57

PRACE OSW

OSW

# ROSYJSKIE SIŁY ZBROJNE NA FRONCIE WALKI INFORMACYJNEJ
## DOKUMENTY STRATEGICZNE

Jolanta Darczewska

PRACE OSW

NUMER 57
WARSZAWA
CZERWIEC 2016

# ROSYJSKIE SIŁY ZBROJNE NA FRONCIE WALKI INFORMACYJNEJ

## DOKUMENTY STRATEGICZNE

Jolanta Darczewska

OSW | CENTRE FOR EASTERN STUDIES
OŚRODEK STUDIÓW WSCHODNICH im. **Marka Karpia**

REDAKCJA
Anna Łabuszewska

WSPÓŁPRACA
Halina Kowalczyk, Katarzyna Kazimierska

OPRACOWANIE GRAFICZNE
PARA-BUCH

ZDJĘCIE NA OKŁADCE
Agencja Shutterstock

SKŁAD
GroupMedia

WYDAWCA
**Ośrodek Studiów Wschodnich im. Marka Karpia**
Centre for Eastern Studies

ul. Koszykowa 6a, Warszawa
Tel. + 48 /22/ 525 80 00
Fax: + 48 /22/ 525 80 40
osw.waw.pl

ISBN 978-83-62936-87-8

Spis treści

## TEZY

1. Obserwowana dziś militaryzacja przestrzeni publicznej Federacji Rosyjskiej jest rezultatem długiego procesu. Od 2000 roku tzw. zagrożenia informacyjne są przedmiotem szeroko nagłaśnianych strategii, które uzasadniają zarówno wojskową politykę informacyjną, jak i zadania związane z walką informacyjną. Nie ograniczają się one do projektów krajowych – Rosja manifestuje ambicje działania na poziomie regionalnym i globalnym, buduje wspólną eurazjatycką przestrzeń informacyjną, zgłasza projekty konwencji międzynarodowych i kodeksów działania w międzynarodowej przestrzeni informacyjnej, demonstrując własną wizję oraz prawo do współdecydowania o bezpieczeństwie globalnym.

2. Mimo stałego podkreślania militarnego wymiaru problematyki bezpieczeństwa informacyjnego monopol w tej dziedzinie miały do niedawna rosyjskie służby specjalne, oficjalnie skupiające się na ochronie społeczeństwa przed destrukcyjnym oddziaływaniem z zewnątrz oraz ochronie informacyjnej infrastruktury krytycznej. Na początku obecnej dekady sytuacja uległa zmianie: przestrzeń publiczną zdominowały działania wojskowego segmentu systemu bezpieczeństwa informacyjnego, o niespotykanym wcześniej rozmachu. Koncentrują się one na legitymizowaniu konfrontacyjnej polityki Kremla wobec NATO i Zachodu, którą zintensyfikowano po powrocie Władimira Putina na Kreml w 2012 roku.

3. Zgodnie z oficjalnymi deklaracjami resort obrony „podjął wyzwania w sferze bezpieczeństwa i obrony Federacji Rosyjskiej", manifestując zdolności do przeciwstawiania się zagrożeniom informacyjnym i współdziałania z sektorem bezpieczeństwa. Takie połączenie elementów strategii bezpieczeństwa wewnętrznego z elementami strategii obrony ściśle powiązało strategiczny wymiar obronny z wymiarem politycznym. W efekcie resort obrony realizuje w przestrzeni publicznej funkcje, które wykraczają poza jego kompetencje obronne (światopoglądową, edukacyjno-dydaktyczną): manifestuje gotowość do powstrzymania fali kolorowych rewolucji skierowanych przeciwko władzom Rosji, do przeciwstawienia się hegemonii USA w przestrzeni informacyjnej, broni statusu języka rosyjskiego i obywateli rosyjskojęzycznych w państwach ościennych oraz interesów narodowych Rosji poza granicami kraju.

4. Pytanie o rolę sił zbrojnych w przestrzeni informacyjnej jest w istocie pytaniem o rolę czynnika siły w polityce wewnętrznej i zagranicznej Kremla.

Na przestrzeni dziejów był on niezmiennie traktowany jako wyznacznik mocarstwowej pozycji Rosji w świecie, instrument odstraszania, środek nacisków politycznych i budowania sfer wpływów. Dziś stał się argumentem uzasadniającym racje Rosji przedstawianej jako eurazjatyckie centrum siły i rozwoju oraz przeciwstawianej wspólnocie euroatlantyckiej. Dla Kremla dążącego do zmiany istniejącego paradygmatu relacji międzynarodowych stanowi on główne uzasadnienie aneksji Krymu, wojny w Donbasie i rosyjskiej interwencji w Syrii.

## WSTĘP

W niniejszym tekście poddano analizie zapisy kilku dokumentów strategicznych. Kompleksowe podejście umożliwia wydobycie różnych aspektów działań informacyjnych Sił Zbrojnych Federacji Rosyjskiej, w tym z dziedziny *cyberpower*. Pozwala także sformułować wnioski o ciągłości podejścia strategicznego oraz trwałości mechanizmów realizacji strategicznych celów.

Tekst składa się z dwóch części: w pierwszej omówiono specyfikę oficjalnych dokumentów, w drugiej – wybrane przejawy operacjonalizacji działań informacyjnych rosyjskich sił zbrojnych w przestrzeni informacyjnej na poziomie krajowym, regionalnym i międzynarodowym.

Zderzenie teorii z praktyką pokazuje rozziew między wojskową myślą strategiczną a działaniami.

# I. ZARYS PROBLEMATYKI – WOJSKOWY WYMIAR PRZESTRZENI INFORMACYJNEJ

## 1. Strategiczne „dwójmyślenie"

Związany z rozwojem Internetu przełom technologiczny w ostatniej dekadzie XX wieku (pojawienie się nowych technologii informatycznych, IT, sprzężonych z technologiami komunikowania się – ICT) zwiększył znaczenie systemów informatycznych. W **Doktrynie wojennej Federacji Rosyjskiej** z 2000 roku po raz pierwszy zauważono, że zinformatyzowane środowisko bezpieczeństwa i obrony wymaga nowych narzędzi i strategii. Dokument ten unaocznił zarazem specyfikę rosyjskiej terminologii, podkreślającej odrębność rosyjskiego podejścia strategicznego. W odróżnieniu od zachodnich strategów, rozpatrujących głównie przestrzeń utechnicznionej informacji (cyberprzestrzeń) jako obszar nowych zinformatyzowanych systemów walki i obrony, Rosjanie od początku podkreślali potrzebę/konieczność działań sił zbrojnych Rosji w „przestrzeni informacyjnej" czy „informacyjne" zagrożenia dla rosyjskiej armii, kładąc nacisk na ich psychologiczny charakter.

Militarny wymiar problematyki informacyjnej (w rosyjskim ujęciu) podkreślała także przyjęta we wrześniu 2000 roku i obowiązująca do dziś **Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej**. Bezpieczeństwo informacji potraktowano w niej jako podstawę bezpieczeństwa państwa, a „broń informacyjną" jako jedno z narzędzi do osiągania celów politycznych. Głębsza analiza fragmentu poświęconego działaniom „informacyjnym" państwa w sferze obrony umożliwia zarazem sformułowanie wniosku o swoistym dwójmyśleniu rosyjskich strategów, łączących podejście informacyjno-techniczne/technologiczne z podejściem informacyjno-psychologicznym.

Uwidoczniło się to zwłaszcza w ocenie zagrożeń informacyjnych, wśród których obok opracowywania przez szereg państw koncepcji wojen informacyjnych, dążenia wielu krajów do dominacji i ograniczenia interesów Rosji w globalnej przestrzeni informacyjnej czy działalności dywersyjnej obcych służb specjalnych za pomocą oddziaływania informacyjno-psychologicznego wymieniono obce działania informacyjno-techniczne (walkę radioelektroniczną, przenikanie do sieci komputerowych ze strony potencjalnych przeciwników, stosowanie kosmicznych, powietrznych, morskich i naziemnych technicznych środków wywiadu i rozpoznania i in.). Doktryna wytyczyła ponadto

główne kierunki doskonalenia działań w sferze obrony[1], dotyczące zarówno informacyjnej przestrzeni psychologicznej, jak i technologicznej.

Ten obszerny dokument, szczegółowo omawiający zagrożenia informacyjne w różnych sferach (gospodarki, polityki wewnętrznej, polityki zagranicznej, nauki i techniki, życia duchowego, w sferze obrony oraz ochrony porządku prawnego Rosji), wprowadził większość pojęć („wojna informacyjna", „broń informacyjna", „maskowanie przeciwdziałania informacyjnego") wykorzystywanych następnie w dokumentach oficjalnych i obszernej literaturze przedmiotu, popularyzującej tę problematykę. **Doktryna bezpieczeństwa informacyjnego FR** z 2000 roku do dziś pozostaje oficjalnym dokumentem ramowym, do którego stale nawiązują późniejsze rosyjskie dokumenty strategiczne. Wyróżniają ją bowiem szeroko zakreślone ramy koncepcyjne: już w tym dokumencie władze Rosji przestrzegały np. przed naruszaniem praw rosyjskich obywateli i osób prawnych za granicą oraz rozpowszechnianiem dezinformacji o polityce zagranicznej Federacji Rosyjskiej, zaś do obiektów ochrony zaliczyły m.in. „język rosyjski jako czynnik duchowego jednoczenia narodów wielonarodowościowej Rosji, język międzypaństwowej komunikacji narodów państw członkowskich Wspólnoty Niepodległych Państw"[2].

Równie szerokie ujęcie, które umożliwia i potęguje brak precyzji terminologicznej, cechuje sukcesywnie już nagłaśniany projekt nowej **Doktryny bezpieczeństwa informacyjnego FR**[3], której przyjęcie zapowiedziano na 2016

[1] Zaliczono do nich: systematyczne wykrywanie zagrożeń informacyjnych i ich źródeł (...); certyfikację oprogramowania ogólnego i specjalnego, pakietów programów użytkowych i środków ochrony informacji w istniejących i tworzonych zautomatyzowanych systemach dowodzenia i wojskowych systemach łączności zawierających elementy techniki komputerowej; stałe doskonalenie środków ochrony informacji przed nielegalnym dostępem, rozwój zabezpieczonych systemów łączności, dowodzenia wojskami i systemów naprowadzania broni, zwiększenie niezawodności specjalnego oprogramowania; doskonalenie struktury funkcjonalnych organów systemu zapewnienia bezpieczeństwa informacyjnego w sferze obrony i koordynacja ich współdziałania; doskonalenie metod i sposobów maskowania strategicznego i operacyjnego, wywiadu i walki elektronicznej, metod i środków aktywnego przeciwdziałania informacyjno-propagandowym i psychologicznym operacjom potencjalnego przeciwnika; szkolenie specjalistów w dziedzinie zapewnienia bezpieczeństwa informacyjnego w sferze obrony.

[2] To podejście nie zmieniło się do dziś. W wypowiedzi z 27 stycznia 2016 roku wiceszef Akademii Sztabu Generalnego FR gen. Siergiej Czwarkin stwierdził np., że jednym z kluczowych zagrożeń bezpieczeństwa narodowego Federacji Rosyjskiej jest spadek znaczenia języka rosyjskiego na świecie. Język i sfera kultury stanowią w jego ocenie ważny obszar konfrontacji w prowadzonych obecnie wojnach informacyjnych (zob. www.russkiymir.ru/news/202777).

[3] Projekt doktryny zob. http://infosystems.ru/assets/files/files/doktrina_IB.pdf

rok. W punkcie 17, dotyczącym specyficznych zadań resortu obrony w przestrzeni informacyjnej, obok długoterminowych działań kontynuowanych (monitoring zagrożeń, doskonalenie systemu bezpieczeństwa informacyjnego oraz rozwój sił i środków walki informacyjnej), pojawiły się nowe wytyczne, takie jak: tworzenie warunków prawnomiędzynarodowego zapobiegania agresji informacyjnej, rozwój wojskowej polityki informacyjnej, strategiczne powstrzymywanie konfliktów w przestrzeni informacyjnej, neutralizowanie oddziaływania informacyjnego na ludność cywilną, w pierwszym rzędzie na młodych obywateli, wzmacnianie historycznych, duchowych i patriotycznych tradycji społeczeństwa itp. Na marginesie należy zauważyć, że wymienione „inicjatywy strategiczne" w gruncie rzeczy są od dawna realizowane w praktyce, należy je zatem traktować jako próbę usankcjonowania stosownych działań Ministerstwa Obrony.

W porównaniu z omówioną strategią ramową kolejne redakcje rosyjskiej doktryny wojennej (2010, 2014) są mniej precyzyjne, powtarzają ogólne sformułowania, wytyczne i postulaty zawarte w dokumencie ramowym[4]. Problematyka bezpieczeństwa informacyjnego jest w nich rozproszona, jej *stricte* wojskowe aspekty – ledwie zasygnalizowane. Obsesyjnie uwypuklono natomiast jej aspekty społeczne i polityczno-wojskowe. W wersji z 2014 roku podkreślono np. tendencję przesuwania się zagrożeń wojennych do przestrzeni informacyjnej i sfery wewnętrznej (p. 11), jak również wykorzystanie technologii informacyjnych i komunikacyjnych w celach wojskowo-politycznych do prowadzenia działań sprzecznych z prawem międzynarodowym, skierowanych przeciwko suwerenności, niezawisłości politycznej i integralności terytorialnej państw (p. 12). Tradycyjnie przewidziano też konieczność doskonalenia współdziałania systemu bezpieczeństwa informacyjnego sił zbrojnych oraz innych wojsk i organów (p. 35) oraz systemów zarządzania informacją na poziomie strategicznym, operacyjnym i taktycznym (p. 46).

## 2. Terminologiczna nowomowa

Ogólnikowe sformułowania, przypominające slogany propagandowe, dla ekspertów zewnętrznych stanowią istotny problem interpretacyjny. Jego przezwyciężeniu nie służą zawarte w niektórych dokumentach słowniki stosowanych

[4] Szerzej na ten temat zob. Jolanta Darczewska, Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji, *Punkt Widzenia OSW*, nr 50, maj 2015; http://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2015-05-19/diabel-tkwi-w-szczegolach-wojna-informacyjna-w-swietle-doktryny

pojęć. Pojęcie kluczowe dla danej problematyki, jakim jest „przestrzeń informacyjna", w dokumencie Ministerstwa Obrony Federacji Rosyjskiej **Koncepcja działalności Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej** (2012)[5] zdefiniowano np. jako „sferę działalności związaną z kształtowaniem, tworzeniem, przekształcaniem, przekazem, wykorzystywaniem i przechowywaniem informacji, wpływającą na świadomość indywidualną i społeczną, a także infrastrukturę informacyjną i *stricte* – informację". Wprowadzając taką definicję, podmieniono niejako pojęcie „systemu informacyjnego", który w Rosji, jak i każdym państwie, jest zbiorem zasobów, ludzi, technologii (w tym IT i ICT), metod i procesów zdobywania, gromadzenia, przetwarzania i prezentacji informacji. Tak zdefiniowana przestrzeń informacyjna, będąca wojskowym polem konfrontacji i polem walk informacyjnych, ma jednocześnie charakter przestrzeni geograficznej, politycznej, ekonomicznej, społecznej oraz cywilizacyjnej (duchowej, językowej, kulturowej). Pojęcie „system" pojawia się w tymże dokumencie dla tradycyjnego podkreślenia jego wszechpotęgi: siły zbrojne określono jako „część systemu bezpieczeństwa informacyjnego FR", ten z kolei mgliście zdefiniowano jako „część systemu bezpieczeństwa narodowego kraju przeznaczoną do realizacji polityki państwa w sferze bezpieczeństwa informacyjnego". Oba pojęcia są powszechnie wykorzystywane w wojskowej praktyce informacyjnej; mają jednak odmienne funkcje propagandowe.

