Z kolei w 2013 r. znowelizowano Ustawę o ochronie dzieci przed szkodliwymi informacjami. Nowelizacja prawa nie tylko zakazała szerzenia treści dotyczących mniejszości seksualnych wśród młodzieży, ale też zwiększyła ochronę prawną uczuć religijnych. Działania te służyły legitymizacji rządowej narracji, która systemowo piętnowała zachodnie wzorce kulturowe jako formę dekadencji, przeciwstawiając im model konserwatywnego społeczeństwa rosyjskiego. W tym samym roku ponownie znowelizowano Ustawę o informacji, technologiach informacyjnych i ochronie informacji (tzw. ustawa Ługowoja). Nowe prawo umożliwiło Roskomnadzorowi wpisywanie witryn na „czarną listę" bez wyroku sądu, jeśli Prokuratura Generalna uzna, że nawołują one do ekstremizmu lub zamieszek. Ze względu na nieprecyzyjne definicje ustawowe, narzędzie to stało się de facto instrumentem cenzury politycznej, pozwalającym eliminować treści krytyczne wobec Kremla. Mechanizm

ten jest szczególnie dotkliwy dla niezależnych portali, które mogą zostać zablokowane za pojedyncze komentarze czytelników, bez analizy intencji autora czy kontekstu publikacji. Skalę zjawiska obrazują dane z 2017 r. – w ciągu pięciu lat funkcjonowania systemu zablokowano aż 275 tysięcy adresów. Nie był to koniec prac nad omawianą ustawą[6].

W 2014 r. państwo uderzyło w niezależnych twórców internetowych, nakładając na najpopularniejszych z nich surowe restrykcje. Blogerzy z zasięgami przekraczającymi 3 tys. wizyt na dobę musieli ujawnić swoje dane osobowe i przestrzegać rygorów typowych dla redakcji prasowych. Mimo że ustawa ta funkcjonowała głównie w teorii, jako tzw. „martwe prawo", oficjalnie wykreślono ją z porządku prawnego dopiero latem 2017 roku. W tym samym roku na mocy nowelizacji kodeksu karnego rozszerzono katalog czynów zabronionych o nawoływanie do działań ekstremistycznych w sieci. Za publikowanie tego typu treści w Internecie wprowadzono sankcję karną, przewidującą nawet do pięciu lat więzienia. Z kolei wprowadzona 21 lipca 2014 roku ustawa o „lokalizacji danych" wymusiła na podmiotach prawnych gromadzenie i przetwarzanie danych rosyjskich obywateli na serwerach znajdujących się fizycznie w granicach Federacji Rosyjskiej. Regulacja ta miała na celu zagwarantowanie służbom specjalnym bezpośredniego wglądu w informacje o użytkownikach oraz uderzyła w podmioty niezależne, drastycznie ograniczając im możliwość korzystania z bezpiecznej infrastruktury zagranicznej. Przyjęta w październiku 2014 r. nowelizacja prawa prasowego drastycznie ograniczyła wpływy zagraniczne na rosyjskim rynku medialnym, wyznaczając limit obcego kapitału na poziomie 20%. Przepisy te wprost zakazały obcokrajowcom posiadania statusu założyciela mediów, co w praktyce miało doprowadzić do marginalizacji lub przejęcia redakcji krytycznych wobec władzy przez lojalne wobec Kremla podmioty. Wydawcy otrzymali wtedy czas do lutego 2017 r. na przeprowadzenie przymusowej restrukturyzacji i dostosowanie struktury udziałów do nowych restrykcji. Przyjęty 6 lipca 2016 r. pakiet ustaw antyterrorystycznych, znany jako „pakiet Jarowej", wprowadził bezprecedensowe wymogi dla sektora telekomunikacyjnego. Operatorzy oraz dostawcy usług internetowych zostali zobligowani do archiwizowania pełnej treści komunikacji użytkowników – w tym nagrań rozmów, SMS-ów oraz plików multimedialnych – przez pół roku. Co więcej, przepisy nakazały udostępnianie tych danych służbom specjalnym z pominięciem drogi sądowej oraz przekazywanie FSB kluczy szyfrujących, co w praktyce miało umożliwić dekodowanie prywatnych wiadomości w komunikatorach. Latem 2017 r. rosyjskie władze postanowiły uszczelnić system blokad internetowych, delegalizując używanie technologii pozwalających na ukrycie tożsamości lub obejście

6 M. Domańska, *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu*, Komentarze OSW 2019, [dostęp 31.01.2026]. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2019-12-04/zakneblowac-runet-uciszyc-spoleczenstwo-kremlowskie-ambicje

restrykcji. Nowe prawo zmusiło operatorów usług, takich jak VPN czy TOR[7], do współpracy z cenzorem – pod groźbą własnej blokady musieli oni odcinać internautom drogę do serwisów wpisanych na czarną listę. Był to decydujący krok w stronę odizolowania rosyjskiego segmentu sieci od niezależnych źródeł informacji[8].

Kluczowym etapem było wprowadzenie w 2017 r. przepisów znoszących anonimowość użytkowników komunikatorów internetowych, co od stycznia 2018 r. wymusiło obowiązek rejestracji przy użyciu numeru telefonu. Równocześnie rozszerzono definicję „agenta zagranicznego" na media działające w Rosji oraz przyznano władzom prawo do blokowania bez wyroku sądu stron „organizacji niepożądanych", czyli podmiotów uznanych za zagrażające bezpieczeństwu lub ustrojowi państwa. Kolejne zaostrzenie cenzury nastąpiło w marcu 2019 r. wraz z przyjęciem pakietu ustaw uderzających w swobodę wypowiedzi. Wprowadzono wówczas zakaz rozpowszechniania tzw. fake newsów, które mogłyby zagrozić porządkowi publicznemu, oraz surowe kary za treści wyrażające brak szacunku wobec państwa, jego symboli, konstytucji czy organów władzy. Ze względu na bardzo nieprecyzyjne definicje tych wykroczeń, przepisy te stały się narzędziem do karania niemal każdej formy krytyki rządu oraz blokowania kompromitujących informacji pochodzących z nieoficjalnych źródeł. Dopełnieniem tej architektury kontroli stała się ustawa o „suwerennym Internecie" z maja 2019 r. Jej oficjalnym celem było zabezpieczenie rosyjskiego segmentu sieci (Runetu) przed zagrożeniami zewnętrznymi i ewentualnym odcięciem od zagranicznych serwerów. W praktyce jednak ustawa ta stworzyła fundamenty pod scentralizowany system zarządzania ruchem internetowym, dając państwu pełną kontrolę nad punktami wymiany danych i transgranicznym przesyłem informacji[9]. Proces opisywany w ustawach z lat 2012–2019 znalazł swoje apogeum po lutym 2022 r. Wtedy „suwerenny Internet" przestał być teorią, a stał się narzędziem całkowitego odcięcia zachodnich mediów społecznościowych, co zostało opisane w kolejnym rozdziale pracy.

