Tomasz R. Aleksandrowicz

Wywiad jako narzędzie w koncepcji nowych wojen. Casus konfliktu ukraińskiego

Słowa kluczowe:
wojna informacyjna, nowe wojny, doktryna rosyjska, służby specjalne, konflikt ukraiński

Wprowadzenie. Czym jest wojna w XXI wieku?

W 1625 r. w Paryżu ukazało się dzieło Huig de Groota (Grocjujsza) *De iure belli ac pacis*. Już sam tytuł tego wiekopomnego dzieła wskazywał, że w prawie narodów obowiązują dwa porządki prawne: jeden, regulujący stan wojny, i drugi, obowiązujący w czasie pokoju. Wojna i pokój były zatem stosunkowo precyzyjnie rozdzielone. Stan taki trwał przez stulecia.

Początek XXI wieku przyniósł radykalne zmiany w środowisku bezpieczeństwa. Można wskazać dwa główne czynniki sprawcze tych zmian: postępujące procesy globalizacyjne i rewolucję informacyjną, będącą m.in. jedną z podstaw rewolucji w sprawach wojskowych (RMA). Z teoretycznego i praktycznego punktu widzenia musimy zmierzyć się z nowymi zjawiskami, do czego – jak wskazał to otwarcie jeden z dowódców NATO – nie jesteśmy przygotowani. Stare, dobrze znane i powszechnie rozumiane pojęcia jak „wojna" czy „konflikt zbrojny" zyskały nowe konotacje; znane od dawna sposoby działania dzięki nowym technologiom zyskały nowy wymiar, jak np. taktyka typu swarming. Współcześnie termin „wojna" ma znacznie więcej wspólnego z rozumieniem Sun Tzu niż klasyczną Clausewitzowską teorią wojny. Wreszcie, powstało nowe środowisko walki, cyberprzestrzeń, a walka informacyjna, szczególnie prowadzona w środowisku sieciowym, nabrała większego znaczenia niż

kiedykolwiek. Wszystkie aspekty tych zmian stanowią wyzwanie zarówno dla nauk o bezpieczeństwie, jak i praktyki.

Analizując współczesne konflikty zbrojne należy odnotować dwie istotne tendencje[1]. Po pierwsze, o ile w 1989 r. aktorzy niepaństwowi występujący jako strona konfliktu zbrojnego ponosili odpowiedzialność za 20% ogólnej liczby ofiar śmiertelnych, to w 2008 r. odsetek ten wzrósł do 80%. Po wtóre, konsekwentnie od początku XX stulecia wzrasta odsetek ofiar śmiertelnych wśród ludności cywilnej (niekombatantów) – na przełomie XX i XXI wieku wynosił on od 80 do 90% ogólnej liczby ofiar[2]. Analiza przytoczonych powyżej danych pozwala na postawienie kilku wniosków.

Zdaje się przemijać epoka wojen toczonych przez masowe armie reprezentujące państwa. Operacje militarne nie stanowią już domeny rządów ani ich przedstawicieli[3]. Coraz częściej prowadzą je niepaństwowe grupy zbrojne, definiowane jako zorganizowane i uzbrojone siły opozycyjne, motywowane czytelnymi celami politycznymi, działające niezależnie od państwa. Grupy te posiadają efektywna strukturę dowodzenia i opisywane są jako partyzantka, milicja, organizacje paramilitarne, organizacje samoobrony, a także grupy terrorystyczne. Od 2008 r. do tej kategorii włącza się także grupy zbrojne motywowane celami kryminalnymi, które – jak np. w Meksyku czy Kolumbii – mogą rzucić wyzwanie i toczyć wyrównaną walkę z podmiotami państwowymi[4]. Powołując się na dane Institute for Strategic Studies, Bolesław Balcerowicz podaje, iż liczba niepaństwowych grup zbrojnych wynosiła w 2007 r. ponad 340, w tym 260 działających aktywnie, a większe grupy łącznie liczyły ok. 800 tys. członków wobec 20 mln żołnierzy regularnych państwowych sił zbrojnych w skali globalnej[5]. Bolesław Balcerowicz stawia w związku z tym

---

1 Zob.: T. Aleksandrowicz, *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 87 i n.

2 E. Hobsbawm, *Globalisation, Democracy and Terrorism*, London 2007, s. 17 i n.

3 Tamże, s. 17.

4 Jak zauważa R.D. Kaplan z think – tanku *Stratford. Global Intelligence*, liczba ofiar śmiertelnych konfliktu w Meksyku związanego z akcjami zbrojnymi karteli narkotykowych w latach 2006 – 2011 sięgnęła 47 000. Dla porównania: liczba ofiar konfliktu wewnętrznego w Syrii w marcu 2012 osiągnęła liczbę 8 000. Zob.: R.D. Kaplan, *With the Focus on Syria, Mexico Burns*, March 28, 2012, http://www.stratfor.com/analysis/focus-syria-mexico-burns-robert-d-kaplan?utm_source=freelist-f&utm_medium=email&utm_campaign=20120328&utm_term=kaplan&utm_content=readmore&elq=a5584048431f433c8422ea90c75183f7 (28.03.2012).