## 3. Armia jako część systemu bezpieczeństwa informacyjnego

Tego rodzaju zbitki pojęciowe nie przesłaniają zasadniczej wymowy omawianych dokumentów: rosyjskie siły zbrojne podejmują działania defensywne (dla obrony integralności własnego systemu informacyjnego przed oddziaływaniem, niszczeniem i zakłócaniem przez przeciwnika), a jednocześnie działania ofensywne (mające na celu oddziaływanie, uszkadzanie i niszczenie systemu informacyjnego przeciwnika). Nie odróżnia to rosyjskiej armii od armii innych państw. Zasadnicza różnica między nimi polega na tym, że rosyjska armia, wespół z pozostałymi podmiotami bezpieczeństwa wewnętrznego i zewnętrznego Federacji Rosyjskiej, wypełnia zadanie obrony rosyjskiej przestrzeni informacyjnej przed konkurencyjnymi modelami rozwoju politycznego, ekonomicznego, społecznego i kulturowego, tj. w gruncie rzeczy obrony rosyjskiego reżimu autokratycznego. I co najmniej od 2000 roku przygotowuje się do konfliktów w przestrzeni informacyjnej oraz buduje zdolności do ich prowadzenia.

[5] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве – zob. http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle

Co więcej, stosowana dziś wobec Zachodu „broń informacyjna" została przetestowana na arenie wewnętrznej podczas budowania „jednolitej przestrzeni informacyjnej FR", tj. przejmowania przez państwo kontroli nad systemem informacyjnym i głównymi środkami masowego przekazu jako jego filarem. Głównym wykonawcą tego zadania były rosyjskie służby specjalne. Podejmowały one różnorakie działania: szykany wobec NGO („agentów zagranicznych") i masowe powoływanie GONGO (organizacje pozarządowe pod kontrolą państwa), tworzenie zaplecza analitycznego (tzw. społeczne think tanki) i dziennikarskiego, cyberataki przeciwko działaczom i mediom opozycyjnym czy zamykanie opozycyjnych mediów i portali społecznościowych pod pretekstem walki z ekstremizmem. Do niedawna służby miały monopol w dziedzinie bezpieczeństwa informacyjnego Federacji Rosyjskiej. Na początku obecnej dekady sytuacja uległa zmianie: przestrzeń publiczną zdominowały działania wojskowego segmentu systemu. Koncentrują się one na legitymizowaniu konfrontacyjnej polityki Kremla wobec NATO i Zachodu.

W tym kontekście należy stwierdzić, że zauważalny w dokumentach strategicznych przechył w stronę akcji informacyjnych jest zabiegiem zamierzonym. Kierując uwagę opinii publicznej na znaczenie czynnika siły w relacjach zewnętrznych, rosyjscy stratedzy uruchamiają zarazem myślenie konfrontacyjne, nieufność i wrogość wobec Zachodu, przede wszystkim Stanów Zjednoczonych i NATO. W stosowanej powszechnie propagandzie, której koncepcyjne założenia zawierają m.in. jawne dokumenty strategiczne, to Zachód wydał Rosji wojnę informacyjną i rozpoczął informacyjny wyścig zbrojeń.

## II. OGÓLNA CHARAKTERYSTYKA ROSYJSKICH DOKUMENTÓW STRATEGICZNYCH

### 1. Źródła

Oprócz wspomnianych **Doktryny wojennej FR oraz Doktryny bezpieczeństwa informacyjnego FR** zarysy wojskowej strategii działań Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej odnajdujemy w szeregu innych dokumentów (zob. Aneks 1). Niektóre z nich, jak np. **Strategia bezpieczeństwa narodowego Federacji Rosyjskiej** z 31 grudnia 2015 roku, powierzchownie odnoszą się do problematyki, podkreślając jednak wagę nowych technologii wojskowych oraz konieczność obrony „suwerenności kulturowej" i społeczeństwa przed destrukcyjnym wpływem informacyjnym. Inne – jak **Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku** z lipca 2013 roku – są w całości dedykowane omawianej problematyce, choć roli sił zbrojnych szczególnie tu nie uwypuklono (podobnie jak innych podmiotów bezpieczeństwa informacyjnego Federacji Rosyjskiej). Warto podkreślić, że wymienione dokumenty są publicznie dostępne, można je znaleźć np. na stronie Rady Bezpieczeństwa Federacji Rosyjskiej[6]. Są one autoryzowane przez Radę i objęte przez nią patronatem informacyjnym, tj. długotrwałą akcją propagandową.

Publicznie dostępny jest także resortowy dokument, jakim jest przygotowana w Ministerstwie Obrony **Koncepcja działalności Sił Zbrojnych FR w przestrzeni informacyjnej**, opublikowana w styczniu 2012 roku. Pozostaje ona najmniej znanym dokumentem strategicznym, w związku z czym poświęcono jej tu więcej uwagi (zob. Aneks 2). Większość resortowych dokumentów strategicznej natury pozostaje jednak niejawna. Światła dziennego nie ujrzały np. **Podstawy polityki wojskowo-technicznej na okres do 2020 roku i dalszą perspektywę** z 26 stycznia 2011 roku, **Podstawowe kierunki polityki państwa w zakresie bezpieczeństwa zautomatyzowanych systemów kierowania procesami technologicznymi i produkcyjnymi obiektów infrastruktury krytycznej Federacji Rosyjskiej** z 3 lutego 2012 roku czy sygnalizowana przez ministra Siergieja Szojgu 30 marca 2015 roku podczas kolegium Ministerstwa Obrony **Koncepcja rozwoju technologii informacyjnych i telekomunikacyjnych Sił Zbrojnych FR na okres do 2020 roku**.

[6] Zob. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года; http://www.scrf.gov.ru/documents/6/114.html

Kompleksowa analiza dokumentów umożliwia nie tylko uchwycenie specyfiki rosyjskiego podejścia strategicznego, ale i wyciągnięcie wniosku o ciągłości tego podejścia, umożliwiającego realizację krótko- i długoterminowych celów armii rosyjskiej w przestrzeni informacyjnej.

## 2. Problem podstawowy: socjotechnika

Rosyjski model refleksji na temat działań armii w przestrzeni informacyjnej różni się zasadniczo od modelu zachodniego. W modelu zachodnim przeważa bardziej adekwatna do działań wojskowych wizja „cyberprzestrzeni". Rosyjscy stratedzy operują pojęciem „przestrzeń informacyjna", rozpatrując ją w kategoriach zagrożeń społecznych, politycznych i cywilizacyjnych. Jest to podejście zamierzone, uzasadnia bowiem wewnętrzną i zewnętrzną politykę Kremla. Uwypuklając „informacyjny", a nie „cybernetyczny" charakter działań rosyjskiej armii, kładą nacisk na samą informację (i jej treść) oraz agitację i mobilizację, co wynika z powierzonej siłom zbrojnym misji neutralizowania oddziaływania informacyjnego na własne kadry i ludność cywilną. Priorytet nadano przy tym udziałowi armii w rządowej propagandzie, realizowanej w praktyce za pośrednictwem jej odrębnego modułu wojskowego, który współtworzą holding medialny Krasnaja Zwiezda oraz powiązane z nim tradycyjne i elektroniczne środki masowego przekazu.

**Jednocześnie rosyjscy stratedzy wyraźnie nawiązują do zachodniej myśli wojskowej; ostatnio np. przybliżają koncepcję wojen hybrydowych. Podkreślają w ten sposób, że rosyjskie działania nie różnią się od analogicznych jakoby działań zachodnich. Zabieg ten, stosowany także w literaturze fachowej, często prowadzi zagranicznych analityków na manowce: rosyjski niejednoznaczny aparat pojęciowy traktują jako lustrzane odbicie własnego. Tymczasem adaptując zachodnie terminy, Rosjanie kierują się własnymi założeniami i logiką, przysposabiają je do własnych potrzeb, tradycji i kultury strategicznej. Przenosząc zachodnie teorie na rosyjski grunt, mieszają koncepcje obrony i ataku, dostosowując je do własnej geostrategii rewanżu**[7].

Znajduje to zastosowanie w praktyce propagandowej: jeśli np. doktryna NATO kładzie nacisk na rozpoznanie wojskowe i ochronę danych z rozpoznania przy

[7] Zob. Владимир Горбулин, „Гибридная война" как ключевой инструмент российской геостратегии реванша, *Зеркало Недели,* 23.01.2015; http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html

użyciu nowych technologii: COMSEC (*communication security*) i COMPUSEC (*computer security*), to rosyjska doktryna uwrażliwia wojskowych na „broń informacyjną" przeciwnika, zamiast „psychologicznej osłony pola walki", rosyjscy wojskowi neutralizują psychologiczne oddziaływanie przeciwnika na ludność cywilną, „broniąc historycznych, duchowych i patriotycznych tradycji w dziedzinie obrony Ojczyzny" itp.

## 3. Czwarte zagrożenie

Spektakularnym przejawem mieszania porządków politycznego i wojskowego jest utrzymujące priorytet w strategicznej myśli wojskowej tzw. czwarte zagrożenie. Zachodnią triadę zagrożeń w cyberprzestrzeni (cyberwojna, cyberterroryzm i cyberprzestępczość) Rosjanie rozszerzają o informacyjną ingerencję w sprawy wewnętrzne suwerennych państw. W dokumencie **Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku** (2013) zdefiniowano je jako „wykorzystywanie technologii informacyjnych i komunikacyjnych jako broni informacyjnej w celach polityczno-wojskowych do ingerencji w sprawy wewnętrzne państw, (...) naruszania porządku publicznego, wzniecania wrogości na tle etnicznym, rasowym, religijnym, propagandy rasistowskich i ksenofobicznych idei i teorii, budzących nienawiść i dyskryminację, podżegających do przemocy".

W **Doktrynie bezpieczeństwa informacyjnego FR** z 2000 roku pojawiło się ono w postaci zagrożeń w sferze życia duchowego, wśród których wymieniono „możliwość naruszenia stabilności społecznej, szkodzenie zdrowiu i życiu obywateli wskutek działalności związków religijnych głoszących fundamentalizm religijny, a także totalitarnych sekt religijnych; wykorzystywanie przez obce służby specjalne środków masowego przekazu działających na terytorium Federacji Rosyjskiej w celu naruszenia zdolności obronnej kraju i bezpieczeństwa państwa oraz rozpowszechniania dezinformacji; niezdolność współczesnego społeczeństwa obywatelskiego Rosji do kształtowania wśród dorastającego pokolenia oraz podtrzymania w społeczeństwie pożądanych wartości etycznych, patriotycznych i odpowiedzialności za los kraju".

W związku z tym postulowano m.in. opracowanie mechanizmu kontroli nad kształtowaniem w społeczeństwie wartości duchowych, odpowiadających interesom narodowym kraju, nad wychowaniem młodzieży w duchu patriotyzmu i odpowiedzialności za los kraju; stworzenie prawa regulującego stosunki w dziedzinie konstytucyjnych ograniczeń praw i wolności człowieka

i obywatela; państwowe wsparcie dla działań na rzecz odrodzenia dziedzictwa kulturalnego narodów i narodowości Federacji Rosyjskiej oraz stworzenie „prawnych i organizacyjnych mechanizmów uniemożliwiających niezgodne z prawem oddziaływanie informacyjno-psychologiczne na masową świadomość społeczeństwa, niekontrolowaną komercjalizację kultury i nauki, a także gwarantujących zachowanie kulturalnych i historycznych wartości narodów i narodowości Federacji Rosyjskiej".

Czwarte zagrożenie ma wymiar praktyczny, służy bowiem do osiągania różnych celów politycznych. Świadczy o tym chociażby modyfikacja treści tego pojęcia. O ile w 2000 roku służyło ono podkreśleniu znaczenia „przeciwdziałania negatywnemu wpływowi zagranicznych organizacji religijnych i misjonarzy", to późniejsze sformułowania doktryn i rozważania ekspertów wojskowych na ten temat przybrały kontekst konieczności walki z kolorowymi rewolucjami „jako technologii politycznej ekspansjonizmu Stanów Zjednoczonych i NATO"[8]. Zagrożenie to uruchomiło lawinę opracowań teoretycznych na temat współczesnych wojen informacyjnych, które – jak się podkreśla – prowadzą do „psychologicznej zagłady" ludności oraz katastrofalnych skutków politycznych i społecznych. Stało się wspólnym mianownikiem dla działań podejmowanych przez różne podmioty państwowe (siły zbrojne, służby bezpieczeństwa i porządku publicznego) i publiczno-prywatne (ośrodki i stowarzyszenia analityczne, fundacje itp.). W codziennej praktyce wojskowo-informacyjnej sformułowania w rodzaju „przestępcza ingerencja USA i NATO"[9] stanowią z jednej strony uniwersalny klucz interpretacyjny współczesnych konfliktów zbrojnych, a z drugiej – argument uzasadniający rosyjską interwencję zbrojną na Ukrainie czy w Syrii.

## 4. Kontekst cywilizacyjny

Omawiane dokumenty wpisują się w całokształt współczesnego rosyjskiego myślenia strategicznego ukierunkowanego na rewizję pozimnowojennego

[8] Nie znaczy to, że dziś zrezygnowano z walki ze „światopoglądowymi dywersantami" przeciwstawianymi wyznawcom prawosławia. Licznych przykładów dostarcza twórczość publicystyczno-popularyzatorska Tatjany Graczowej, dziekan Akademii Sztabu Generalnego FR. W wyrażenia w rodzaju „wojująca sieć Watykanu" obfituje np. jej książka: Татьяна Грачева, Память русской души. Алгоритмы геополитики и стратегии тайных войн мировой закулисы, Рязань 2011.

[9] Takiego sformułowania użył prof. Aleksandr Bartosz, członek Akademii Nauk Wojskowych, dyrektor Centrum Informacyjnego Problematyki Bezpieczeństwa Międzynarodowego przy Moskiewskim Uniwersytecie Lingwistycznym, zob. Александр Бартош, Цветные революции и гибридные войны современности; http://nvo.ng.ru/gpolit/2016-01-22/1_revolutions.html

porządku międzynarodowego, czego podstawę ma stanowić odmienność cywilizacyjna (odmienne wartości) tzw. świata rosyjskiego (русский мир), poszerzanego do „świata eurazjatyckiego". Wpisują się też w rosyjską kulturę strategiczną, której niezbywalną cechą jest traktowanie czynnika siły jako środka osiągania celów politycznych. Geopolityczno-cywilizacyjna rywalizacja ze Stanami Zjednoczonymi i ich sojusznikami uwarunkowała znamienną ewolucję rosyjskich dokumentów strategicznych, których raczej powściągliwa retoryka z początku minionej dekady sukcesywnie ustępowała miejsca retoryce konfrontacyjnej. Rywalizacja z wrogiem „sytuacyjnym" (rozszerzenie NATO) przekształciła się w starcie z wrogiem „absolutnym", który kwestionuje rolę Rosji jako liczącego się bieguna siły na świecie. Znalazło to skondensowany wyraz w nowej **Strategii bezpieczeństwa narodowego Federacji Rosyjskiej** (2015), w której zwerbalizowano strategiczne myślenie blokowe. Uznając Stany Zjednoczone „dążące do utrzymania swej dominacji w sprawach globalnych" oraz NATO za głównego przeciwnika, którego „rosnący potencjał siłowy i funkcje globalne stanowią oczywiste pogwałcenie prawa międzynarodowego", w pkt. 14 i 16 wprowadzono pojęcie „regionu euroatlantyckiego", przeciwstawiając go „regionowi eurazjatyckiemu", co umożliwiło z kolei przeciwstawienie geopolitycznej koncepcji eurazjatyckiej – koncepcji euroatlantyckiej, zaś Sojuszu Północnoatlantyckiego – Organizacji Układu o Bezpieczeństwie Zbiorowym (OUBZ). W pkt. 90 podkreślono zarazem: „Rosja dąży do przekształcenia OUBZ w uniwersalną organizację międzynarodową, zdolną do odpowiedzi na zagrożenia wojskowo-polityczne, wojskowo-strategiczne oraz zagrożenia w sferze informacyjnej".