Ewolucja dokumentów strategicznych

Analiza rosyjskiej aktywności w sferze cyfrowej wymaga szczegółowego spojrzenia na proces kształtowania się ram doktrynalnych, które legitymizują działania Moskwy na arenie międzynarodowej. Ewolucja dokumentów strategicznych Federacji Rosyjskiej w obszarze bezpieczeństwa informacyjnego nie jest jedynie procesem technologicznym, lecz przede wszystkim odzwierciedleniem zmieniającej się filozofii

7 Tor (The Onion Router) – zdecentralizowana sieć anonimizująca, która kieruje ruch przez losowe węzły, szyfrując go warstwowo, aby ukryć adres IP i tożsamość użytkownika. Używany do przeglądania internetu z wysoką prywatnością, omijania cenzury i dostępu do sieci Tor (darknet), działa jako bezpłatne oprogramowanie typu open-source.

8 M. Domańska, op. cit. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2019-12-04/zakneblowac-runet-uciszyc-spoleczenstwo-kremlowskie-ambicje

9 Ibidem.

politycznej Kremla. Na przestrzeni ostatnich dekad rosyjska myśl strategiczna przeszła wyraźną transformację: od prób adaptacji do globalnych standardów sieciowych, aż po wypracowanie unikalnej, autorytarnej koncepcji „suwerenności cyfrowej".

Doktryna Bezpieczeństwa Informacyjnego Federacji Rosyjskiej z 2000 roku

Pierwsze próby uregulowania sfery cyberprzestrzeni po rozpadzie ZSRR zostały zawarte w Doktrynie Bezpieczeństwa Informacyjnego z 2000 r. Powstawała ona w specyficznym momencie dziejowym – w okresie gwałtownego nadrabiania przez Rosję dystansu technologicznego względem Zachodu oraz rosnącej świadomości znaczenia Internetu w procesach politycznych. Już na wstępie dokumentu bezpieczeństwo informacyjne zostało zdefiniowane jako stan ochrony interesów narodowych w sferze informacyjnej, na które składa się równowaga interesów jednostki, społeczeństwa oraz państwa. Kluczowym wyróżnikiem tej doktryny, odróżniającym ją od zachodnich strategii w sferze IT, było przyjęcie szerokiej definicji „sfery informacyjnej". Rosja włączyła w jej skład nie tylko infrastrukturę telekomunikacyjną i systemy komputerowe, ale także same zasoby informacyjne oraz – co najistotniejsze – systemy formowania opinii publicznej. W analizowanym dokumencie, pojęcie, które na Zachodzie utożsamiano by z „cyberbezpieczeństwem", zostało rozbite na dwa komplementarne wektory. Zrozumienie tego podziału jest kluczowe dla interpretacji rosyjskiej myśli strategicznej:

1. wektor techniczno-technologiczny – obejmuje on ochronę fizycznej infrastruktury, zapewnienie integralności systemów dowodzenia i kontroli oraz przeciwdziałanie szpiegostwu technologicznemu. Doktryna wskazuje tutaj na zagrożenie wynikające z dominacji zagranicznych producentów oprogramowania i sprzętu, co interpretowano jako potencjalne źródło „tylnych furtek" i podatności na zewnętrzny sabotaż.
2. wektor informacyjno-psychologiczny – to tutaj doktryna wprowadza najbardziej innowacyjne i kontrowersyjne zapisy. Cyberprzestrzeń jest traktowana jako kanał przesyłowy dla treści, które mogą „deformować system wartości" obywateli. Bezpieczeństwo informacyjne w tym ujęciu to ochrona „duchowej i moralnej sfery życia społecznego" przed obcymi wpływami kulturowymi i dezinformacją.

Doktryna z 2000 r. systematyzuje zagrożenia w czterech głównych grupach, przy czym w każdej z nich aspekty techniczne przeplatają się z politycznymi:

- Zagrożenia dla konstytucyjnych praw i wolności – paradoksalnie, choć dokument mówi o ochronie wolności słowa, kładzie jednocześnie nacisk na zwal-

czanie „manipulacji informacją", co w praktyce otworzyło drogę do reglamentacji treści w sieci;
- Zagrożenia dla polityki państwowej – obejmują one utrudnianie dostępu do oficjalnych informacji państwowych oraz „dyskredytację" organów władzy poprzez kampanie dezinformacyjne prowadzone w sieciach cyfrowych;
- Zagrożenia dla rozwoju przemysłu i nauki – wskazano tu na niebezpieczeństwo drenażu mózgów oraz kradzieży własności intelektualnej drogą elektroniczną, co uderza w suwerenność technologiczną kraju;
- Zagrożenia dla systemów bezpieczeństwa narodowego – najbardziej techniczny aspekt, dotyczący ataków na systemy łączności wojskowej i infrastrukturę krytyczną (np. energetykę).

Istotnym elementem Doktryny z 2000 r. jest postulat autarkii technologicznej. Dokument wprost wskazuje, że poleganie na technologiach importowanych z Zachodu jest systemową słabością Federacji Rosyjskiej. Cyberbezpieczeństwo jest tu zatem rozumiane nie tylko jako „odporność sieci", ale także jako niezależność od zagranicznego łańcucha dostaw. W tym celu wprowadzono postulat certyfikacji zagranicznego sprzętu i oprogramowania oraz stymulowania rodzimej produkcji mikroelektroniki. Był to wczesny etap koncepcji „suwerennego internetu" (Runetu), która w pełni zmaterializowała się dopiero dwie dekady później. W przeciwieństwie do modeli liberalnych, gdzie cyberbezpieczeństwo jest często domeną współpracy sektora prywatnego z publicznym, Doktryna z 2000 r. nadaje państwu rolę hegemona i jedynego gwaranta bezpieczeństwa. Dokument dopuszcza szerokie uprawnienia służb specjalnych w zakresie monitorowania ruchu sieciowego w celu wykrywania „zagrożeń informacyjnych". Warto zauważyć, że dokument ten antycypował militaryzację cyberprzestrzeni. Sugerował, że granica między czasem pokoju a czasem wojny w sferze informacyjnej jest płynna, a ataki na sferę psychologiczną obywateli mogą być traktowane jako akt agresji równoważny z atakiem kinetycznym[10].

Doktryna Bezpieczeństwa Informacyjnego z 2000 r. nie była jedynie technicznym podręcznikiem ochrony danych. Był to manifest polityczny, który zdefiniował informację jako zasób strategiczny podlegający ścisłej kontroli państwowej. Poprzez zatarcie różnic między ochroną infrastruktury (cyberbezpieczeństwem technicznym), a ochroną przekazu (bezpieczeństwem psychologicznym), Rosja stworzyła teoretyczne ramy dla późniejszych działań w zakresie cenzury Internetu, operacji wpływu oraz budowy izolowanych systemów cyfrowych. Z perspektywy historycznej dokument ten był „protokołem rozbieżności" między rosyjskim a zachodnim rozumieniem wolności w cyberprzestrzeni.

10 Opracowano na podstawie: *Federal'nyj zakon ot 27.07.2006 N 149-FZ „Ob informacii, informacionnyh tehnologijah i o zascite informacii"* [w:] *System Informacji Prawnej Garant*, [dostęp: 08.02.2026] https://base.garant.ru/182535/

Doktryna Bezpieczeństwa Informacyjnego Federacji Rosyjskiej z 2016 roku

Doktryna z 2016 r., podpisana w atmosferze napięć po aneksji Krymu i w obliczu oskarżeń o ingerencję w wybory w USA, znacząco zredefiniowała środowisko międzynarodowe. O ile dokument z 2000 r. kładł nacisk na rozwój technologiczny, o tyle wersja z 2016 r. postrzega przestrzeń informacyjną jako obszar permanentnej rywalizacji geopolitycznej.

W tekście Doktryny pojawia się silne przekonanie o narastaniu agresywnych działań ze strony obcych państw, co prowadzi do ostatecznego zatarcia granicy między stanem pokoju a stanem wojny. Cyberbezpieczeństwo przestaje być kwestią administracyjną, a staje się integralnym elementem strategii militarnej i kontrwywiadowczej. Za pomocą dokumentu pojęcie suwerenności w sieci zostaje wyniesione do rangi absolutnego priorytetu. Doktryna wprost wskazuje na dążenie niektórych państw do „dominacji technologicznej" i wykorzystywania IT do ingerencji w sprawy wewnętrzne Rosji. W odpowiedzi na te zagrożenia, dokument legitymizuje budowę „Suwerennego Internetu" (Runetu). Cyberbezpieczeństwo techniczne zostaje tu utożsamione z możliwością autonomicznego funkcjonowania rosyjskiego segmentu sieci w przypadku odcięcia go od globalnych węzłów. To ewolucja od postulatu „korzystania z własnego sprzętu" (2000 r.) do „tworzenia własnej, niezależnej infrastruktury zarządzania siecią" (2016 r.). Dokument z 2016 r. jeszcze mocniej akcentuje zagrożenia o charakterze informacyjno-psychologicznym, wprowadzając pojęcia takie jak destabilizacja polityczna i społeczna, czyli wykorzystywanie technologii informacyjnych do wzniecania „kolorowych rewolucji" oraz promowania ideologii ekstremistycznych i terrorystycznych, a także erozja wartości kulturowych – w tym przypadku ataki na „tradycyjne rosyjskie wartości duchowo-moralne" są tu traktowane na równi z atakami na systemy bankowe czy energetyczne. W tym ujęciu cyberbezpieczeństwo to nie tylko ochrona przed wirusami, ale przede wszystkim przed „wirusami ideologicznymi". Doktryna legitymizuje tym samym systemową cenzurę oraz monitoring mediów społecznościowych jako działania o charakterze obronnym.

Zaktualizowany dokument kładzie nacisk na rozwój sił i środków wojny informacyjnej. Rosja otwarcie przyznaje, że musi posiadać potencjał do prowadzenia operacji w cyberprzestrzeni w celu powstrzymywania potencjalnych agresorów. Jednocześnie dokument wprowadza dualizm w polityce zagranicznej. Na zewnątrz Rosja promuje na forum ONZ koncepcję „międzynarodowego bezpieczeństwa informacyjnego", opartego na suwerenności państw (w opozycji do zachodniego modelu wol-

nego internetu). Z kolei wewnątrz buduje system totalnej kontroli przepływu danych i identyfikacji użytkowników[11].

Przejście od Doktryny z 2000 r. do tej z 2016 r. ukazuje proces sekurytyzacji informacji. To, co na początku wieku było próbą uporządkowania sfery cyfrowej, stało się fundamentem pod budowę cyfrowego autorytaryzmu. Rosja skutecznie skonsolidowała techniczne aspekty cyberbezpieczeństwa z kontrolą treści, tworząc model, w którym stabilność polityczna reżimu jest tożsama z bezpieczeństwem informacyjnym państwa.

Strategia rozwoju społeczeństwa informacyjnego w Federacji Rosyjskiej na lata 2017–2030

Kolejnym istotnym dokumentem strategicznym Federacji Rosyjskiej, kluczowym dla obszaru bezpieczeństwa, jest strategia rozwoju społeczeństwa informacyjnego na lata 2017–2030. W jej części ogólnej sformułowano metody realizacji polityki wewnętrznej i zagranicznej w zakresie technologii informacyjno-komunikacyjnych, które mają służyć budowie społeczeństwa informacyjnego oraz krajowego sektora cyfrowego. Do fundamentów tej strategii zaliczono między innymi gwarancję dostępu do informacji, swobodę w wyborze metod ich pozyskiwania oraz nadrzędność tradycyjnych rosyjskich wartości duchowych i moralnych. Zasady te mają być respektowane przez obywateli podczas korzystania z nowoczesnych narzędzi komunikacji, przy jednoczesnym zapewnieniu przez państwo ochrony interesów narodowych oraz zgodności z prawem procesów gromadzenia i dystrybucji danych.