Umieszczenie w Strategii bezpieczeństwa narodowego Federacji Rosyjskiej (po raz kolejny) kwestii rewitalizacji OUBZ („wschodniego NATO") świadczy, że Rosjanie nie wykazują się szczególną inwencją, nie generują nowych idei strategicznych. Jak już wspomniano, wiele koncepcji i idei zapożyczają z doktryn zachodnich. Także wiele rosyjskich koncepcji strategicznych można traktować jako odpowiedź na zachodnie strategie. Zamieszczony na początku 2012 roku na stronie Ministerstwa Obrony dokument **Koncepcja działalności Sił Zbrojnych FR w przestrzeni informacyjnej** był np. odpowiedzią na ogłoszony w 2011 roku dokument **The U.S. Department of Defense Strategy for Operating in Cyberspace**[10].

[10] U.S. Department of Defense Strategy for Operating in Cyberspace, July 2011; www.defense.gov/news/d20110714cyber.pdf

Rosyjska koncepcja nawiązuje do dokumentu Departamentu Obrony USA, który deklarował pięć inicjatyw strategicznych:

- uznanie cyberprzestrzeni za przestrzeń operacyjną sił zbrojnych;
- doskonalenie środków ochrony sieci komunikacyjnej Departamentu Obrony USA;
- partnerstwo państwowo-prywatne na rzecz realizacji strategii cyberbezpieczeństwa;
- kolektywna obrona i kolektywne zapobieganie cyberatakom w ramach NATO i innych układów sojuszniczych;
- innowacyjność (rozwój sił i środków cyberbezpieczeństwa).

Nawiązywała także do przyjętej w tymże roku amerykańskiej **International Strategy for Cyberspace**[11], w której ataki komputerowe na infrastrukturę krytyczną USA zrównano z aktami agresji i wskazywano polityczne oraz wojskowe tego konsekwencje, łącznie z użyciem wszelkich dostępnych sił i środków. Analogicznie do cyberprzestrzeni, przestrzeń informacyjną w dokumencie rosyjskim uznano za pole strategiczne i kolejny teatr działań wojennych. Dla Rosji zastrzeżono „możliwość wyegzekwowania prawa z użyciem wszelkich dostępnych środków wojskowych", podczas gdy analogiczny zapis w strategii amerykańskiej miał w rosyjskich ocenach dowodzić „konfrontacyjnej" strategii USA. O reaktywnym charakterze tych dokumentów świadczy sama chronologia ich pojawienia się:

| **Stany Zjednoczone** | **Federacja Rosyjska** |
|---|---|
| The U.S. Department of Defense Strategy for Operating in Cyberspace (2011) | Koncepcja działalności Sił Zbrojnych FR w przestrzeni informacyjnej (2012) |
| International Strategy for Cyberspace (2011) | Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku (2013) |

[11] https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

## 5. Wewnętrzny i zewnętrzny odbiorca rosyjskiej refleksji strategicznej

Głównym adresatem zachodnich strategii wojskowych są władze poszczególnych krajów. Wojskowi przedstawiają w nich plany działania, wytyczają nowe kierunki tych działań, wskazują istniejące braki. Rosyjskie dokumenty strategiczne są inicjowane odgórnie, co znajduje wyraz w stosownych dekretach prezydenta Putina[12]. Są elementem szerszej strategii informacyjnej Kremla i mają konkretnych adresatów, zarówno wewnętrznych, jak i zewnętrznych. Antyzachodnia retoryka jest wykorzystywana jako środek w polityce wewnętrznej: wcześniej budowała np. zapotrzebowanie obywateli na silne państwo, cieszące się autorytetem na arenie międzynarodowej, dziś buduje gotowość mobilizacyjną społeczeństwa, umacniając poczucie zagrożenia ze strony Zachodu.

Drugim odbiorcą jest opinia publiczna w krajach WNP. Jej pozyskanie ma ułatwić realizację geopolitycznych celów Kremla, takich jak: utrzymanie wpływów na obszarze b. ZSRR czy zapobieganie integracji państw postradzieckich z Zachodem. Oba te wymiary – wewnętrzny i regionalny – są ściśle ze sobą splecione, co umożliwia wspomniana wyżej koncepcja świata eurazjatyckiego. W rezultacie obrona przed tzw. czwartym zagrożeniem jest przedstawiana jako obrona wspólnoty cywilizacyjnej przed wtargnięciem obcego kodu kulturowego. Stosuje się przy tym ten sam typ narracji budowanej na przeciwstawieniu „swój – obcy". Wikłając kraje WNP w ściślejszą współpracę wojskową, Kreml wzmacnia narzędzia dominacji na obszarze postradzieckim i straszy je konsekwencjami polityki wielowektorowej, uwzględniającej inne niż integracja z Rosją kierunki. Ostatnio, dążąc do poszerzenia grona sojuszników, Rosjanie przedstawiają się jako obrońcy „narodowej suwerenności w globalnej przestrzeni informacyjnej". Stosowne pojęcie odnajdujemy w projekcie nowej **Doktryny bezpieczeństwa informacyjnego FR**, gdzie zdefiniowano je jako „zdolność państwa do prowadzenia samodzielnej i niezależnej polityki w globalnej przestrzeni informacyjnej w celu obrony własnych interesów

[12] W tym kontekście można przytoczyć ujawnioną w części **Koncepcję państwowego systemu wykrywania, uprzedzania i likwidacji skutków ataków komputerowych** z 12 grudnia 2014 roku (Nr K 1274), a opracowaną na podstawie stosownego dekretu prezydenta Władimira Putina z 15 stycznia 2013 roku o stworzeniu państwowego systemu monitoringu, uprzedzania i likwidacji skutków ataków komputerowych na zasoby informacyjne Federacji Rosyjskiej. Na marginesie: instytucjonalnym koordynatorem systemu centrów terytorialnych jest Federalna Służba Bezpieczeństwa, wiadomo także, że poszczególne części systemu, w tym Siły Zbrojne Federacji Rosyjskiej, mogą tworzyć własne centra, które pozostają w sferze ich wyłącznej odpowiedzialności.

narodowych i przestrzeni informacyjnej". Do odbiorcy wewnętrznego i regionalnego było adresowane rozszerzenie w doktrynie wojennej z 2010 roku zakresu użycia siły o obronę ludności rosyjskojęzycznej. Zabieg miał podwójny cel: wzmagał presję na kraje z najbliższego sąsiedztwa i mobilizował rosyjskojęzycznych obywateli tych krajów, obywateli Federacji Rosyjskiej zaś umacniał w przekonaniu, że silne państwo skutecznie broni ich interesów.

Trzecią grupą odbiorców są liderzy opinii na Zachodzie czy szerzej – międzynarodowa opinia publiczna. Rosyjskie dokumenty tzw. planowania strategicznego są przez ekspertów zewnętrznych traktowane jako wiarygodne źródło do analizy rosyjskiej percepcji zagrożeń i rzeczywistych intencji rosyjskich władz wojskowych i politycznych. Warto jednak pamiętać, że – jak wszystkie informacje dotyczące resortów bezpieczeństwa i obrony Rosji – podlegają one ograniczeniom proceduralnym wynikającym ze ścisłego reżimu ochrony tajemnicy państwowej. Narzuca to zasadę ograniczonego zaufania do publicznych dokumentów i oficjalnych oświadczeń wojskowych. Ich podstawowym celem jest, jak się wydaje, kształtowanie wśród potencjalnych przeciwników Rosji przekonania o nieskuteczności, a zatem bezprzedmiotowości wszelkich form nacisku na Rosję i jej sojuszników. Z tego względu stanowią one raczej instrument dyplomacji i propagandy wojskowej niż deklarację rzeczywistych intencji.

W zderzeniu z praktyką użycia sił zbrojnych uzasadnioną nieufność wobec rosyjskich dokumentów strategicznych budzi także ich „obronna" retoryka, niezmiennie podkreślająca pokojowe intencje Rosji, działania zgodne z prawem międzynarodowym, dążenie do demilitaryzacji przestrzeni informacyjnej czy apele o zaprzestanie wyścigu zbrojeń informacyjnych. Taka narracja towarzyszy także działaniom sił zbrojnych podporządkowanym jawnej konfrontacji geopolitycznej, jak np. na Ukrainie czy w Syrii. Sekretarz Rady Bezpieczeństwa Federacji Rosyjskiej Nikołaj Patruszew w tym kontekście oświadczył np.: „Stany Zjednoczone przy wsparciu państw Zachodu zamierzają utrzymać swą dominację w sprawach globalnych i dążą do ograniczenia możliwości prowadzenia przez Federację Rosyjską samodzielnej polityki wewnętrznej i zagranicznej"[13].

[13] Вызов принят, Николай Патрушев: подготовлена обновленная Стратегия национальной безопасности РФ, *Российская Газета*, 22.12.2015, http://rg.ru/2015/12/22/patrushev-site.html

## 6. Nowe trendy?

Ostatnio w rozważaniach rosyjskich wojskowych (choć nie w głównym ich nurcie) pojawiają się anglosaskie terminy „cyberstrategia", „cyberzagrożenia", „cyberprzestrzeń", „cyberwojna". Do debaty publicznej wprowadzają je naukowcy, dyplomaci apelujący o „internacjonalizację wysiłków na rzecz cyberrozbrojenia" oraz politycy, np. szefowa komitetu Dumy ds. bezpieczeństwa Irina Jarowaja w kontekście „suwerenności cyfrowej" Rosji czy nadzorujący rosyjską zbrojeniówkę wicepremier Dmitrij Rogozin, który w marcu 2012 roku zapowiedział powołanie rosyjskiego cyberdowództwa na wzór U.S. CyberCom. Z inicjatywy Rogozina nagłośniono powołanie Fundacji Badań Perspektywicznych (w jego ocenie – rosyjskiej DARPA[14]). Z wykładu wicepremiera wygłoszonego w ramach tzw. platformy patriotycznej Jednej Rosji[15] wynika jednak, że „cyberzagrożenia" Rogozin traktuje jako tożsame z „zagrożeniami informacyjnymi", propagandowo rozgrywając stereotyp „suwerenności cyfrowej" (tj. rosyjskiej samowystarczalności technologicznej). Należy też odnotować, że mimo podejmowanych prób[16] cyberstrategia do dziś nie stała się przedmiotem odrębnej refleksji doktrynalnej. Tego rodzaju próby przełamania tradycji terminologicznej (którą zdominował przymiotnik „informacyjny") nie oznaczają zmiany podejścia rosyjskich strategów wojskowych do danej problematyki: nadal podkreślają oni priorytet zagrożeń związanych ze społeczno-politycznymi aspektami walki informacyjnej, a nie zagrożeń cybernetycznych, mających bezpośredni charakter wojskowy. Oznaczają natomiast, że apele wojskowych i ekspertów dotyczące umocnienia wojskowo-strategicznego cyberpotencjału Rosji znajdują zrozumienie na szczytach władzy[17]. Mogą także oznaczać, że

[14] DARPA (Defense Advanced Research Projects Agency) – istniejąca od 1958 roku amerykańska agencja powołana do rozwoju badań kluczowych technologii wojskowych. Rosyjska Fundacja Badań Perspektywicznych (http://fpi.gov.ru) została powołana pod koniec 2012 roku, na jej czele stanął gen. Andriej Grigorjew, b. szef Federalnej Służby Kontroli Technicznej i Eksportu, odpowiedzialnej w Rosji za techniczną stronę bezpieczeństwa informacyjnego Federacji Rosyjskiej. Fundacja organizuje i finansuje badania w zakresie technologii wojskowych i technologii podwójnego przeznaczenia.

[15] Лекция Рогозина в рамках проекта партии «Гражданский университет»; http://er.ru/news/102261/

[16] W latach 2012–2014 z inicjatywą na forum Rady Federacji wystąpił działacz Jednej Rosji Rusłan Gattarow; Комиссия СФ инициирует обсуждение стратегии кибербезопасности РФ; http://ria.ru/defense_safety/20140110/988508179.html

[17] Pośrednio potwierdza to wypowiedź ministra telekomunikacji Nikołaja Nikiforowa, który podczas ubiegłorocznego forum młodzieżowego „Tauryda" pod Sewastopolem na Krymie ujawnił, że do „pełnej suwerenności cyfrowej" Rosji brakuje miliona programistów. Minister przypomniał też założenia opublikowanej w 2013 roku **Strategii rozwoju przemysłu technologii informacyjnych Federacji Rosyjskiej na lata 2014–2020 i perspekty-**

postulat rozwoju cyberpotencjału Rosji jest instrumentem konkretnych lobbies w rosyjskiej zbrojeniówce i elit siłowych[18].

## 7. Podejście systemowe

Rosyjskie dokumenty, będąc elementem strategii informacyjnej (w tym wojskowej), pełnią inne funkcje niż ich odpowiedniki na Zachodzie.

Funkcja **prognostyczna** wskutek zmanipulowania stanu sytuacji międzynarodowej jest tu zepchnięta na margines. Na plan pierwszy wysunięto natomiast inne funkcje:

- **światopoglądową** (pokazuje miejsce Rosji w świecie i jej zmagania z głównymi globalnymi ośrodkami siły),
- **metodologiczną** (kształtuje spójne podejście do rozwiązywanych przez Kreml problemów w polityce wewnętrznej i zagranicznej),
- **edukacyjną** czy **dydaktyczną** (kształtuje morale armii i społeczeństwa, poszerza potencjał mobilizacyjny),
- **mobilizacyjną** (służy wykorzystaniu wszystkich możliwych sił i środków oraz zarządzaniu tym potencjałem).

Podejście systemowe umożliwia z jednej strony demonstrację siły, a z drugiej – stosowanie niewojskowych środków walki (politycznych, ekonomicznych, informacyjnych, humanitarnych, dyplomatycznych i innych), a także działań niebezpośrednich (sankcje, blokada szlaków komunikacyjnych, zastraszanie użyciem siły, sabotaż, dywersja itp.). W doktrynie wojennej z 2014 roku odnajdujemy je na przykład w części poświęconej współczesnym konfliktom zbrojnym, które charakteryzują m.in. „kompleksowe użycie sił zbrojnych, jak również politycznych, ekonomicznych, informacyjnych i innych środków

**wy na okres 2025 roku** (Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года, http://www.minsvyaz.ru/ru/documents/4084/), zgodnie z którą w 2020 roku liczba programistów w Rosji ma osiągnąć 700 tysięcy.

[18] Znamienny fakt: założycielami i wydawcami wychodzącego od 2014 roku kwartalnika *Вопросы кибербезопасности* (www.cyberrus.com) są zamknięta spółka akcyjna pod nazwą Naukowo-Produkcyjne Zjednoczenie „Eszełon" (http://npo-echelon.ru/) oraz Naukowe Centrum Informacji Prawnej przy Ministerstwie Sprawiedliwości.

niewojskowych, realizowanych przy szerokim wykorzystaniu potencjału protestu i sił operacji specjalnych (...)". W Podstawach polityki państwa w dziedzinie międzynarodowego bezpieczeństwa informacyjnego do roku 2020 znajdujemy z kolei sformułowanie, iż dokument powstał m.in. „w celu zorganizowania współpracy międzyresortowej przy realizacji państwowej polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego, a także osiągnięcia parytetu technologicznego z czołowymi mocarstwami globalnymi w rezultacie upowszechnienia technologii informacyjnych i komunikacyjnych w realnym sektorze gospodarki" (pkt 5). Podejście systemowe uwypuklono w Koncepcji działalności Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej, gdzie ustanowiono zasadę ścisłego współdziałania armii i służb specjalnych w obrębie jednolitego systemu bezpieczeństwa informacyjnego Federacji Rosyjskiej[19].