Deklarowanym celem Rosji jest przeciwdziałanie militarnemu wykorzystaniu Internetu. Należy jednak zauważyć, że mimo oficjalnych haseł o wolności dostępu do wiedzy, dokument ten w praktyce sankcjonuje mechanizmy państwowej kontroli nad obiegiem informacji. Strategia identyfikuje szereg zagrożeń wynikających z postępu technologicznego, które uderzają w bezpieczeństwo rosyjskiej infrastruktury krytycznej, zwłaszcza poprzez uzależnienie od zagranicznych rozwiązań technicznych. Utrudnia to ochronę interesów państwowych i obywatelskich. Wskazać należy także problem niskiej jakości treści w sieci, co uznaje się za zagrożenie, gdyż obywatele mogą ulegać narracjom narzucanym przez państwa i podmioty będące właścicielami technologii przesyłu danych. Eliminacja tych ryzyk ma nastąpić poprzez aktywne kształtowanie przestrzeni informacyjnej zgodnie z potrzebami społeczeństwa w zakresie wiarygodnych informacji, rozwój własnej infrastruktury komunikacyjnej oraz budowę konkurencyjnych, rosyjskich technologii. Strategia zakłada stworzenie nowej bazy technologicznej dla gospodarki i ochronę interesów

11 Opracowano na podstawie: *Doktrina informacionnoj biezopasnosti Riedieracyi*, utwierżdena Priezidientom Rossijskoj Fiedieracyi 5 sientiabria 2000 g. № PR-1895, [w:] Oficjalna strona Rady Bezpieczeństwa Federacji Rosyjskiej, [dostęp: 08.02.2026] http://www.scrf.gov.ru/security/information/document5/

narodowych w sferze cyfrowej. W wymiarze prawnym dokument dąży do uszczelnienia kontroli nad dystrybucją treści w Internecie oraz systematycznego zastępowania zagranicznych rozwiązań rodzimymi odpowiednikami. Całość składa się na wizję suwerenności cyfrowej, opartą na państwowym nadzorze nad informacjami i odcięciu się od zewnętrznych wpływów. Wśród narzędzi kształtujących tę przestrzeń wymieniono popularyzację języka rosyjskiego, wspieranie narodowej kultury, nauki oraz tradycyjnych form przekazywania wiedzy[12].

Jak wykazuje powyższa analiza, państwowa aktywność w zwalczaniu obcych wpływów zyskuje solidne podstawy prawne, w tym zapisy o doskonaleniu metod blokowania i usuwania treści zakazanych przez rosyjskie prawo federalne. Omawiana strategia wprost przewiduje możliwość sterowania zasobami Internetu poprzez faworyzowanie informacji pochodzenia rosyjskiego, ograniczanie źródeł zewnętrznych oraz promowanie tradycyjnych mediów, takich jak radio czy prasa. Szczególnie niepokojącym elementem, rzutującym na bezpieczeństwo międzynarodowe, jest przyznanie Rosji prawa do ingerencji w sprawy innych państw pod pozorem ochrony mniejszości rosyjskojęzycznej, co obejmuje nie tylko własnych obywateli za granicą, ale też osoby posługujące się językiem rosyjskim niezależnie od ich obywatelstwa. W myśl zapisu dokumentu, infrastruktura informacyjna ma podlegać scentralizowanemu monitoringowi i zarządzaniu. Celem w tym przypadku jest wyraźne dążenie do pełnej substytucji technologii zagranicznych rosyjskimi produktami może w efekcie doprowadzić do całkowitego nadzoru nad aktywnością społeczeństwa w sieci. Co więcej, dokument rezerwuje dla państwa prawo do dowolnego kształtowania polityki informacyjnej i ekonomicznej w rosyjskim segmencie Internetu oraz prowadzenia działań kontrujących militarne wykorzystanie sieci. Oznacza to, że strategia ta de facto wspiera prowadzenie wojny informacyjnej w obu wymiarach: obronnym i zaczepnym. Dokument sytuuje Rosję w roli lidera rynków informacyjnych i wprowadza regulacje dyskryminujące zagraniczne podmioty technologiczne[13].

Strategię tę należy interpretować jako reakcję na zmiany w globalnym środowisku bezpieczeństwa. Analiza wykazuje, że priorytetem Moskwy jest przejęcie pełnej kontroli nad przepływem informacji na własnym terytorium i uniezależnienie się od zewnętrznych ośrodków wpływu. Działania te sprowadzają się do upaństwowienia zasobów internetu oraz zamknięcia rynku dla podmiotów zagranicznych. W ramach zwalczania zdefiniowanych zagrożeń Rosja zamierza rygorystycznie nadzorować przestrzeń cyfrową, przypisując kluczową rolę w wojnie informacyjnej

12 Opracowano na podstawie: *Ukaz Priezidienta Rossijskoj Fiedieracyi ot 09.05.2017 g. № 203 „O Strategii razwitija informacionnogo obszczestwa w Rossijskoj Fiedieracyi na 2017–2030 gody"*, [dostęp: 08.02.2026] http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

13 K. Zapała, *Cele FR w zakresie bezpieczeństwa informacyjnego na podstawie zapisów rosyjskich dokumentów strategicznych*, Instytut Nowej Europy 2020, [dostęp: 08.02.2026], https://ine.org.pl/cele-fr-w-zakresie-bezpieczenstwa-informacyjnego-na-podstawie-zapisow-rosyjskich-dokumentow-strategicznych/

zarówno mediom tradycyjnym, jak i zorganizowanym kampaniom w mediach społecznościowych.

Ustawa o „suwerennym Internecie"

Ustawa o „suwerennym internecie" (*Zakon o suwieriennom intiernietie*), przyjęta w maju 2019 r. i wdrożona w listopadzie tego samego roku, stanowi punkt kulminacyjny wieloletniego procesu legislacyjnego i ideologicznego. Warto zauważyć, że zgodnie z oficjalnym ustawodawstwem, wspomniana ustawa jest swego rodzaju rozbudowaniem opisywanej w pierwszej części artykułu Ustawy informacji, technologiach informacyjnych i ochronie informacji. Nie jest ona jedynie odpowiedzią na doraźne wyzwania technologiczne, lecz stanowi praktyczną implementację wizji świata zawartej w omówionych powyżej fundamentalnych dokumentach strategicznych Federacji Rosyjskiej. Najważniejszym novum wprowadzonym przez ustawę z 2019 r. była zmiana paradygmatu cenzury. Dotychczasowy system był nieszczelny i łatwy do obejścia za pomocą prostych narzędzi typu VPN. Nowe prawo nakazało operatorom telekomunikacyjnym instalację technicznych środków przeciwdziałania zagrożeniom opartych na technologii Deep Packet Inspection (DPI).Wdrożenie systemów DPI pozwoliło państwu na:

- selektywne zarządzanie ruchem – możliwość celowego spowalniania transferu danych dla konkretnych aplikacji (np. YouTube czy Twitter) bez całkowitego ich blokowania, co ma na celu zniechęcenie użytkowników do korzystania z „niepożądanych" serwisów;
- głęboką filtrację treści – w przeciwieństwie do blokowania całych domen, DPI pozwala na analizę zawartości pakietów danych, co umożliwia wycinanie konkretnych podstron, fraz kluczowych lub multimediów w czasie rzeczywistym;
- centralizację zarządu – w przypadku wystąpienia „sytuacji nadzwyczajnej", kontrolę nad wszystkimi węzłami DPI w kraju przejmuje centralnie Roskomnadzor, co w rzeczywistości pozwala na odcięcie transgranicznego ruchu internetowego za pomocą jednego polecenia systemowego.

Zgodnie z opisanymi wcześniej wytycznymi Strategii 2017–2030, ustawa z 2019 r. zmaterializowała koncepcję „izolowanego Internetu". Kluczowym elementem tej architektury stał się System Nazw Domen. Rosja, obawiając się teoretycznej możliwości odcięcia jej od serwerów root zarządzanych przez organizację ICANN, stworzyła własną replikę globalnego spisu adresów internetowych. Równolegle proces ten jest wspierany przez dążenie do tzw. suwerenności sprzętowej[14].

14 Opracowano na podstawie: *Federal'nyj zakon ot 01.05.2019 N 90-FZ „O wniesienii izmienienij w Federal'nyj zakon „O swiazi' i Federal'nyj zakon „Ob informacii, informacionnyh tiehnologijah i o zaszczitie informacii"* [w:] Baza Aktów Prawnych Consultant.ru, [dostęp: 08.02.2026], https://www.consultant.ru/document/cons_doc_LAW_323815/

Choć ustawa o „suwerennym Internecie" skupia się na warstwie programowej i przesyłowej, towarzyszą jej dyrektywy nakazujące administracji publicznej i infrastrukturze krytycznej przechodzenie na rosyjskie procesory (np. Elbrus, Bajkał) oraz systemy operacyjne (np. Astra Linux). Jest to próba domknięcia cyfrowej fortecy na poziomie fizycznym, co ma uniemożliwić zdalne wyłączenie rosyjskich systemów przez producentów zachodniego hardware'u. Wartym podkreślenia jest, że wdrażanie ustawy o „suwerennym Internecie" drastycznie zmieniło krajobraz cywilny w Rosji. Mechanizmy te zostały w pełni przetestowane i wykorzystane po lutym 2022 r., umożliwiając błyskawiczne zablokowanie platform Meta (Facebook, Instagram) oraz dziesiątek niezależnych portali informacyjnych. Do skutków wspomnianych działań zaliczyć można m.in. utrudnienia kontaktu z zagranicą – dla państw sąsiednich, w tym Polski, stanowi to wyzwanie wywiadowcze i dyplomatyczne, gdyż utrudnia dotarcie z niezależnym przekazem do rosyjskiego społeczeństwa[15].

Maria Domańska z Ośrodka Studiów Wschodnich już w 2019 r. zauważyła, że oficjalna retoryka uzasadniająca nowe regulacje potrzebą obrony przed zewnętrzną cyberdywersją pełni funkcję czysto ideologiczną. Jest ona emanacją paranoi rosyjskich elit politycznych (głównie tzw. siłowików), którzy w technologiach cyfrowych upatrują narzędzi zachodniego wywiadu, służących do destabilizacji reżimu. W tej optyce „suwerenizacja" internetu nie jest projektem technicznym, lecz geopolitycznym manifestem mocarstwowości. Realnym celem nie jest jednak ochrona infrastruktury, lecz uzyskanie pełnej kontroli nad krajowym obiegiem informacji, co czyni tę ustawę narzędziem polityki wewnętrznej, a nie obronnej. Ustawodawstwo wpisuje się w trwający od 2012 r. proces systematycznego ograniczania wolności w sieci. Jest to reakcja Kremla na lęk przed oddolnymi protestami, które – w narracji władz – są zawsze inspirowane z zewnątrz (tzw. scenariusz kolorowych rewolucji). Poprzez centralizację zarządzania ruchem państwo zyskuje narzędzia do selektywnego blokowania treści i inwigilacji użytkowników. Działania te mają wywołać tzw. efekt mrożący, zmuszając społeczeństwo do autocenzury w obliczu pogarszającej się sytuacji gospodarczej kraju. Głównymi beneficjentami zmian są służby specjalne (FSB) oraz Roskomnadzor, które zyskują niemal nieograniczony dostęp do danych bez nadzoru sądowego. Proces ten ma również drugie, korupcyjne dno – budowa „suwerennego Internetu" to lukratywny rynek dla firm powiązanych z elitą władzy, służący do drenażu funduszy państwowych. Jednocześnie wysokie koszty implementacji przepisów uderzają w mniejszych i zagranicznych operatorów, co prowadzi do wymuszonej konsolidacji i de facto nacjonalizacji rynku usług cyfrowych w Rosji[16].

15 M. Domańska, op. cit. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2019-12-04/zakneblowac-runet-uciszyc-spoleczenstwo-kremlowskie-ambicjech

16 M. Domańska, op. cit. https://www.osw.waw.pl/pl/publikacje/analizy/2019-04-19/twierdza-runet-walka-kremla-z-wrogim-internetem

Analiza ustawy o „suwerennym Internecie" w kontekście Doktryny z 2016 roku i Strategii na lata 2017-2030 wykazuje rzadką w rosyjskiej polityce konsekwencję. Rosja przestała postrzegać Internet jako szansę na rozwój gospodarczy, a zaczęła traktować go jako egzystencjalne zagrożenie dla stabilności reżimu. Runet w 2026 r. jest systemem zamkniętym, scentralizowanym i całkowicie podległym służbom specjalnym, co stanowi modelowy przykład transformacji globalnej sieci w narzędzie cyfrowego autorytaryzmu. Z całą pewnością ustawa o „suwerennym Internecie" jest zwieńczeniem rosyjskiej doktryny bezpieczeństwa.