Należy odnotować, że system bezpieczeństwa informacyjnego Federacji Rosyjskiej z trudem poddaje się opisowi. Wynika to z różnych przyczyn. Po pierwsze, bezpieczeństwo informacyjne jest obszarem transsektorowym, tj. dotyczy różnych dziedzin: obrony, bezpieczeństwa, dziedziny społecznej, gospodarki, kultury itp. Po drugie, misję działania na rzecz bezpieczeństwa informacyjnego Rosji powierzono wielu instytucjom i organom państwowym. **Szkielet systemu współtworzą służby specjalne, siły zbrojne, formacje policyjne, część administracji, ale także zaplecze eksperckie, szkoleniowe, badawcze i produkcyjne. Państwowy system dopełnia prywatny sektor bezpieczeństwa, ściśle z nim współpracujący. Efekt synergii zapewniają wzajemne zależności między nimi oraz narzucona im prawnie konieczność współdziałania.**

Każdy z zarysowanych wyżej segmentów systemu ma specyficzne cechy związane z przypisanym mu obszarem odpowiedzialności. Wśród struktur bezpieczeństwa informacyjnego można znaleźć instytucje działające niejawnie (służby wywiadowcze), jak i w pełni transparentnie (np. Państwowa Służba

[19] Manifestacją tej zasady w praktyce są nagłaśniane od 2014 roku ćwiczenia Ministerstwa Obrony, Federalnej Służby Bezpieczeństwa, Ministerstwa Łączności, MSW i in., podczas których ocenia się ryzyka związane z oddziaływaniem zewnętrznym na rosyjską przestrzeń informacyjną. Ministerstwo Obrony było ponadto inicjatorem I Międzyresortowej Konferencji „System międzyresortowego współdziałania informacyjnego", która odbyła się 19 listopada 2015 roku. Z inicjatywy ministra Siergieja Szojgu pojawił się też prezydencki dekret o trybie zbierania informacji w kwestiach obrony Federacji Rosyjskiej i wymiany tej informacji z września 2014 roku (http://stat.ens.mil.ru/science/conference/smiv2015/about.htm).

Nadzoru w zakresie Łączności, Technologii Informacyjnych i Komunikacji Masowych[20]). Niektóre formacje mają ogromne kompetencje i szeroki katalog zadań, inne są ściśle wyprofilowane. Dotyczy to także segmentów składowych systemu bezpieczeństwa informacyjnego, którym autonomicznie zarządza resort obrony[21].

[20] Ros. Госкомнадзор. Służba podlega Ministerstwu Łączności i Komunikacji Masowych. Prowadzi m.in. rejestry operatorów łączności, rejestry środków masowego przekazu, wydaje zgodę na działalność mediów i zakazuje ich działalności (w tym portali internetowych i blogów), wydaje zgodę na publikacje wydawnictw zagranicznych na terytorium Federacji Rosyjskiej itp.

[21] Na przykład Narodowe Centrum Obrony wyposażono w wiele funkcji, łączy ono bowiem elementy systemu dowodzenia, kontroli, łączności, rozpoznania, integrując systemy dowodzenia z systemami rozpoznania i logistyki; służy także jako wideokonferencyjne centrum informacji i propagandy wojskowej, podczas gdy tworzona przy Centralnym Archiwum Wojskowym kompania naukowców została powołana do demistyfikacji fałszowania historii rosyjskiej wojskowości.

## III. DZIAŁANIA SYSTEMU INFORMACYJNEGO NA POZIOMIE OPERACYJNYM – *CASE STUDY*

Wojskowa polityka informacyjna jest częścią militarystycznej polityki Kremla. Jej bezpośrednie konsekwencje przejawiają się w militaryzacji języka polityki i propagandy, narzucaniu opinii publicznej swoistego stanu wojennego czy diametralnej zmianie wizerunku rosyjskiej armii. Armia przestała być *lumpenmilitariatem* i negatywnym bohaterem (do czego doprowadziły m.in. wojny w Czeczenii). Obecnie jest postrzegana jako główny filar mocarstwowej Rosji, silnego państwa. Przede wszystkim jednak zaowocowała przejściem do działań ofensywnych i uprzedzających. Rosja siłą domaga się respektowania swoich stref wpływów w sąsiedztwie (agresja wobec Ukrainy, interwencja zbrojna w Syrii). Burząc europejską i globalną architekturę bezpieczeństwa, przedstawia się zarazem jako gwarant procesów pokojowych. Wykorzystując czynnik siły do budowy swej pozycji międzynarodowej, daje do zrozumienia, że o rozwiązaniu tych konfliktów Zachód powinien rozmawiać przede wszystkim z Rosją (aby uniknąć wielkiej wojny). Forsując odrębne podejście do problematyki międzynarodowego bezpieczeństwa informacyjnego, manifestuje swe prawo do współdecydowania w kwestiach bezpieczeństwa globalnego.

Niżej przedstawiamy wybrane przykłady działań informacyjnych rosyjskiego systemu informacyjnego, ze szczególnym uwzględnieniem jego wojskowego segmentu

(1) na poziomie globalnym,
(2) na poziomie regionalnym oraz
(3) na poziomie krajowym.

Wychodzimy przy tym z założenia, że dopiero analiza działań operacyjnych umożliwia zidentyfikowanie długo- i krótkoterminowych celów strategicznych Rosji. Te z kolei unaoczniają ogromny rozziew między myślą wojskową a praktyką działań informacyjnych Sił Zbrojnych Federacji Rosyjskiej.

### 1. Cele współpracy międzynarodowej w przestrzeni informacyjnej

Od lat Rosja lansuje na arenie międzynarodowej własne koncepcje bezpieczeństwa informacyjnego i podejmuje inicjatywy, które przedstawia jako swój wkład w doktrynę globalnego bezpieczeństwa informacyjnego[22]. W Koncepcji

[22] Zob. np. Бедрицкий А.В., Информационное доминирование» США и асимметричное информационное противоборство / США и Канада: экономика, политика, культура. –

działalności Sił Zbrojnych FR w przestrzeni informacyjnej znalazło to wyraz w części dotyczącej powstrzymywania strategicznego, w zapisie: „Głównym celem współpracy międzynarodowej jest ustanowienie międzynarodowego systemu prawa regulującego działania państw w globalnej przestrzeni informacyjnej, z działaniami militarnymi włącznie". Zewnętrzny kontekst problematyki ma tutaj dwie płaszczyzny: globalną i regionalną („Siły Zbrojne Federacji Rosyjskiej priorytetowo traktują współpracę z krajami Układu o Bezpieczeństwie Zbiorowym, Wspólnoty Niepodległych Państw i Szanghajskiej Organizacji Współpracy, będą zwiększać liczbę partnerów i rozwijać współpracę na bazie wspólnego interesu").

Lakoniczne sformułowania dokumentów strategicznych nie pozwalają zidentyfikować szerszych celów polityczno-wojskowych Rosji w jej relacjach ze światem zewnętrznym. Manifestowane cele strategiczne mijają się ponadto z celami realizowanymi w praktyce. Rzeczywiste cele wyłaniają się raczej z tych części dokumentów, które przybliżają percepcję zagrożeń (wśród których na pierwszym miejscu wymieniane są zagrożenia informacyjne świadczące jakoby o ingerencji w wewnętrzne sprawy Rosji i wymierzone przeciwko jej żywotnym interesom, a pochodzące z Zachodu, rozumianego przede wszystkim jako USA i NATO) bądź omawiają kwestię użycia siły dla przeciwdziałania zagrożeniom. Ta ostatnia wydaje się kluczowa: w kolejnych dokumentach zakres użycia siły poszerzano, początkowo o kontekst bezpieczeństwa regionalnego (obrona obywateli rosyjskojęzycznych), by przejść do użycia siły w celu osiągnięcia celów w polityce międzynarodowej. Zagrożenia informacyjne są przy tym przedstawiane jako bezpośrednie źródło konfliktu, do którego rozstrzygnięcia można użyć wszelkich możliwych sił i środków.

Przedmiotem szczególnej troski rosyjskich strategów jest militarna i technologiczna przewaga Stanów Zjednoczonych i ich sojuszników, w tym – używając rosyjskiej terminologii – w sferze informacyjnej. Znalazło to wyraz w dokumencie z 24 lipca 2013 roku **Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku**[23], będącym odpowiedzią na analogiczną amerykańską strategię. Prezentując własne podejście, Rosja zgłasza *votum separatum* wobec amerykańskiej

М. : ИСКРАН, 2007. – № 2. – С. 91–102; Бедрицкий А.В., Международные договоренности по киберпространству – возможен ли консенсус; http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf

[23] Zob. Основы государственной политики Российской Федерации в области международной информационной безопасности..., *op. cit.*

wizji, podzielanej – co się podkreśla – przez Europę. Dokument szkicuje główne wektory aktywności Rosji na arenie międzynarodowej: budowanie systemu międzynarodowego bezpieczeństwa informacyjnego, kształtowanie mechanizmów współpracy międzynarodowej w tym zakresie oraz budowanie szerokiego frontu poparcia rosyjskich inicjatyw na rzecz internacjonalizacji zarządzania Internetem i Międzynarodowym Związkiem Telekomunikacyjnym (ITU)[24]. Deklaruje także ścisłą współpracę Rosji z jej sojusznikami, przede wszystkim członkami Szanghajskiej Organizacji Współpracy, Organizacji Układu o Bezpieczeństwie Zbiorowym, WNP i BRICS (grupa państw skupiająca Brazylię, Rosję, Indie, Chiny i Republikę Południowej Afryki).

Język tego dokumentu wyraźnie nawiązuje do retoryki zimnowojennej: jak dawniej ZSRR, tak teraz Rosja walczy nie tylko o demilitaryzację kosmosu i apeluje o zahamowanie wyścigu zbrojeń, ale zabiega także o internacjonalizację globalnej przestrzeni informacyjnej, nieproliferację broni informacyjnej oraz o utrzymanie suwerenności informacyjnej państw, zarówno informacyjno-technologicznej (osiągnięcie technologicznego parytetu, pokonanie nierówności w tej dziedzinie między państwami rozwiniętymi i rozwijającymi się), jak i ich suwerenności politycznej (kilkakrotnie pojawia się zwrot: „akty agresji informacyjnej ukierunkowane na dyskredytację suwerenności państw").

Towarzyszące dokumentowi działania można potraktować jako przejaw operacjonalizacji strategicznych celów Rosji. „Inicjatywę strategiczną" wzmocniono instytucjonalnie: koordynatorem działalności na rzecz międzynarodowego bezpieczeństwa informacyjnego został MSZ. Na Kremlu powołano dodatkowo urząd pełnomocnego przedstawiciela prezydenta do spraw międzynarodowego bezpieczeństwa informacyjnego: został nim dyplomata Andriej Krutskich.

[24] Ofensywę dyplomatyczną na rzecz rewizji dotychczasowego systemu administrowania siecią globalną Rosja podjęła na forum ONZ już w minionej dekadzie. Zintensyfikowała ją podczas przygotowań i w trakcie Światowego Szczytu Telekomunikacyjnego w Dubaju (grudzień 2012). W koalicji z Chinami zabiega o prawnomiędzynarodowe uregulowanie Internetu pod egidą Międzynarodowego Związku Telekomunikacyjnego (ITU – wyspecjalizowana agenda ONZ do standaryzacji i regulacji światowego rynku telekomunikacyjnego). Kluczowy postulat sprowadza się do wyprowadzenia rejestrów domenowych z gestii ICANN, Internetowej Korporacji do Nadawania Nazw i Numerów (międzynarodowa organizacja *non profit* z siedzibą w Los Angeles, powstała w 1998 roku. Przejęła zarządzanie Internetem z rąk rządu USA) i przekazania ich w gestię rządów. Zgodnie z propozycją Federacji Rosyjskiej, państwa członkowskie ITU powinny mieć suwerenne prawo do zarządzania Internetem na swoim terytorium i większej nad nim kontroli, ITU zaś winien nadzorować problematykę bezpieczeństwa cyberprzestrzeni i zwalczania cyberprzestępczości.

Jak ujawnił *Kommiersant*, „Rada Bezpieczeństwa i stosowne zaangażowane resorty otrzymały polecenie przedstawienia prezydentowi konkretnych propozycji w zakresie realizacji Podstaw"[25]. W samym dokumencie czytamy: „polityka państwa w tym zakresie będzie realizowana przez federalne organy władzy wykonawczej, zgodnie z ich kompetencjami, (...), a także w ramach partnerstwa publiczno-prywatnego".

Opublikowanie dokumentu w żadnej mierze nie oznaczało przystąpienia do realizacji zawartych w nim postulatów. To strategiczne zadanie jest realizowane co najmniej od początku obecnego stulecia. Należy zatem sądzić, że chodziło raczej o podtrzymanie ciągłości akcji informacyjnej i rozszerzenie jej na arenę regionalną. Świadczy o tym zorganizowana aktywność środowiska ekspercko-analitycznego: liczne publikacje, w tym przeznaczone dla odbiorcy zagranicznego[26], a także konferencje poświęcone tej problematyce w Moskiewskim Państwowym Instytucie Spraw Międzynarodowych (MGIMO), Rosyjskim Instytucie Badań Strategicznych (RISI) i in. Analogiczne kampanie informacyjne towarzyszyły promocji projektu **Konwencji ONZ o zapewnieniu międzynarodowego bezpieczeństwa informacyjnego** (2011) oraz zgłoszonego w ONZ przez Rosję i Chiny (przy poparciu Tadżykistanu i Kirgistanu) projektu **Zasad postępowania w zakresie międzynarodowego bezpieczeństwa informacyjnego** (2011). Ich treść nie różni się od treści Podstaw: łączy je idea, iż wojna informacyjna jest przestępstwem przeciwko pokojowi na świecie i bezpieczeństwu międzynarodowemu. Projekty oenzetowskich dokumentów kreślą szeroko ujmowane zagrożenia w przestrzeni informacyjnej (obok cyberterroryzmu i cyberprzestępczości zaliczono do nich: nieposzanowanie kultury, historii i systemów społecznych krajów, rozprzestrzenianie broni informacyjnej, ograniczanie dostępu do najnowszych technologii IT) oraz definiują zasady międzynarodowego bezpieczeństwa informacyjnego (m.in. takie jak: niwelowanie różnic w zakresie poziomu informatyzacji państw, prawo do stanowienia suwerennych norm prawnych i zarządzania przestrzenią informacyjną na własnym terytorium, zasada jurysdykcji terytorialnej w zakresie

[25] Елена Черненко, Мир домену твоему. Россия определилась с информационной безопасностью, *Коммерсант*, 1.08.2013; http://www.kommersant.ru/doc/2245463

[26] W towarzyszącej dokumentowi akcji propagandowej stanowisko Rosji przeciwstawiano konfrontacyjnemu podejściu Stanów Zjednoczonych, które stawiają sobie za cel „zapewnienie własnej wyższości i globalnej dominacji w przestrzeni cybernetycznej (...). Rosja nie dąży do dominowania w cyberprzestrzeni. Zamiast tego nalega na przyjęcie w tej sferze ogólnych zasad postępowania, które pozwoliłyby uniknąć cyberprzestępstw i cyberzagrożeń"; http://pl.sputniknews.com/polish.ruvr.ru/2013_08_02/Rosja-okreslila-koncepcje-cyberbezpieczenstwa/

penalizacji przestępstw informacyjnych, zasada nieingerencji w przestrzeń informacyjną państw itp.).

Do sformułowania tych zasad przyczynili się eksperci Ministerstwa Obrony Rosji, którzy od dawna zapowiadają objęcie cyberprzestrzeni dorobkiem prawa międzynarodowego, w tym międzynarodowego prawa wojennego[27], argumentując, że użyciu „broni informacyjnej" sprzyja brak przepisów regulujących jej stosowanie. Uczestniczą także w różnych konferencjach w kraju i za granicą, np. dorocznych konferencjach poświęconych problematyce międzynarodowego bezpieczeństwa informacyjnego w Garmisch-Partenkirchen w Bawarii, których Rosja jest współorganizatorem[28]. Ze skąpych informacji wynika ponadto, że w przygotowaniu strategicznych dokumentów uczestniczy Centrum Badań Wojskowo-Strategicznych przy Sztabie Generalnym Sił Zbrojnych FR[29].