Skutki i perspektywy – rosyjski model „cyfrowego lewiatana" a bezpieczeństwo międzynarodowe

Biorąc pod uwagę przeanalizowane dokumenty, można stwierdzić, że współczesna Rosja, dążąc do pełnej suwerenizacji swojej przestrzeni cyfrowej, tworzy model ustrojowy, który można określić mianem „cyfrowego lewiatana". Jest to system, w którym państwo przejmuje absolutną kontrolę nad technologią nie po to, by stymulować rozwój, lecz by zapewnić przetrwanie autorytarnej struktury władzy. Skutki tej transformacji wykraczają daleko poza granice Federacji Rosyjskiej, wpływając na globalną architekturę Internetu. W 2024 r. badaczka rosyjskiej sieci Ksenia Jermoszyna zauważyła, że: „Z tego co widzę w mediach i słyszałam od dostawców, Putin jest technosceptykiem. Nie ufa technologiom Internetu i się ich boi. Uważa, że są niebezpieczne i sam się stara powstrzymywać od internetowej aktywności. Jest wyznawcą tej kagiebowskiej narracji, że Internetowi nie można ufać, bo dookoła są wrogowie i stąd się biorą prawa do zwiększania kontroli. Rosyjskie władze dążą więc do stworzenia swojej sieci, w której będą miały swoje treści i będzie się ona opierała na innych wartościach niż sieć stworzona przez Amerykanów"[17].

Kluczowym skutkiem wewnątrzpolitycznym tego procesu jest, jak opisano w poprzednim rozdziale, wywołanie tzw. efektu mrożącego. Poprzez centralizację zarządzania ruchem internetowym oraz powszechne wdrożenie systemów głębokiej analizy pakietów, państwo zyskało zdolność do permanentnej inwigilacji i selektywnego blokowania treści. W rezultacie Internet przestał pełnić funkcję platformy mobilizacji społecznej, stając się sterylną przestrzenią nadzoru, w której świadomość obecności służb specjalnych w węzłach wymiany danych wymusza na obywatelach daleko posuniętą autocenzurę i mimikrę polityczną. Projekt „suwerennego Internetu" posiada również głęboki wymiar ekonomiczny i instytucjonalny, prowadząc do stopniowej nacjonalizacji rynku cyfrowego. Implementacja rygorystycznych przepisów

17 *W stronę Chin. Jak w Rosji tworzy się „suwerenny internet". Wywiad z badaczką rosyjskiej sieci Ksenią Jermoszyną rozmawiał* J. Bielakow, Biełsat TV, 10 czerwca 2019, [dostęp: 08.02.2026] https://pl.belsat.eu/82167158/w-strone-chin-jak-w-rosji-tworzy-sie-suwerenny-internet-wywiad-z-badaczka-rosyjskiej-sieci-ksenia-jermoszyna.

uderza przede wszystkim w mniejszych operatorów oraz podmioty zagraniczne, wymuszając ich wyparcie przez państwowe monopole lub firmy kontrolowane przez okołokremlowski establishment. Zjawisko to sprzyja korupcji systemowej, gdzie gigantyczne nakłady budżetowe na infrastrukturę kontrolną stają się formą renty politycznej dla służb specjalnych, w szczególności FSB[18]. W tym ujęciu bezpieczeństwo informacyjne staje się lukratywnym parawanem dla drenażu funduszy państwowych, co w perspektywie długofalowej skazuje Rosję na technologiczne zacofanie względem Zachodu. Z punktu widzenia bezpieczeństwa międzynarodowego działania Rosji są jednym z głównych motorów procesu fragmentacji globalnej sieci, określanego mianem „Splinternetu". Rosyjska koncepcja suwerenności informacyjnej otwarcie kwestionuje model otwartego Internetu, promując w zamian wizję świata podzielonego na cyfrowe enklawy podległe ścisłej jurysdykcji państwowej. Takie podejście nie tylko destabilizuje globalną architekturę cyfrową, ale staje się również modelem atrakcyjnym dla innych reżimów niedemokratycznych, co prowadzi do budowy antyzachodnich koalicji na forach międzynarodowych[19].

Analiza rosyjskich dążeń do suwerenności cyfrowej jest niepełna bez głębokiego odniesienia do modelu chińskiego, znanego jako Projekt Złota Tarcza (*Golden Shield Project*). Chiny, jako pionier cyfrowego autorytaryzmu, stworzyły najbardziej zaawansowany na świecie system cenzury i nadzoru, który dla Kremla stanowi zarazem inspirację, jak i nieosiągalny wzorzec technologiczny. Kluczowa różnica między obiema koncepcjami wynika z genetyki sieci w obu krajach. Podczas gdy Rosja próbowała „okiełznać" Internet już istniejący i wolny, Chiny budowały swój ekosystem równolegle z restrykcjami, co pozwoliło na organiczne wplecenie mechanizmów kontroli w samą architekturę przesyłu danych[20]. Model chiński opiera się na tzw. „aktywnej cenzurze", która wykracza daleko poza proste blokowanie adresów IP. System wykorzystuje zaawansowane filtrowanie słów kluczowych na poziomie bram sieciowych państwa (DNS filtering) oraz inspekcję pakietów (DPI) na skalę masową. Co istotne, w Chinach ciężar cenzury został przeniesiony na sektor prywatny. Giganci, tacy jak Tencent czy ByteDance, są prawnie zobowiązani do samoregulacji treści pod groźbą utraty licencji. To sprawia, że cenzura w Chinach jest zdecentralizowana wykonawczo, ale scentralizowana ideologicznie[21]. Algorytmy sztucznej inteligencji w czasie rzeczywistym analizują obrazy, dźwięki i tekst, usuwając treści „szkodliwe" zanim zdążą one uzyskać szerokie zasięgi. W przeciwieństwie do Rosji, gdzie blokady są często widoczne i budzą opór, chiński firewall działa „przezroczyście", tworząc u użytkownika iluzję, że zakazane treści po prostu nie istnieją. Niezwykle ważnym elemen-

18 I. Borogan, A. Soldatov, *The Red Web: The Kremlin's Wars on the Internet*, Public affairs 2015, s. 54-57.
19 M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press 2017, s. 45-50, [dostęp 07.02.2026] https://www.researchgate.net/publication/326861681_Will_the_Internet_fragment_Sovereignty_globalization_and_cyberspace
20 J. Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, Zed Books 2019, s. 25.
21 R. MacKinnon, *Consent of the Networked: The Worldwide Struggle For Internet Freedom*, Basic Books 2012, s. 38.

tem sukcesu Chin, którego Rosja desperacko próbuje dowieść u siebie, jest stworzenie narodowych championów technologicznych. Blokada Google, Facebooka czy Twittera w Chinach nie wywołała buntu społecznego, ponieważ państwo pozwoliło na rozwój funkcjonalnych odpowiedników: Baidu, WeChat czy Weibo[22]. Platformy te nie tylko zaspokajają potrzeby użytkowników, ale są również całkowicie transparentne dla chińskich służb bezpieczeństwa. Rosja, mimo posiadania platform, takich jak VKontakte czy Yandex, wciąż zmaga się z silną pozycją usług zachodnich, co czyni proces odcinania od globalnej sieci znacznie bardziej kosztownym politycznie i społecznie[23].

Główny punkt sporny w porównaniu obu systemów leży w strategii egzekwowania konformizmu politycznego. Chiny postawiły na system oceny obywateli, gdzie aktywność w sieci wpływa na realne życie – od możliwości zakupu biletu na pociąg po dostęp do kredytów. Jest to forma „cyfrowego behawioryzmu", który promuje konformizm bez konieczności masowych aresztowań. Rosja natomiast, nie posiadając tak wyrafinowanych narzędzi inżynierii społecznej, opiera się na tradycyjnym aparacie represji. Jak zauważają badacze, rosyjski model to „cenzura przez strach"; państwo wybiera jednostki i pokazowo je karze za wpisy w mediach społecznościowych, by wywołać efekt mrożący w całej populacji[24]. Niemniej, współpraca technologiczna między Rosją a Chinami w zakresie cyberbezpieczeństwa zacieśniła się, szczególnie po 2022 r. Rosja importuje chiński sprzęt do inwigilacji i konsultuje rozwiązania prawne dotyczące izolacji sieci. Jednakże pełne skopiowanie „Wielkiego Firewallu" wydaje się niemożliwe z trzech powodów. Po pierwsze, Rosja jest uzależniona od zachodnich komponentów sprzętowych w znacznie większym stopniu niż Chiny. Po drugie, chińska sieć od początku miała ograniczoną liczbę punktów styku ze światem zewnętrznym, podczas gdy rosyjski Internet jest ekstremalnie rozproszony (tysiące małych dostawców usług). Po trzecie, rosyjscy użytkownicy są znacznie bardziej przyzwyczajeni do obchodzenia blokad (użycie VPN w Rosji po 2022 r. wzrosło lawinowo), podczas gdy w Chinach korzystanie z narzędzi omijających cenzurę jest marginalizowane przez brak realnej potrzeby. Tym samym, o ile Chiny stworzyły „cyfrowy ogród" otoczony murem, o tyle Rosja buduje „cyfrowe więzienie" wewnątrz już istniejącego miasta. Model chiński jest projektem cywilizacyjnym, dążącym do stworzenia alternatywnej nowoczesności, podczas gdy model rosyjski jest projektem obronnym, nastawionym na reaktywną cenzurę i fizyczną eliminację zagrożeń dla stabilności reżimu[25]. Dla bezpieczeństwa międzynarodowego oznacza

22 M. Mueller, *Will the Internet Fragment?*, Polity Press 2017, s. 80.
23 K. Chawryło, M. Domańska, *Wielki rosyjski firewall. Próba ostatecznej rozprawy Kremla z wolnym internetem*, Raport OSW 2025, [dostęp 08.02.2026] https://www.osw.waw.pl/pl/publikacje/raport-osw/2025-12-19/wielki-rosyjski-firewall
24 A. Soldatov, I. Borogan, *The Red Web*, PublicAffairs 2015, s. 345.
25 J. Darczewska, *Diabeł tkwi w szczegółach Wojna informacyjna w świetle doktryny wojennej Rosji*, Raport OSW 2016, s. 18, [dostęp 08.02.2026] https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf

to, że Rosja będzie coraz częściej sięgać po chińskie technologie, by domknąć swój system, co ostatecznie przyspieszy proces globalnej bipolarności cyfrowej.

Podsumowanie

Głównym wnioskiem płynącym z badań jest stwierdzenie, że rosyjskie pojęcie suwerenności cyfrowej jest nierozerwalnie związane z paradygmatem autarkii informacyjnej. Jak wykazano, proces ten nie był gwałtowną reakcją na sankcje, lecz konsekwentnie realizowaną od 2000 r. strategią, która zakładała, że zależność od zachodnich technologii (zarówno w sferze hardware, jak i software) stanowi egzystencjalne zagrożenie dla państwa. Implementacja „suwerennego Internetu" (Runetu) dowiodła, że Rosja jako jedno z nielicznych państw na świecie wypracowała zdolność do technicznego odizolowania własnego segmentu sieci przy jednoczesnym zachowaniu jego funkcjonalności dla celów wewnętrznych. Kolejnym kluczowym wnioskiem jest potwierdzenie dualistycznego charakteru rosyjskiego bezpieczeństwa informacyjnego. Zacieranie różnic między sferą techniczną a psychologiczną pozwoliło Kremlowi na penalizację aktywności w sieci nie tylko w oparciu o kryteria techniczne, ale przede wszystkim treściowe (ideologiczne). Ustawodawstwo z lat 2012–2024, ze szczególnym uwzględnieniem „pakietu Jarowej" oraz ustaw o „fake newsach", stworzyło systemowy mechanizm inwigilacji, który wywołał tzw. efekt mrożący. W efekcie cyberprzestrzeń w Rosji stała się przestrzenią wysokiego ryzyka, gdzie za „nieprawomyślny" komentarz czy udostępnienie informacji grożą sankcje karne identyczne z tymi za sabotaż infrastruktury krytycznej.

W perspektywie międzynarodowej, rosyjski model „cyfrowego lewiatana" stanowi wyzwanie dla globalnej stabilności sieci. Dążenie Moskwy do fragmentacji Internetu (tzw. Splinternet) uderza w fundamenty liberalnego ładu informacyjnego. Analiza porównawcza z modelem chińskim wykazała, że o ile Pekin budował swój „Wielki Firewall" jako system filtracji od podstaw, o tyle Rosja stworzyła system hybrydowy – łączący nowoczesną inżynierię ruchu (DPI) z tradycyjnymi, brutalnymi represjami służb bezpieczeństwa (FSB). To podejście okazuje się niezwykle atrakcyjne dla innych reżimów autorytarnych, co sugeruje, że w najbliższej dekadzie będziemy świadkami powstawania cyfrowych bloków politycznych, co trwale zakończy erę tzw. „globalnej wioski".