Zachód nie poparł inicjatyw Rosji, upatrując w nich instrument do zaostrzenia kursu wewnętrznego: walki z wolnością słowa i ograniczania dostępu do Internetu. Wewnętrzna i zewnętrzna opinia publiczna niezmiennie natomiast otrzymuje komunikaty, że Rosja jest mocarstwem informacyjnym i inicjatorem międzynarodowych rozwiązań powstrzymujących informacyjny wyścig

[27] Zob. np. S.A. Komov, S.V. Korotkov, S.N. Rodionov International Information Security: Military Aspects. Military Thought, volume 12, number 4, 2003, p. 1–5; I.N. Dylevsky, S.A. Komov, S.V. Korotkov, Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law. Disarmament Forum, ICTs and international Security, number 3, 2007, p. 35–43; S.M. Boyko, I.N. Dylevsky, S.A. Komov, S.V. Korotkov, S.N. Rodionov, On International Legal Qualifications of Information Operations. Military Thought, volume 17, number 1, 2008, p. 15–25; International Information Security: Problems And Decisions, Shapter 3, Military-Political Aspects For Provision of International Information Security, Edited by Komov S.A., Moscow 2011.

[28] Представители МО РФ о применимости норм и принципов международного права к военной деятельности в информационном пространстве, https://digital.report/predstaviteli-mo-rf-o-primenimosti-norm-i-printsipov-mezhdunarodnogo-prava-k-voennoy-deyatelnosti-v-informatsionnom-prostranstve/; Анатолий Стрельцов о проблемах адаптации международного права к информационным конфликтам, https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/

[29] Zob. np. Александр Пинчук, Центр военно-стратегической мысли, 26.01.2010, http://old.redstar.ru/2010/01/26_01/2_02.html. Zob. także С.Г. Чекинов, Центр военно-стратегических исследований Генерального Штаба Вооруженных Сил Российской Федерации: история и современность, *Военная Мысль*, № 1/2010, стр. 3–5. Pułkownik Czekinow, szef Centrum, wiąże jego pojawienie się w 1985 roku z zasadniczą zmianą sytuacji w związku z rozpoczęciem procesu redukcji strategicznych potencjałów jądrowych. „Towarzyszyło temu wdrażanie systemów wysokoprecyzyjnej broni konwencjonalnej, militaryzacja kosmosu i aktywna walka informacyjna (...), bowiem wraz z transformacją zimnej wojny w jej nowe formy i sposoby sprzeczności międzypaństwowe nie tylko nie osłabły, ale jeszcze bardziej się zaostrzyły".

zbrojeń. W lipcu 2015 roku podczas Eurazjatyckiego Infoforum w Sewastopolu przedstawiciel prezydenta Rosji ds. międzynarodowego bezpieczeństwa informacyjnego Andriej Krutskich oświadczył, że zaproponowane przez Rosję bazowe zasady postępowania w sieciach globalnych zostały zaaprobowane przez ekspertów ONZ. O rosyjskim sukcesie w tej dziedzinie świadczą w jego opinii także porozumienia o współpracy w dziedzinie międzynarodowego bezpieczeństwa informacyjnego podpisane podczas ostatniego szczytu BRICS, a wcześniej w ramach Szanghajskiej Organizacji Współpracy i Organizacji Układu o Bezpieczeństwie Zbiorowym. Dało mu to asumpt do konkluzji, iż „Rosja połączyła dwie trzecie świata wspólną logiką zapobiegania wojnom informacyjnym"[30].

Bardziej wnikliwa analiza tych inicjatyw wskazuje, że Rosji chodzi nie tyle o współpracę międzynarodową, ile o zakwestionowanie istniejącego porządku prawnomiędzynarodowego. Zamiast deklarowanej współpracy rosyjscy stratedzy budują krańcową nieufność wobec USA. Określają w ten sposób miejsce Rosji w nowym porządku na świecie, rezerwując dla niej prawo do współdecydowania w kwestiach bezpieczeństwa globalnego. Taką tezę potwierdza też analiza rosyjskich dokumentów strategicznych w ich warstwie symbolicznej, jako zespół argumentów, typu narracji czy stereotypów. Doktrynalne konstrukcje w rodzaju „wojna informacyjna", „broń informacyjna", „dominująca pozycja Stanów Zjednoczonych na świecie", „wyścig zbrojeń", „parytet technologiczny" czy „demilitaryzacja przestrzeni informacyjnej" nie tworzą warunków do konstruktywnego dialogu, podobnie jak sama terminologia z przymiotnikiem „informacyjny", utrudniająca zbliżenie podejść zachodniego i rosyjskiego. Świadczą, iż – eskalując niekonstruktywne działania – Rosja w gruncie rzeczy nie ma pozytywnego programu współpracy: taki program winien być bowiem budowany na wspólnych celach.

## 2. Poziom regionalny: na wzór radziecki?

Trendy obserwowane w środowisku bezpieczeństwa na obszarze postradzieckim są dla Rosji niekorzystne; o wpływy w regionie rywalizują z nią USA, UE,

[30] Евразийские форумы «Инфофорум-Евразия», http://infoforum.ru/main/evraziiskie-forymy-infoforym-evraziia. Jak poinformowano, organizatorami ostatniego forum eurazjatyckiego były: Komitet Dumy Państwowej ds. Bezpieczeństwa, Narodowe Forum Bezpieczeństwa Informacyjnego „Infoforum", przy wsparciu aparatu pełnomocnego przedstawiciela prezydenta FR do spraw międzynarodowego bezpieczeństwa informacyjnego, aparatu Rady Bezpieczeństwa FR, MSW, FSB, MSZ, Organizacji Układu o Bezpieczeństwie Zbiorowym, władz Sewastopola i Republiki Krym.

Chiny, Turcja, Iran i in. Większość państw regionu nie odczuwa zewnętrznego zagrożenia militarnego. Jedność strategicznego obszaru obronnego leży więc głównie w interesie Rosji. Ponadto obszar WNP nie stanowi dziś wspólnoty geopolitycznej i cywilizacyjnej. Na Kaukazie Południowym rosyjskie wpływy cywilizacyjne kurczą się na rzecz Turcji, w Europie Wschodniej – na rzecz UE. Na całym obszarze następuje erozja ekonomicznych i częściowo wojskowych wpływów Rosji na rzecz Chin, których strategiczne inicjatywy (np. Jedwabny Szlak) czynią z nich atrakcyjne centrum przyciągania. Kontrolę nad regionem Rosja niezmiennie traktuje jako potwierdzenie swego statusu mocarstwa i mechanizm tworzący bariery dla polityki wielowektorowej krajów regionu i ich integracji ze strukturami przez Moskwę niekontrolowanymi. Z tego względu we wszystkich omówionych dokumentach podkreślono pierwszoplanowe znaczenie polityki Rosji wobec WNP i ścisłej współpracy wojskowej z regionalnymi organizacjami.

**Strategiczne cele swej polityki na tym obszarze Rosja określiła tuż po rozpadzie ZSRR**. Są to:

- zachowanie wspólnej przestrzeni obronnej,
- utrzymanie jednolitej przestrzeni cywilizacyjno-kulturowej,
- obrona praw ludności rosyjskojęzycznej,
- kontrola wydobycia i transportu surowców energetycznych,
- ochrona granic zewnętrznych WNP,
- przeciwdziałanie wpływom innych państw.

W sferze obronnej skupiono się na:

- utrzymaniu kontroli nad instalacjami wojskowymi b. ZSRR i obecności wojskowej w kluczowych punktach,
- zarządzaniu regionalnymi konfliktami,
- zagwarantowaniu monopolu Rosji na posiadanie broni jądrowej (dla sojuszników gwarancje jądrowe są dziś głównym argumentem na rzecz wojskowej współpracy z FR).

Współpracę tę Rosja prowadzi wielotorowo: w ramach WNP, Organizacji Układu o Bezpieczeństwie Zbiorowym i Szanghajskiej Organizacji Współpracy, a także porozumień dwustronnych, tworząc powielające się mechanizmy konsultacyjne i wykonawcze (można się np. zastanawiać, czemu służy podpisane w 2013 roku z Białorusią porozumienie o współpracy w dziedzinie międzynarodowego bezpieczeństwa informacyjnego, skoro podpisała analogiczne

dokumenty w ramach OUBZ i WNP). Oprócz środków wojskowych (które w 2008 i 2014 roku poszerzyła o użycie siły w celu obrony obywateli rosyjskojęzycznych w Gruzji i na Ukrainie), do realizacji tych celów Rosja uruchomiła całe spektrum środków politycznych i ekonomicznych. Słowem – strategiczna ofensywa jest prowadzona na wielu frontach, w tym informacyjnym.

Na **informacyjnym froncie cywilizacyjnym** należy sytuować wspomniane wyżej Eurazjatyckie Infoforum. Jest ono jedną z wielu informacyjnych platform integracyjnych Rosji na obszarze b. ZSRR. W ostatnich latach ich liczba wzrosła. Przy MGIMO powołano w 2012 roku Centrum Badań Wojskowo-Politycznych, którego produktem są dwa portale pod nazwą „Obrona eurazjatycka"[31]. W kwartalniku kremlowskiego Rosyjskiego Instytutu Badań Strategicznych (RISI) *Problemy Nacyonalnoj Stratiegii*[32] pojawiła się rubryka „Nowa Eurazja". W 2013 roku utworzono portal eurasiancenter.ru przy Agencji Rossija Siegodnia, w 2015 powołano agencję informacyjną Eurasia Daily[33].

W ramach tzw. partnerstwa publiczno-prywatnego nowe platformy obudowano szeregiem inicjatyw „społecznych". Instytut OUBZ powołał niedawno Stowarzyszenie Analityczne OUBZ i Młodzieżową Szkołę OUBZ[34]. Celem tych projektów jest koordynowanie działalności naukowców, politologów, ekspertów i liderów młodzieżowych organizacji politycznych i społecznych z państw członkowskich na rzecz wspólnej polityki informacyjnej, lobbingu interesów Rosji i udziału w kampaniach antyzachodnich. Koordynatorem Stowarzyszenia jest *notabene* znany teoretyk i praktyk wojen informacyjnych, prof. Igor Panarin.

31 http://eurasian-defence.ru/ i http://eurasian-oborona.ru/

32 http://riss.ru/bookstore/journal/

33 https://eadaily.com/ru/ Agencje te uczestniczą w kampaniach informacyjnych, mobilizują i dyscyplinują sojuszników. Zob. np. Лукашенко должен понять, что его единственный союзник — Россия, Eadaily, 8.02.2016; https://eadaily.com/ru/news/2016/02/08/lukashenko-dolzhen-ponyat-chto-ego-edinstvennyy-soyuznik-rossiya

34 Zob. Instytut OUBZ (http://www.odkb-csto.org/institute/) powstał w 2009 roku na bazie Moskiewskiego Instytutu Badań nad Integracją. Jego filie otworzono wówczas w Kijowie i Erywaniu. Działalność w Armenii trafiła na podatny grunt, filia działa do dziś, natomiast filię w Kijowie zamknięto. Stowarzyszenie Analityczne i Młodzieżowa Szkoła OUBZ to organizacje zdominowane przez Rosjan. Dla przykładu: Kazachstan w Stowarzyszeniu Analitycznym OUBZ reprezentują dwa ośrodki analityczne, Rosję – ponad dwadzieścia. Na zamkniętym spotkaniu Stowarzyszenia 16 grudnia 2015 roku sojuszników reprezentowali eksperci z Kirgistanu i Armenii, z komunikatu można wysnuć wniosek o nadreprezentacji ekspertów rosyjskich (z RISI, MGIMO, Instytutu Wschodoznawstwa Rosyjskiej Akademii Nauk).

Bazę prawną tej działalności stanowią podpisane w różnym czasie liczne oficjalne dokumenty, takie np. jak: **Koncepcja kształtowania przestrzeni informacyjnej Wspólnoty Niepodległych Państw** (1996), **Koncepcja współpracy państw WNP w sferze bezpieczeństwa informacyjnego** (2008), **Koncepcja współpracy państw WNP w walce z przestępstwami dokonywanymi przy użyciu technologii informacyjnych** (2013). Do ich realizacji powołano mnóstwo mechanizmów wykonawczych, jak: Rada Szefów Agencji Informacyjnych WNP, Stowarzyszenie Narodowych Agencji Informacyjnych WNP, Regionalna Wspólnota Łączności, Rada Koordynacyjna ds. Informatyzacji, Komisja ds. Bezpieczeństwa Informacyjnego WNP i in.

Działania informacyjno-psychologiczne w regionie opierają się na koncepcji Eurazji, stanowiącej zmodyfikowaną doktrynę tzw. bliskiej zagranicy, z Rosją w roli lidera integracji według modelu centrum–peryferie. Peryferie rozpatrywane są jako rynek zbytu mało konkurencyjnej produkcji i strategiczne przedpole, gdzie rozlokowane są rosyjskie bazy. Koncepcję eurazjatycką przeciwstawia się koncepcji euroatlantyckiej. Polemika z tą ostatnią buduje i podtrzymuje napięcie wewnętrznej i zagranicznej opinii publicznej, stanowiąc zarazem szerszą koncepcyjną podstawę działań, w tym także wojskowych. Niezależnie od stosowanej argumentacji (walka o narodowe interesy i narodową suwerenność krajów regionu), Rosja niezmiennie dąży do ścisłego rozgraniczenia obszarów wpływów i odpowiedzialności. Od czasu pomarańczowej rewolucji eksploatuje (i eskaluje) zagrożenia związane z „eksportem demokracji zachodniej". Do dziś swą interwencję zbrojną na Krymie i w Donbasie Rosja przedstawia jako swoistą misję wyzwoleńczą – w celu wyrwania Ukrainy spod dominacji USA.

Mimo mnogości i różnorodności rosyjskich inicjatyw integracyjnych ich skuteczność jest niska, co odnotowują sami kremlowscy eksperci[35]. W tym kontekście należy rozpatrywać postulat zawarty w Strategii bezpieczeństwa narodowego FR (punkt 90), dotyczący „przekształcenia OUBZ w uniwersalną

[35] Zob. Г. Тищенко, И. Николайчук, Л. Абаев, В. Карякин, Проблемы национальной безопасности России в военно-политической и оборонной сферах: современное состояние. „Доклады РИСИ". В: „Проблемы национальной стратегии", № 6 (33) 2015. W konkluzjach raportu „Problemy bezpieczeństwa narodowego Rosji w sferze polityczno-wojskowej i obronnej. Stan obecny" eksperci wojskowi kremlowskiego Rosyjskiego Instytutu Badań Strategicznych pesymistycznie oceniają możliwość powołania przez Rosję „nowego" bloku wojskowego na wzór NATO: nie widząc także potencjału pogłębienia wojskowej współpracy rosyjsko-chińskiej (w ramach konsultacyjnej Szanghajskiej Organizacji Współpracy), postulują zdynamizowanie działalności OUBZ.

organizację międzynarodową, zdolną do odpowiedzi na zagrożenia wojskowo-polityczne, wojskowo-strategiczne oraz zagrożenia w sferze informacyjnej". Jest to kolejna próba rewitalizacji OUBZ: nową tożsamość i propagandowy status „wschodniego NATO" zyskała ona po raz pierwszy w 2002 roku, kiedy Układ Taszkencki przemianowano w OUBZ i oficjalnie przedstawiono jako organizację zdolną do przeciwstawienia się nowym zagrożeniom, takim jak ekstremizm, terroryzm, nielegalny handel bronią, nielegalna migracja, zorganizowana przestępczość narkotykowa. Obecne *novum* polega na poszerzeniu zadań OUBZ o zwalczanie zagrożeń informacyjnych oraz nadaniu jej statusu organizacji uniwersalnej (cokolwiek miałoby to oznaczać).