Należy również zauważyć, że rosyjska aktywność w cyberprzestrzeni po 2022 r. ostatecznie potwierdziła tezę o informacyjnym charakterze współczesnych konfliktów zbrojnych. Cyberataki na infrastrukturę krytyczną Ukrainy i państw wschodniej flanki NATO były nierozerwalnie połączone z kampaniami dezinformacyjnymi, mającymi na celu erozję zaufania społecznego do instytucji demokratycznych. Dla

państw, takich jak Polska, oznacza to konieczność redefinicji własnych strategii bezpieczeństwa: cyberobrona nie może ograniczać się jedynie do aspektów technicznych, ale musi obejmować również budowę odporności społecznej na operacje psychologiczne.

Konkludując, Federacja Rosyjska przekształciła cyberprzestrzeń w instrument projekcji siły i narzędzie ochrony monopolu ideologicznego. Proces legislacyjny, który rozpoczął się od ochrony dzieci przed szkodliwymi treściami, zakończył się budową totalnego systemu nadzoru, w którym informacja jest traktowana jako broń masowego rażenia. Perspektywy na lata 2027–2030 wskazują na dalsze zacieśnianie kontroli, w tym wykorzystanie sztucznej inteligencji do predykcyjnej analizy nastrojów społecznych i automatycznego usuwania treści opozycyjnych. „Suwerenność ideologiczna" w rosyjskim wydaniu jest zatem eufemizmem oznaczającym całkowitą eliminację pluralizmu informacyjnego w imię stabilności autorytarnej władzy.

Bibliografia

Literatura

Borogan I., Soldatov A., *The Red Web: The Kremlin's Wars on the Internet*, Public affairs, New York 2015.

Budzisz M., *Wszystko jest wojną. Rosyjska kultura strategiczna*, Warszawa 2021.

Chawryło K., Domańska M., *Wielki rosyjski firewall. Próba ostatecznej rozprawy Kremla z wolnym internetem*, Raport OSW 2025, https://www.osw.waw.pl/pl/publikacje/raport-osw/2025-12-19/wielki-rosyjski-firewall [dostęp 08.02.2026].

Darczewska J., *Zawładnąć umysłami i urządzić świat. Rosyjska strategia dywersji i dezinformacji*, Raport OSW, Warszawa 2014.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Raport OSW, Warszawa 2014.

Darczewska J., *Diabeł tkwi w szczegółach Wojna informacyjna w świetle doktryny wojennej Rosji*, Raport OSW, Warszawa 2016.

Domańska M., *Twierdza Runet: walka Kremla z „wrogim" Internetem*, Analizy OSW 2019, https://www.osw.waw.pl/pl/publikacje/analizy/2019-04-19/twierdza-runet-walka-kremla-z-wrogim-internetem [dostęp 08.02.2026].

Griffiths J., *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, Zed Books, London 2019.

Kozłowski A., *Cyberwojownicy Kremla*, „Biuletyn OPINIE FAE", 6/2014, https://www.researchgate.net/publication/345906006_Cyberwojownicy_Kremla/link/5fb17d0545851518fda9b7a0/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 [dostęp 15.01.2026].

MacKinnon R., *Consent of the Networked: The Worldwide Struggle For Internet Freedom*, Basic Books, New York 2012.

Mueller M., *Will the Internet Fragment? Sovereignty*, Globalization and Cyberspace, Polity Press, Cambridge 2017. https://www.researchgate.net/publication/326861681_Will_the_Internet_fragment_Sovereignty_globalization_and_cyberspace [dostęp 07.02.2026].

Zapała K., *Cele FR w zakresie bezpieczeństwa informacyjnego na podstawie zapisów rosyjskich dokumentów strategicznych*, Instytut Nowej Europy 2020, https://ine.org.pl/cele-fr-w-zakresie-bezpieczenstwa-informacyjnego-na-podstawie-zapisow-rosyjskich-dokumentow-strategicznych/ [dostęp: 08.02.2026].

Źródła prawa

Doktrina informacionnoj biezopasnosti Riedieracyi, utwierżdena Priezidientom Rossijskoj Fiedieracyi 5 sientiabria 2000 g. № PR-1895, http://www.scrf.gov.ru/security/information/document5/, [dostęp: 08.02.2026].

Federal'nyj zakon ot 27.07.2006 N 149-FZ „Ob informacii, informacionnyh tehnologijah i o zascite informacii" https://base.garant.ru/182535/ [dostęp: 08.02.2026].

Ukaz Priezidienta Rossijskoj Fiedieracyi ot 09.05.2017 g. № 203 „O Strategii razwitija informacionnogo obszczestwa w Rossijskoj Fiedieracyi na 2017–2030 gody", http://static.kremlin.ru/media/acts/files/0001201705100002.pdf [dostęp: 08.02.2026].

Federal'nyj zakon ot 01.05.2019 N 90-FZ „O wniesienii izmienienij w Federal'nyj zakon ‚O swiazi' i Federal'nyj zakon ‚Ob informacii, informacionnyh tiehnologijah i o zaszczitie informacii', https://www.consultant.ru/document/cons_doc_LAW_323815/, [dostęp: 08.02.2026].

Źródła internetowe

Bielakov J., *W stronę Chin. Jak w Rosji tworzy się „suwerenny internet"*, Biełsat TV, 10 czerwca 2019, https://pl.belsat.eu/82167158/w-strone-chin-jak-w-rosji-tworzy-sie-suwerenny-internet-wywiad-z-badaczka-rosyjskiej-sieci-ksenia-jermoszyna [dostęp: 08.02.2026].

Domańska M., *Zakneblować Runet, uciszyć społeczeństwo. Kremlowskie ambicje „suwerenizacji" Internetu*, Komentarze OSW 2019. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2019-12-04/zakneblowac-runet-uciszyc-spoleczenstwo-kremlowskie-ambicjech [dostęp 31.01.2026].

Hircock S., *Cyber Shield 2025*, https://www.army.mil/article/286378/cyber_shield_2025 [dostęp 31.01.2026].

Polowninko A., *Internet zamieniat sriedoj oborota dostowiernoj informacyi „Novaja Gazieta"*, https://novayagazeta.ru/articles/2021/07/06/internet-zameniat-sredoi-oborota-dostovernoi-informatsii [dostęp: 08.02.2026].