Można wątpić, by „nowa" OUBZ rozwiązała stare problemy. Sojusznicy traktują ją jako narzędzie do rozwiązywania swoich specyficznych celów, w dodatku celów wzajemnie sprzecznych[36]. Skuteczność sojuszy wojskowych zależy ponadto od realizacji wspólnych zadań, a nie liczby podpisanych porozumień. Lista sojuszników nie została poszerzona. Przeciwnie – organizację opuścił Uzbekistan. Sojusznicy toczą między sobą swoistą wojnę propagandową: w listopadzie 2015 roku Białorusini sygnalizowali możliwość wyjścia z OUBZ Tadżykistanu. Argumentowali przy tym, że podjęta we wrześniu 2013 roku decyzja o udzieleniu pomocy wojskowo-technicznej w celu wzmocnienia sił granicznych tego kraju nie doczekała się realizacji. Oprócz białoruskiego sprzętu i kilku pojazdów pochodzących z demobilu od armii Armenii Tadżycy nie uzyskali pomocy, wyrażając wielokrotnie niezadowolenie z tego powodu[37]. Rosyjskie Ministerstwo Obrony wręcz odwrotnie – niezmiennie donosi o stałej gotowości rosyjskich baz w Tadżykistanie i Kirgistanie oraz umacnianiu w ramach OUBZ granicy afgańsko-tadżyckiej. W ocenie rosyjskiego wiceministra obrony gen. Anatolija Antonowa Rosja aktywnie wspiera modernizację sił zbrojnych sojuszników, szkoli ich kadry wojskowe, dostarcza broń i sprzęt[38].

[36] Sojusznicy wysyłają też sprzeczne komunikaty. Jeśli w 2011 roku prezydent Białorusi Aleksandr Łukaszenka podkreślał możliwość ewentualnego wykorzystania Kolektywnych Sił Reagowania OUBZ do przeciwdziałania przewrotom państwowym, to obecnie akcentuje znaczenie wojskowej współpracy białorusko-chińskiej (zob. Сергей Острына, Враг у ворот – ОДКБ созерцает и молчит; http://www.belvpo.com/ru/61214.html; Белорусско-китайские заслуги в ликвидации «ЕвроПРО»: РСЗО «Полонез», http://www.belvpo.com/ru/52976.html).

[37] http://www.belvpo.com/ru/61214.html

[38] Владимир Богданов, ОДКБ проведет спецоперации по пресечению нелегальной миграции, *Российская Газета*, 5.02.2016; http://www.rg.ru/2016/02/05/strany-odkb-provedut-specoperacii-po-presecheniiu-nelegalnoj-migracii.html

O wzmacnianiu komponentu wojskowego OUBZ systematycznie donosi też sekretarz generalny moskiewskiej kwatery tej organizacji gen. Nikołaj Bordiuża. W 2014 roku informował o powołaniu Konsultacyjnego Centrum Koordynacyjnego OUBZ w Kwestiach Reagowania na Incydenty Cybernetyczne, a także Centrum Reagowania Kryzysowego[39]. W czasie konfliktu rosyjsko-ukraińskiego Bordiuża wielokrotnie podkreślał, że siły pokojowe OUBZ są gotowe do działań poza granicami państw członkowskich, w tym na Ukrainie. W czerwcu 2015 roku Rada Ministrów Obrony OUBZ postanowiła wprowadzić nowe metody organizacji ćwiczeń wojskowych. Mają one przybierać formę niezapowiedzianych sprawdzianów gotowości bojowej, na wzór prowadzonych przez Rosję.

Równolegle nagłaśnia się prace nad powołaniem centrum cyberbezpieczeństwa WNP (brak danych na temat jego nazwy, funkcji czy podziału kompetencji pomiędzy poszczególnych członków). Moskwa, tradycyjnie, przedstawia je jako przejaw altruistycznej pomocy sojuszniczej. Wiele wskazuje, że budowane centrum powiela mechanizmy wypróbowane wcześniej. Fiasko strategicznej inicjatywy powstrzymania degradacji d. Połączonego Systemu Obrony Powietrznej ZSRR, podjętej na forum WNP w 1992 roku (nie wszystkie państwa były zainteresowane konkretnymi przedsięwzięciami, wychodząc z założenia, że odbudowa systemu, zwłaszcza potencjału ostrzegania o napadzie rakietowym, jest potrzebna w pierwszej kolejności Rosji) zmusiło Moskwę do budowania regionalnych systemów obrony powietrznej w ramach OUBZ. Dla podtrzymania i rozszerzenia tego systemu Rosja gotowa była wyposażyć Kazachstan, Armenię i Białoruś w nowoczesne kompleksy S-300 (generalnie jednak nie wzmacnia sojuszników nowoczesną bronią: woli przemieszczać na ich terytorium własny sprzęt i wojsko, powiększając asymetryczność relacji).

[39] http://redstar.ru/index.php/nekrolog/item/26173-odkb-gotova-k-lyubym-vyzovam. Centrum OUBZ tworzone przez Ministerstwo Obrony FR ma być włączone w system zarządzania obroną FR. Zapowiedział to Władimir Putin, co skrupulatnie, acz propagandowo nieudolnie, odnotował Sputnik.pl: „W Rosji zostało otwarte nowe Centrum Narodowe Zarządzania Obroną FR. Zostało ono zrobione całkowicie w oparciu o rosyjskie technologie i bardzo dobre oprogramowanie, nie mające na razie odpowiedników na świecie. Dzisiaj sekretarz naszej organizacji wspomniał, że wszystkie kraje OUBZ zostaną zaangażowane w pracę tego centrum zarządzania obroną. Jestem przekonany, że to również podniesie sterowność narodowymi systemami obrony przez nasze wojska, poprawi koordynację naszej pracy" - powiedział Putin na posiedzeniu Rady Bezpieczeństwa Zbiorowego OUBZ; http://pl.sputniknews.com/polish.ruvr.ru/2014_12_23/Kraje-OUBZ-wezma-udzial-w-pracy-narodowego-centrum-zarzadzania-obrona-FR-5017

O ile wzmocnienie potencjału oddziaływania informacyjno-psychologicznego jest potrzebne Rosji do prowadzenia politycznych kampanii antyamerykańskich i antynatowskich oraz podtrzymania procesów integracyjnych (przy każdej nadarzającej się okazji przypomina ona sojusznikom o zagrożeniach informacyjnych oraz konieczności przygotowania się do odparcia agresji informacyjnej), to zapowiadane centra cyberobrony należy rozpatrywać przede wszystkim w kategoriach ekonomicznych. Kraje regionu, zwłaszcza Azerbejdżan i Kazachstan, są dla niej ważnym rynkiem zbytu sprzętu i uzbrojenia wojskowego, ale także rynkiem usług informatyzacji, łączności i telekomunikacji, w tym wojskowej. Internet i nowe technologie telekomunikacyjne są obszarem dochodowym; wartość tego rynku stale rośnie. Nie trzeba dodawać, że o kształcie regionalnych projektów cyberbezpieczeństwa i cyberobrony decydują Rosjanie. W tym celu powołali m.in. system tzw. organizacji bazowych. Status organizacji bazowej państw WNP w kwestiach metodologicznego, szkoleniowego i organizacyjnego zabezpieczenia informatyzacji uzyskał Wszechrosyjski Naukowo-Badawczy Instytut Problemów Techniki Obliczeniowej i Informatyzacji[40]. Szkolenie specjalistów OUBZ w zakresie bezpieczeństwa cybernetycznego i walki psychologicznej stworzono na bazie rosyjskiego MIFI[41]. Wykorzystując przewagę militarną, Rosja buduje w regionie jednolitą cyberprzestrzeń, wzmacniając jednocześnie narzędzia dominacji politycznej, ekonomicznej i technologicznej na obszarze WNP.

Czas weryfikuje rosyjskie inicjatywy strategiczne. Rosja kontynuuje działania ekonomiczne, cywilizacyjne, kulturowe, polityczne i wojskowe w krajach regionu, podporządkowuje je własnym interesom, mimo iż nie przynosi to oczekiwanych przez nią rezultatów. Niektóre z tych działań są kontrproduktywne. Rosyjska polityka wobec Ukrainy np. wśród partnerów z OUBZ spowodowała szok. Mimo to liderzy państw OUBZ nadal podpisują wspólne deklaracje. Jednocześnie żaden z nich do dziś nie uznał suwerenności państwowej samozwańczych Osetii Południowej i Abchazji, które w ostatnich dokumentach (Doktrynie wojennej z 2014 roku i Strategii bezpieczeństwa narodowego z 2015

[40] Ros. Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации» (ФГУП ВНИИПВТИ) – zob. www.pvti.ru

[41] MIFI – Moskiewski Instytut Inżynieryjno-Fizyczny powstał na bazie instytutu badawczego rosyjskiej zbrojeniówki. W 2011 roku jego Wydział Cybernetyki poszerzono o katedrę bezpieczeństwa informacyjnego. Kształci specjalistów na czterech kierunkach: technologie ochrony systemów komputerowych, systemy zarządzania infrastrukturą krytyczną, bezpieczeństwo zautomatyzowanych systemów zarządzania oraz zabezpieczenie analityczne bezpieczeństwa informacyjnego.

roku) Rosja zaliczyła do swych sojuszników. Żaden z partnerów z OUBZ nie poparł też aneksji Krymu ani rosyjskiej interwencji w Donbasie. Sojusznicy nie przyłączyli się do rosyjskich sankcji wobec Turcji i Ukrainy. Nie potępili Turcji po zestrzeleniu rosyjskiego Su-24 na pograniczu turecko-syryjskim w listopadzie 2015 roku. Wbrew zapowiedziom o możliwej interwencji sojuszniczej pod auspicjami ONZ z września 2015 roku stanowisko OUBZ w sprawie rosyjskiej interwencji w Syrii z 21 grudnia 2015 roku ograniczyło się do potępienia terroryzmu i poparcia rezolucji Rady Bezpieczeństwa ONZ w sprawie politycznego uregulowania konfliktu. Ich deklaracja przypomina starą radziecką nowomowę: sojusznicy skonstatowali „wzrost napięcia w przestrzeni eurazjatyckiej, strefie odpowiedzialności OUBZ" i zapowiedzieli „umacnianie potencjału siłowego organizacji oraz dalszy rozwój współpracy w walce z terroryzmem zarówno na szczeblu politycznym, jak i na szczeblu służb specjalnych, ministerstw i resortów".

## 3. Poziom krajowy: wojskowa organizacja społeczeństwa

O ile na arenie międzynarodowej i regionalnej rezultaty wojskowej strategii informacyjnej są znikome, to na arenie wewnętrznej odnosi ona jednoznaczny sukces. Jej krótko- i długoterminowe cele są zbieżne. Są one także zbieżne z celami Kremla, dążącego do mobilizacji i konsolidacji społeczeństwa wokół reżimu. Dość wspomnieć, że podczas centralnych uroczystości z okazji Dnia Obrońcy Ojczyzny 21 lutego 2016 roku prezydent Władimir Putin dziękował rosyjskiej armii, która „w Syrii broni rosyjskich interesów", po raz kolejny insynuując „spisek Zachodu przeciwko interesom Rosji".

Sukces militarystycznej propagandy jednoznacznie potwierdzają badania opinii publicznej, według których liczba osób negatywnie nastawionych wobec Zachodu rośnie lawinowo. Za głównego potencjalnego wroga obywatele Rosji uznają dziś Stany Zjednoczone: tak uważa 53% uczestników sondażu centrum badania opinii publicznej WCIOM przeprowadzonego w październiku 2015 roku (w 1990 roku odsetek ten wynosił 19%). 48% ankietowanych obawia się zbrojnego ataku na Rosję (w 1990 roku – 13%). Zmieniła się ocena zdolności bojowych armii. Obecnie co trzeci Rosjanin uważa, że armia rosyjska jest najlepsza na świecie, a 49% – że jedną z najlepszych (w 1990 roku – 21%).

Co ciekawe, jeszcze wyraźniejsze wyniki przyniosły przeprowadzone w lutym 2016 roku badania cieszącego się opinią niezależnego ośrodka Centrum Lewady. Dwie trzecie ankietowanych (65%) wyraziło przekonanie o istnieniu realnego zagrożenia militarnego dla Rosji; absolutna większość (81%) uznała, że

w przypadku wystąpienia takiego zagrożenia armia ich obroni. Coraz więcej Rosjan (według tego badania) opowiada się za zachowaniem powszechnego obowiązku służby wojskowej (w 2016 roku – 58% wobec 40% w 2014).

Taka sytuacja jest efektem wieloletnich działań systemowych, w tym zwłaszcza uruchomionego w 2000 roku systemu kształcenia specjalistów w zakresie bezpieczeństwa informacyjnego, a także prowadzonego od 2001 roku szeroko zakrojonego programu „Patriotyczne wychowanie obywateli Federacji Rosyjskiej". Program jest koordynowany przez Rosyjskie Państwowe Centrum Wojskowe i Historyczno-Kulturalne[42] przy Rządzie FR. Dyrektorem tej agencji rządowej jest admirał Wiaczesław Fietisow. Na początku swej działalności skupiała się ona na realizacji wojskowej polityki historycznej, skoncentrowanej na tradycjach bojowych i bohaterskich dokonaniach rosyjskiej armii, „odkłamywaniu" historii wojskowości fałszowanej jakoby przez część rosyjskich historyków i Zachód, dbałości o pomniki i miejsca pamięci poległych za wolność ojczyzny, a także wspomaganiu rosyjskich weteranów walk. W realizowanej obecnie trzeciej edycji programu rządowego na lata 2016–2020[43] położono nacisk na współdziałanie armii i społeczeństwa, a także patriotyczno-wojskowe wychowanie dzieci i młodzieży. Program jest realizowany przez ministerstwa: Obrony, Oświaty, Kultury i Sportu przy udziale innych struktur rządowych (MSZ, Ministerstwa Sytuacji Nadzwyczajnych, Federalnej Służby Bezpieczeństwa, Federalnej Służby Antynarkotykowej, Służby Wykonywania Kar, Agencji ds. Młodzieży i in.), a także organizacji społecznych (DOSAAF, Wszechrosyjskiej Organizacji Weteranów Wojny, Sił Zbrojnych i Organów Porządku Prawnego, Ogólnorosyjskiej Organizacji Inwalidów Wojennych, Rosyjskiego Związku Weteranów, Fundacji Absolwentów Uczelni Wojskowych „Zasługi. Kodeks. Pamięć. Honor", Rosyjskiego Związku Młodzieży, Międzyregionalnej Fundacji „Świat Młodzieży") oraz religijnych (głównie za pośrednictwem Patriarchatu Moskiewskiego) i in. W realizacji programu obligatoryjnie uczestniczą administracje lokalne, w których powołano odrębne struktury do spraw patriotyczno-wojskowego i obywatelskiego wychowania młodzieży.

Planowane na lata 2016–2020 przedsięwzięcia na ogół powielają obserwowane wcześniej: obok monitoringu i analizy skuteczności programów regionalnych,

[42] Ros. Росвоенцентр.

[43] Мероприятия по реализации государственной программы «Патриотическое воспитание граждан Российской Федерации на 2016–2020 годы», http://www.rosvoencentr-rf.ru/obobshchennye-doklady/gosprogramma-pvg-rf-2016-2020/meropriyatiya-po-realizatsii.php

skupiają się one na powoływaniu klubów i stowarzyszeń patriotycznych w placówkach oświaty, kultury i sportu[44]. W ramach programu przygotowywane są rekomendacje metodyczne i pomoce naukowe w rodzaju „Bohaterowie Ziemi Rosyjskiej", „Historia Ojczyzny w pieśniach Chóru Aleksandrowa", organizowane są regionalne konferencje „Patriotyzm jako jednocząca idea Rosji w XXI wieku". Jednym z deklarowanych celów jest zapewnienie masowego udziału młodzieży w obchodach przypadającej w 2020 roku 75. rocznicy zakończenia Wielkiej Wojny Ojczyźnianej. Młodemu pokoleniu przypisano symboliczną rolę „warty pamięci", „kontynuatora historycznej misji zwycięstwa", „spadkobiercy wspólnego zwycięstwa narodów Rosji" (pod takimi hasłami odbędą się organizowane w 2020 roku biegi i gry terenowe, seminaria i konferencje okrągłostołowe). Tradycyjnie umieszczono w programie zorganizowaną turystykę do miejsc związanych z „misją wyzwoleńczą armii Imperium Rosyjskiego, Armii Czerwonej i Armii Radzieckiej" w różnych okresach historii oraz „przywrócenie pamięci o poległych w latach 1941–1945 podczas wyzwalania Krymu i Sewastopola, a także Polski i Niemiec".

Jednym z ważniejszych podmiotów wojskowego segmentu systemu informacyjnego jest Akademia Nauk Wojskowych (AWN)[45]. Wbrew nazwie nie jest ona instytucją naukową: została powołana dekretem Borysa Jelcyna z 1995 roku jako „centrum niezależnych badań obronnych". Niezmiennym jej prezesem jest gen. armii Mahmud Gariejew[46]. Wśród założycieli Akademii znalazły się: Rosyjski Instytut Studiów Strategicznych (znajdujący się wówczas w strukturze Służby Wywiadu Zagranicznego), Komitet Uczonych „O bezpieczeństwo globalne", Liga Wspierania Przedsiębiorstw Obronnych, Uniwersytet Rosyjsko-Amerykański, Rosyjski Związek Przemysłowców i Przedsiębiorców, Centrum Badań Międzynarodowych i Wojskowo-Strategicznych, Fundacja Badań Społeczno-Ekonomicznych i Politycznych i in. W połowie lat 90. Akademia „zagospodarowała" pracowników rozwiązanych instytucji naukowo-badawczych oraz zwolnione do rezerwy kadry polityczno-wojskowe i wojskowo-techniczne. Dziś pod tą prestiżową nazwą kryje się stowarzyszenie centrów

[44] Ten trend uległ wzmocnieniu w roku bieżącym, o czym świadczy powołanie pod patronatem Ministerstwa Obrony ogólnorosyjskiego ruchu „Młoda Armia". Pierwsze kluby „Młodej Armii" pojawiły się w 2008 roku. Ich inicjatorami byli nauczyciele „podstaw bezpieczeństwa w życiu codziennym". Zob. np. Минобороны создает молодежную организацию „Юнармия", *Коммерсант,* 5.04.2016, http://www.kommersant.ru/doc/2956367

[45] www.avnrf.ru/

[46] Gariejew ma 93 lata i, jak się podkreśla w notkach biograficznych, 18 orderów i 27 medali; jako zastępca szefa Sztabu Generalnego Sił Zbrojnych ZSRR był jednym ze współautorów **Koncepcji obronnej Układu Warszawskiego**, 1987.

analitycznych i struktur badawczych sił zbrojnych, MSW, Służby Granicznej, Federalnej Służby Bezpieczeństwa, Ministerstwa Sytuacji Nadzwyczajnych, a także cywilnych ekspertów i dziennikarzy wyspecjalizowanych w problematyce obronności.

Akademia łączy działalność badawczą, koncepcyjną i metodologiczną z działalnością organizacyjną: buduje zaplecze wykonawcze wojskowych działań informacyjnych i realizuje projekty systemowe. Wyniki badań naukowych członków Akademii są prezentowane w kwartalniku *Wiestnik AWN*[47] dostępnym na oficjalnym portalu Akademii. Sztandarowymi projektami społeczno-edukacyjnymi są Akademia Informacyjnej Samoobrony[48], która od 2008 roku wydaje kwartalnik *Wojny Informacyjne*[49] oraz współuczestniczy w państwowym programie patriotycznego wychowania społeczeństwa: organizuje doroczny konkurs plastyczny dla dzieci i młodzieży związany z problematyką historyczno-wojskową, prowadzi wojskowo-sportowe Centrum Młodzieżowe „Alfa" (propaguje wschodnie sztuki walki), organizuje imprezy masowe (w rodzaju „Спасибо деду за победу", pol. „Dziękujemy dziadkowi za zwycięstwo"), przygotowała serię podręczników do nauczania w klasach 5–11 przedmiotu podstawy bezpieczeństwa w życiu codziennym (odpowiednik przysposobienia obronnego, poszerzonego o techniki przetrwania, sztukę kamuflażu, elementy geopolityki i światopoglądowe)[50]. Celem tych projektów jest krzewienie idei militarystycznego patriotyzmu i dumy z rosyjskiej armii, wpajanie obowiązku obrony ojczyzny, kształtowanie zainteresowań obronnych i postaw „społeczeństwa kontrwywiadowczego".

Akademia ściśle współpracuje z Ministerstwem Obrony i Sztabem Generalnym Sił Zbrojnych Federacji Rosyjskiej (*notabene* jej prezydium i redakcja kwartalnika *Wiestnik AWN* mają siedziby w pomieszczeniach Katedry Historii Wojskowości Akademii Sztabu Generalnego na prospekcie Uniwersyteckim 14 w Moskwie). O symbiozie czynnej i pozostającej w stanie spoczynku części

[47] http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov?layout=blog

[48] Instytucja samookreśla się jako „dobrowolne stowarzyszenie społeczne specjalistów badających wpływ informacji na psychikę człowieka, a także techniki i metody informacyjnej samoobrony".

[49] http://www.iwars.su/

[50] Przedmiot podstawy bezpieczeństwa działalności życiowej wprowadzono do nauczania powszechnego na mocy ustawy o kształceniu w Federacji Rosyjskiej z 29 grudnia 2012 roku. Kształcenie w tym zakresie przewiduje zarówno zajęcia lekcyjne, jak i pozalekcyjne (ćwiczenia praktyczne z zakresu ratownictwa w centrach Ministerstwa Sytuacji Nadzwyczajnych oraz ośrodkach szkoleniowych Ministerstwa Obrony).

wojskowego systemu informacyjnego świadczą zarówno regularne kontakty między nimi, jak i spójność przekazu. Przyczynkiem do analizy tej spójności może być np. wykład szefa sztabu gen. Walerija Gierasimowa podczas dorocznego zgromadzenia członków Akademii pod koniec lutego 2016 roku. Kreśląc „nowe" zagrożenia militarne dla Rosji, generał wymienił tzw. ruchy kolorowe i negatywny wpływ na świadomość rosyjskiego społeczeństwa zewnętrznego oddziaływania informacyjnego, niszczącego historyczne, duchowe i patriotyczne tradycje obrony Rosji. Do wojskowych uczonych zaapelował o głębszą refleksję i nowe idee, dotyczące strategicznych kierunków działań sił zbrojnych w kosmosie i przestrzeni informacyjnej, uwzględniające doświadczenia operacji na Ukrainie i w Syrii[51].

Mówiąc o nowych potrzebach wyposażenia armii pod kątem prowadzonych wojen informacyjnych, powtórzył strategiczne cele sygnalizowane w punkcie 46 Doktryny wojennej FR z grudnia 2014 roku: podkreślił znaczenie kanałów wymiany informacji z innymi organami i służbami oraz ścisłego współdziałania formacji militarnych różnych resortów, a także wojskowego i niewojskowego komponentu obrony terytorialnej w przypadku wystąpienia sytuacji kryzysowej. Uwypuklając w tym kontekście rolę Narodowego Centrum Obrony, zaakcentował konieczność doskonalenia systemów zarządzania informacją i ich zintegrowania ze zautomatyzowanymi systemami kontrolnymi na poziomie strategicznym, operacyjnym i taktycznym.

Działalność Akademii umożliwia odciążenie budżetu obronnego. Akcje prowadzone za jej pośrednictwem finansują głównie przedsiębiorstwa przemysłu zbrojeniowego, ale także Rada Bezpieczeństwa, Rada Federacji, Duma Państwowa i poszczególne resorty, na których zlecenie AWN prowadzi projekty badawcze, eksperckie i wykonawcze. Wydawane przez Akademię kwartalniki finansuje z kolei Wojskowe Towarzystwo Ubezpieczeniowe, zaś przyznawane młodym uczonym nagrody im. A. Suworowa i A. Swieczyna – Fundacja Wspierania Badań w zakresie Bezpieczeństwa Narodowego „Nauka – XXI wiek", wespół z którą realizowany jest projekt „Armia i społeczeństwo"[52]. Sponsorzy, darczyńcy i mecenasi tych projektów wchodzą w skład AWN jako jej członkowie honorowi. Według danych ze sprawozdania z działalności za 2015 roku obecnie liczy ona 839 członków rzeczywistych, 432 członków korespondentów i 91 członków honorowych (z czego 30% to oficerowie czynni, 70% – generalicja i kadry

[51] Tekst tego wystąpienia zob. Валерий Герасимов, По опыту Сирии, Военно-промышленный Курьер, 9.03.2016, http://www.vpk-news.ru/articles/29579

[52] http://www.arm-ob.ru/

naukowo-badawcze w rezerwie i stanie spoczynku). Sama tytulatura nawiązująca do tytulatury Rosyjskiej Akademii Nauk ma podkreślać społeczny prestiż tego gremium rosyjskich uczonych wojskowych: członkiem Akademii Nauk Wojskowych może zostać obywatel Federacji Rosyjskiej lub obywatel innego państwa (w praktyce – Białorusi; istnieje bowiem Białoruski Regionalny Oddział AWN), który ukończył 18 lat i ma stopień naukowy doktora (ros. кандидат наук). Lektorzy posługują się tytułem profesor Akademii Nauk Wojskowych.

Oficjalnie tego rodzaju projekty i przedsięwzięcia mają na celu połączenie wysiłków władz, społeczeństwa i armii na rzecz kształtowania systemu wartości cywilizacyjnych, którego istotnym elementem jest historia i tradycja zwycięstw rosyjskiej armii. Ma to doprowadzić do wzmocnienia autorytetu i podniesienia prestiżu służby wojskowej oraz wyeliminowania negatywnych tendencji, które pojawiły się wskutek próżni duchowej i ideologicznej w latach 90. XX wieku, co z kolei zaowocowało osłabieniem podstaw państwa rosyjskiego. Sygnalizowany na początku pierwszej kadencji prezydentury Władimira Putina powrót państwa i uruchomione wówczas programy, w tym program wojskowego wychowania patriotycznego, miały zaowocować systemową spójnością i zbudowaniem silnej tożsamości państwowej, opartej na narzuconej odgórnie wizji wspólnej historii i wartości cywilizacyjnych (podobnie jak ZSRR, Rosja jest państwem wielonarodowym i wielokulturowym i raczej trudno w tym przypadku mówić o wspólnocie pochodzenia i kultury; także historia narodów Rosji nie jest czynnikiem scalającym). Nie napotykało to jednak i nadal nie napotyka większych psychologicznych i mentalnościowych barier. O ile w latach 90. społeczeństwo oburzało się z powodu patologii w rosyjskiej armii (tzw. дедовщина, czyli fala; czystki etniczne podczas operacji czeczeńskich, grabieże i gwałty na ludności cywilnej), to dziś zachwyca się „patriotami Krymu", uprzejmymi „zielonymi ludzikami", rosyjskim uzbrojeniem, sukcesami operacji w Syrii, uczestniczy w masowych imprezach podporządkowanych celom militarystycznej propagandy. Przy okazji manifestuje propaństwowy patriotyzm i dumę z wszechpotężnego scentralizowanego państwa i jego szefa.

W praktyce wzmacnianiu organizacji wojskowej państwa i potencjału mobilizacyjnego towarzyszył proces wojskowej organizacji społeczeństwa, który jest kontynuowany. Jest to szeroko zakrojony, sterowany odgórnie, głęboki proces długiego trwania, o czym świadczą projekty adresowane do najmłodszych. W konkursach rysunku i festiwalach piosenki organizowanych na 70-lecie zwycięstwa w 2015 roku przewidziano udział dzieci w kategorii wiekowej 5–7 lat, sieć sklepów wojskowych Wojentorg poszerzyła niedawno asortyment o „zmilitaryzowane" misie (czołgistę, lotnika, marynarza itp.). U podstaw tego

rodzaju misyjnych przedsięwzięć wojskowych leży mit o niezwyciężonej rosyjskiej armii. Powszechna w społeczeństwie obecność symboliki wojskowej i patriotyzm w kolorze khaki już doprowadziły do militaryzacji świadomości społeczeństwa Rosji. Taki rezultat unaocznia z kolei, że w koncepcję działań armii w przestrzeni informacyjnej wbudowano nie tylko zacieranie granic między wojną a pokojem, współdziałanie między wojskowym i niewojskowym segmentem systemu, ale także legitymizację Putinowskiego reżimu. Atak na reżim w narracji sił zbrojnych jest zagrożeniem militarnym, podważaniem samego istnienia Rosji jako spójnej, wewnętrznie jednorodnej przestrzeni politycznej, ekonomicznej, społecznej i informacyjnej. Także wizja/ocena świata i zewnętrznych zagrożeń militarnych są budowane z perspektywy interesu Kremla. W tym przypadku krótko- i długoterminowe cele strategiczne Kremla i wojskowych są zbieżne. Unaocznia to zarazem, że głównym źródłem władzy w Rosji jest siła, zaś konsolidacja społeczeństwa wokół Kremla odbywa się poprzez ciągłe wykorzystywanie obrazu wroga i nieustannie pokonującej go rosyjskiej armii. Nie powinno więc dziwić, że wśród zabawek sprzedawanych w Wojentorgu obok misia lotnika i misia pełniącego misję „arktyczną" znajdujemy misia dżudokę i misia hokeistę[53]. Przez tego rodzaju propagandę przemycono w sposób dostępny dla malucha wizerunek zwierzchnika sił zbrojnych, gwaranta istniejącego w Rosji reżimu.

[53] http://rusnews2015.ru/mishki-nanosyat-otvetnyj-udar/

## IV. PODSUMOWANIE: ARMIA W SŁUŻBIE POLITYKI

Działania Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej są podporządkowane szerszej, długoterminowej strategii bezpieczeństwa informacyjnego Rosji. W rezultacie rosyjska armia realizuje zarówno zadania ściśle wojskowe (niepubliczne), jak i niewojskowe (publiczne): zgodnie z rosyjską kulturą strategiczną czynnik siły uzasadnia status mocarstwowy Rosji oraz wewnętrzną i zagraniczną politykę jej władz. W dążeniu do świata wielobiegunowego Kreml wykorzystuje to do utrzymania i poszerzenia wpływów w najbliższym sąsiedztwie i poza nim. Zasadniczym punktem odniesienia i głównym przeciwnikiem armii rosyjskiej jest armia amerykańska i jej sojusznicy z NATO. Wojskowa polityka informacyjna uwypukla możliwości rosyjskich sił zbrojnych, osłabiając jednocześnie pozycje potencjalnych przeciwników.

Analiza rosyjskich dokumentów strategicznych uwzględniających udział armii w realizacji celów polityczno-wojskowych prowadzi do wniosku o ewolucji poglądów rosyjskich strategów w kierunku ich radykalizacji w kwestii użycia siły. Funkcję odstraszania jądrowego, obejmującą początkowo przeciwdziałanie atakowi nuklearnemu, rozszerzono na przeciwdziałanie atakowi konwencjonalnemu i (ostatnio) atakowi informacyjnemu (według rosyjskiej terminologii). Rozszerzony zakres odstraszania psychologicznego wynika z potrzeby zwiększenia presji zarówno na potencjalnych agresorów, jak i sojuszników z najbliższego sąsiedztwa. Służyły temu korekty sukcesywnie wprowadzane do rosyjskich doktryn, zastraszające opinię publiczną i pogłębiające nieufność wobec Zachodu.

Znaczenie odstraszania informacyjnego (i szerzej – czynnika wojskowego) będzie rosło. Oprócz siły i będącej jednym z głównych narzędzi wojny informacyjnej dyplomacji Rosja nie ma innych ważkich argumentów w polityce międzynarodowej. Stanowią one główny filar mocarstwowego (regionalnego) statusu Rosji. Jako słabnący biegun siły na świecie, Rosja będzie wykorzystywać wszelkie dostępne siły i środki, by zahamować proces słabnięcia. Na obecnym etapie prezentuje potencjał destrukcji, maskując to dążeniem do utrzymania globalnej równowagi sił i osiągnięcia różnych parytetów, w tym „parytetu informacyjnego".

Warto na koniec podkreślić, że na poziomie strategicznym cele działań informacyjnych Sił Zbrojnych Federacji Rosyjskiej wytyczono w sposób jak najbardziej ogólny. Obejmują one również działania w zakresie rozwoju cyberpower, cyberobrony i cyberofensywy. Pełne rozpoznanie tych celów wymaga nie

tylko głębokiej znajomości techniki decyzyjnej w Rosji, ale także wiedzy na temat możliwości technologicznych i organizacyjnych, które tylko państwo jest w stanie zapewnić.

Realizacja wyżej wymienionych celów na poziomie operacyjnym sprowadza się do koordynacji działań różnych podmiotów, wykonujących zadania różnej natury. Analiza tych działań wskazuje, że Rosjanie nie przejawiają większej inwencji, niezmiennie powielają te same metody. A metody te, przejrzyste dla krajów z regionu, stają się także coraz lepiej rozpoznawalne także na Zachodzie.

## ANEKS 1

### Lista dokumentów źródłowych

Doktryna wojenna Federacji Rosyjskiej, 2014; http://www.scrf.gov.ru/documents/33.html

Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej, 2000; http://www.scrf.gov.ru/documents/6/5.html

Projekt doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej, 2015; http://infosystems.ru/assets/files/files/doktrina_IB.pdf

Strategia bezpieczeństwa narodowego Federacji Rosyjskiej do 2020 roku, 2015; http://www.scrf.gov.ru/documents/99.html

Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku, 2013; http://www.scrf.gov.ru/documents/6/114.html

Koncepcja działalności Sił Zbrojnych FR w przestrzeni informacyjnej; http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle

Fragment Koncepcji państwowego systemu wykrywania, uprzedzania i likwidacji skutków ataków komputerowych na zasoby informacyjne Federacji Rosyjskiej; http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf

## ANEKS 2

### Koncepcja działalności Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej – omówienie

**Jedynym publicznie dostępnym resortowym dokumentem strategicznym jest opublikowana w lutym 2012 roku Koncepcja działalności Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej. Zaprezentowana tu wizja wojskowych, podkreślających z jednej strony systemowe podejście do kwestii bezpieczeństwa i obrony przestrzeni informacyjnej Federacji Rosyjskiej, a z drugiej – globalny zasięg działań informacyjnych, nie różni się zasadniczo od wizji przedstawionej w części I niniejszego opracowania. Dokument stanowi ponadto rodzaj polityczno-wojskowego marketingu, wyraźnie obliczonego na pozytywne przyjęcie zarówno w kraju, jak i za granicą (opublikowano ją w dwóch wersjach językowych, po rosyjsku i angielsku).**

Kilkunastostronicowy dokument składa się z czterech części:

1. Słownik kluczowych terminów i ich definicji,
2. Zasady,
3. Reguły,
4. Środki budowy zaufania.

Dokument rozpoczyna Wstęp, kończy Konkluzja. Przestrzeń informacyjną określono w preambule jako kolejny teatr działań wojennych (obok lądu, morza, powietrza i kosmosu): „Szybki rozwój systemów informacji rozmaitego przeznaczenia, takich jak Internet i media elektroniczne, doprowadził w drugim tysiącleciu do powstania globalnej przestrzeni informacyjnej. Podobnie jak ląd, morze, powietrze i kosmos, przestrzeń informacyjna w armiach krajów najbardziej rozwiniętych jest aktywnie wykorzystywana do różnych zadań wojskowych". W samej definicji przestrzeni informacyjnej zaakcentowano wpływ informacji na świadomość indywidualną i grupową. Oprócz działań w sferze psychologicznej wojskowe działania w przestrzeni informacyjnej obejmują sferę techniczną (urządzenia sprzętowe, hardware, i oprogramowanie, software). W kilku miejscach podkreślono, że przestrzeń informacyjna jest zintegrowaną przestrzenią bezpieczeństwa i obrony („Siły Zbrojne Federacji Rosyjskiej podejmują wyzwania obrony i bezpieczeństwa płynące z globalnej przestrzeni informacyjnej; (...) używają zasobów informacji wojskowej w celu rozwiązywania problemów obrony i bezpieczeństwa").

W zawartym **w części 1. Słowniku kluczowych pojęć** resort samookreślił siły zbrojne jako część sił bezpieczeństwa informacyjnego FR, samo bezpieczeństwo informacyjne sił zbrojnych – jako „bezpieczny stan zasobów, odporny na potencjalne oddziaływanie broni informacyjnej". Wojskowa definicja wojny informacyjnej nie zrywa z klasycznym paradygmatem wojny. Określono ją jako: „**konfrontację dwóch (lub więcej) państw w przestrzeni informacyjnej** w celu wyrządzenia szkód systemom informacyjnym, procesom i zasobom, infrastrukturze krytycznej i innym strukturom, zdestabilizowania systemu politycznego, ekonomicznego i społecznego, zmasowanej psychologicznej intoksykacji ludności w celu zdestabilizowania społeczeństwa i państwa, a także zmuszenia państwa do przyjęcia decyzji zgodnych z interesami strony przeciwnej". W definicji połączono natomiast dwa aspekty tej wojny: informacyjno-techniczny oraz informacyjno-psychologiczny. Celem rażenia informacyjnego jest destabilizacja systemu politycznego, ekonomicznego i społecznego państwa, zaś obiektami – organy zarządzania państwem, systemy infrastruktury telekomunikacyjnej, społeczeństwo (zarówno ludność cywilna, jak i stan osobowy armii), środki informacji masowej (w pierwszym rzędzie elektroniczne). Także wykorzystywana przy tym broń informacyjna („technologie, środki i metody informacyjne, stosowane w celach prowadzenia wojny informacyjnej") ma podwójną naturę: informacyjno-techniczną oraz informacyjno-psychologiczną.

**Część 2. (Zasady)** jest najobszerniejsza; przybliża pryncypia, jakimi Siły Zbrojne Federacji Rosyjskiej kierują się w przestrzeni informacyjnej. Są to zasady: legalności, priorytetu działań informacyjnych, kompleksowości (użycie przez siły zbrojne wszystkich dostępnych sił i środków), współdziałania w obrębie systemu bezpieczeństwa informacyjnego Federacji Rosyjskiej, współpracy na poziomie regionalnym i globalnym oraz zasada innowacyjności. O ile zasady legalności, współpracy międzynarodowej, w tym w pierwszym rzędzie – regionalnej, są stałym elementem wszystkich rosyjskich dokumentów strategicznych, służąc manifestowaniu pokojowych, obronnych intencji rosyjskiego państwa oraz podkreślaniu, że Rosja ma wielu sojuszników podzielających jej podejście, o tyle pozostałe zasługują na bardziej wnikliwą uwagę, odsłaniają bowiem technologię wojskowych operacji walki informacyjnej. I tak **zasada priorytetu działań informacyjnych** wymaga od armii dokładnego rozpoznania zagrożeń i procesów operacyjnych, dokładnej ich analizy i rozwinięcia w porę środków obronnych. Jak czytamy, „uznanie tych środków za priorytet w warunkach współczesnych jest spowodowane tym, iż w globalnej przestrzeni informacyjnej tworzonej przez Internet, elektroniczne media i mobilne systemy komunikacji zaangażowane są setki milionów ludzi (w różnych krajach i na różnych kontynentach)".

Zawarte w tej części tezy:

(1) Współczesny świat jest światem wojny informacyjnej;

(2) Niesie ona katastrofalne skutki;

(3) Neutralizacja tego zagrożenia wymaga globalnego zakresu działań Sił Zbrojnych Federacji Rosyjskiej

wpisują się w doktrynalną percepcję zagrożeń oraz odpowiedzi na nie z użyciem wszelkich dostępnych sił i środków.

**Zasada kompleksowości** przybliża z kolei charakter i skalę działań. Jak czytamy, „działalność sił zbrojnych w przestrzeni informacyjnej obejmuje aktywność personelu, operacje oddziałów, kamuflaż operacyjny, wojnę elektroniczną, komunikację, zautomatyzowane tajne zarządzanie, pracę personelu informacyjnego, oraz ochronę systemów informacyjnych przed uderzeniami elektronicznymi, komputerowymi bądź innego typu. Dowódcy i personel na każdym szczeblu są bezpośrednio zaangażowani w działania w przestrzeni informacyjnej w czasie wojny i pokoju, w przygotowywanie operacji, jak i same operacje (operacje walki). Wszystkie te operacje, niezależnie od funkcji i odpowiedzialności za rozwijanie i planowanie działań i akcji podległych oddziałów, są powiązane wspólną koncepcją działania w przestrzeni informacyjnej". Resort potwierdza tym samym, że prowadzone w czasie wojny i w czasie pokoju operacje są planowane i spięte wspólną koncepcją. Obejmują zarówno działania defensywne, jak i ofensywne, pasywne i aktywne, w tym operacje specjalne wymagające kamuflażu. Do operacji walki włączono walkę elektroniczną (zakłócanie, paraliż kanałów łączności) oraz ataki komputerowe.

**Zasada współdziałania** wymaga od resortu obrony skoordynowania jego działań w przestrzeni informacyjnej z innymi federalnymi organami wykonawczymi (eufemizm, za którym kryją się przede wszystkim służby specjalne). Interakcja – jak podkreślono – zachodzi w obrębie systemu bezpieczeństwa informacyjnego FR, opierającego się na Doktrynie bezpieczeństwa informacyjnego FR (2000). Interoperacyjności wymaga także **zasada innowacyjności**, tj. wykorzystywania w szkoleniu i działaniach w przestrzeni informacyjnej najbardziej zaawansowanych technologii i technik, a także podejmowania wyzwań związanych z bezpieczeństwem informacji z udziałem wykwalifikowanego personelu. „Dlatego do rozwoju narzędzi i technologii winny być wykorzystywane badania najbardziej zaawansowanych ośrodków innowacyjnych

FR prowadzone w ramach programów badań i rozwoju realizowanych przez państwo i jego rozmaite agencje". Dalej czytamy, że kształcenie specjalistów prowadzą uczelnie podległe Ministerstwu Obrony, ale „dodatkowo mogą być angażowani także absolwenci innych szkół wyższych FR". Zasady kompleksowości i współdziałania wynikają z systemowego podejścia do problematyki bezpieczeństwa informacyjnego, narzucającego łączenie w czasie i przestrzeni działań wszystkich sektorów bezpieczeństwa Federacji Rosyjskiej, ich środków, metod i sposobów działania oraz budowanie zdolności poszczególnych struktur do skoordynowanego działania.

**Część 3. (Reguły)** dotyczy odstraszania i prewencji konfliktów oraz sposobów ich rozwiązywania. Nie różnią się one od ogólnych zasad polityki wojskowej, przedstawionych w Doktrynie wojennej FR, którą zresztą przywołano („Wojskowa polityka FR ma na celu zapobieganie wyścigowi zbrojeń, odstraszanie i prewencję konfliktów militarnych"). W tym celu zaleca się rozwój systemu bezpieczeństwa informacyjnego Sił Zbrojnych, utrzymywanie sił i środków bezpieczeństwa informacyjnego w stałej gotowości, podejmowanie wszelkich sił i środków celem wczesnego wykrycia potencjalnych konfliktów wojennych w przestrzeni informacyjnej oraz ich organizatorów, podżegaczy i wspólników, szczegółową analizę przyczyn i uwarunkowań konfliktu i jego eskalacji oraz **przejęcie zarządzania konfliktem** (kontroli nad nim), aby zapobiec katastrofie. Na uwagę zasługuje punkt ostatni (10), postulujący „oficjalne, w sposób obiektywny i we właściwym czasie wyjaśnianie opinii publicznej powodów i przyczyn konfliktu", a także kształtowanie opinii publicznej, tj. „stosowne jej ukierunkowanie i mobilizację oraz tworzenie globalnego środowiska przestrzeni informacyjnej, sprzyjającego zmniejszeniu możliwości dalszej eskalacji konfliktu". Kwestia rozwiązywania konfliktów wyraźnie nawiązuje do tekstu amerykańskiej strategii działania w cyberprzestrzeni: jeśli zawiodą działania pojednawcze, zwracanie się do RB ONZ, inne pokojowe inicjatywy, Rosja zastrzega sobie możliwość wyegzekwowania prawa do indywidualnej lub kolektywnej samoobrony, z użyciem wszelkich dostępnych środków wojskowych. Wpływ cyberstrategii USA zaznaczył się także w implementacji koncepcji zarządzania konfliktami, uznaniu przestrzeni informacyjnej za przestrzeń operacyjną oraz zasady innowacyjności.

Zaprezentowana strategia odstraszania zakłada wykorzystanie wszelkich niezbędnych środków (politycznych, ekonomicznych, dyplomatycznych, informacyjnych), które składają się na nacisk FR. W sferze informacyjnej polega na kontrinformowaniui opinii publicznej na różnych poziomach, łącznie z globalnym. W związku z tym podkreślono konieczność rozbudowy „infrastruktury

informacyjnej" na obcych terytoriach: „W interesie samoobrony indywidualnej i zbiorowej należy wykorzystywać niezbędne środki bezpieczeństwa informacyjnego na terytorium obcych państw, zgodnie z dobrowolnie osiągniętymi porozumieniami; (...) w czasie konfliktu należy informować lokalne i zagraniczne media o rozwoju sytuacji, promować deeskalację konfliktu oraz utrwalać osiągnięcia, uwzględniając opinię publiczną". Dwa punkty tej części kładą nacisk na priorytet współpracy we wzmacnianiu międzynarodowego bezpieczeństwa informacyjnego, w tym zwłaszcza regionalnego w ramach Organizacji Układu o Bezpieczeństwie Zbiorowym (w skład której wchodzą Armenia, Białoruś, Kazachstan, Kirgistan, Rosja i Tadżykistan), Wspólnoty Niepodległych Państw (WNP), Szanghajskiej Organizacji Współpracy (z udziałem Chin, Kazachstanu, Kirgistanu, Rosji, Tadżykistanu i Uzbekistanu) oraz podejmowaniu na forum ONZ starań w celu uchwalenia uniwersalnie uznawanego kodeksu norm i zasad prawa międzynarodowego w przestrzeni informacyjnej. Praktyczny wymiar tych reguł można sprowadzić do osiągnięcia kilku efektów strategicznych: militarnego odstraszania, zdolności do projekcji siły, stworzenia systemu odporności na agresję informacyjną, zarządzania konfliktami informacyjnymi oraz utrzymania sił i środków walki informacyjnej w stałej gotowości.

**Część 4. (Środki budowy zaufania)** to najkrótsza część dokumentu towarzysząca deklaracji, że prowadząc operacje w przestrzeni informacyjnej, Siły Zbrojne będą się starały rozwijać środki budowy zaufania. Obejmują one:

„1. wymianę koncepcji bezpieczeństwa w przestrzeni informacyjnej,

2. wymianę informacji na temat krytycznych wydarzeń i zagrożeń w przestrzeni informacyjnej oraz podjętych środków,

3. konsultacje w sprawie działań w przestrzeni informacyjnej, które mogłyby mieć znaczenie dla stron oraz współpracy w rozwiązywaniu konfliktów wojennych".

W **Konkluzji** podkreślono: „Siły Zbrojne Federacji Rosyjskiej będą się starały maksymalnie wykorzystać możliwości przestrzeni informacyjnej w celu wzmocnienia obronności kraju, odstraszania i prewencji konfliktów wojennych, współpracy wojskowej oraz budowania międzynarodowego bezpieczeństwa informacyjnego dla dobra wspólnoty globalnej".