5 B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Warszawa 2010, s. 44. Por. na ten temat: C. Brudelein, *The Role of Non – State Actors in Building Human Security:*

tezę o zacieraniu się granic pomiędzy wojną, przestępczością zorganizowaną i gwałceniem praw człowieka[6].

Zanika pojęcie frontu i obraz konfliktu zbrojnego toczonego przez dwie stające naprzeciw siebie masowe armie. Przyjmując za zasadną tezę o braku wojen pomiędzy rozwiniętymi państwami demokratycznymi, trudno jest równocześnie wykluczyć całkowicie możliwość wybuchu „klasycznej" wojny pomiędzy państwami słabiej rozwiniętymi technologicznie. Wystarczy wskazać w tym kontekście na starcia zbrojne pomiędzy Rosją a Gruzją w 2008 r., by jednoznacznie stwierdzić, iż „klasyczna wojna" nie jest jeszcze w skali globu niemożliwa.

Nie będzie zatem przesadą stwierdzenie, iż największy wpływ na zmianę sposobów prowadzenia konfliktów zbrojnych mają praktyczne rezultaty rewolucji informacyjnej rozumiane jako radykalne zwiększenie możliwości pozyskiwania, przetwarzania, analizy i przekazywania informacji, a w rezultacie – koordynacji działań poszczególnych elementów składowych biorących udział w konkretnym przedsięwzięciu. Z tego punktu widzenia współczesne technologie informacyjne umożliwiły praktyczna realizację postulatów strategicznych Sun Tzu i pełne wykorzystanie jego myśli na współczesnym polu walki.

Zarysowane powyżej zmiany skłaniają wielu teoretyków i praktyków do dokonania rewizji szeregu pojęć, które w nauce były od dawna ugruntowane, od niedawna zaś ich konotacje zaczęły budzić wątpliwości. Operowanie nieostrymi pojęciami, jak słusznie zauważa Bolesław Balcerowicz, nie służy dobremu komunikowaniu się[7]. Przegląd literatury dowodzi, że bardzo często pojęciami takimi jak wojna czy konflikt zbrojny posługiwano się w pewnej mierze intuicyjnie, dodając różnego rodzaju przymiotniki (np. zimna wojna) czy tworząc *de facto* nowe pojęcia nie podając ich precyzyjnej definicji (np. *Global War on Terror*)[8]. Wywoływało to (i wywołuje nadal) szereg nieporozumień, terminologicznego i metodologicznego zamętu. Trudno np. zgodzić się z tezą jednego z badaczy głoszącą, iż „współczesna (XXI wiek) wojna legalizuje terroryzm jako równoprawną z innymi dotychczas uznawanymi za dopuszczalne metodę

the Case of Armed Groups in Infra – State Wars, Geneva Center for Human Dialog, May 2000, http://www.hdcentre.org/files/the%20role%20of%20non-state%20actors.pdf (28.03.2012).

6 B. Balcerowicz, *O pokoju. O wojnie. Między esejem a traktatem*, Warszawa 2013, s. 87.

7 Tamże, s. 81.

8 Zob. M.L. Dudziak, *War Time. An Idea, It's History, It's Consequences*. Oxford 2012.

prowadzenia konfliktu zbrojnego" i uznającą terroryzm za „nowy paradygmat wojny"[9].

Stanisław Koziej w nowym wydaniu „Teorii sztuki wojennej" stwierdza wprost, że „zmiany warunków polityczno – militarnych oraz gwałtowny rozwój środków walki zbrojnej wprowadzają wiele nowych elementów do całej sztuki wojennej. Pojawia się potrzeba ponownego przejrzenia i skorygowania niektórych istniejących do tej pory poglądów, koncepcji, ustaleń. Dotyczy to także sfery pojęciowej. Niektóre z pojęć zmieniają swoje znaczenie, mają też miejsce całkiem nowe zjawiska, które muszą znaleźć swoje odzwierciedlenie w terminologii"[10]. Wtóruje mu Bolesław Balcerowicz postulując dokonanie przeglądu znaczeniowego takich pojęć, jak konflikt między państwami, przemoc zbrojna, organizacja czy siły zbrojne[11].

Konflikt ukraiński

Problemy te zyskały na znaczeniu w rezultacie kryzysu ukraińskiego. Czy pomiędzy Ukrainą a Rosją toczy się wojna? Czy organizowanie, uzbrajanie, wsparcie w środkami walki informacyjnej i klasycznym uzbrojeniem tzw. zielonych ludzików przez Moskwę należy traktować jako wojnę, prowadzenie działań zbrojnych, przemoc zbrojną? Pytanie dotyczy, rzecz jasna, statusu Rosji w tym konflikcie, bowiem z punktu widzenia Ukrainy mamy do czynienia z wojną domową/powstaniem. To problem dramatycznie pilny, powstaje bowiem nieuchronne pytanie, w jaki sposób NATO będzie reagować na tego typu działania Rosji podejmowane przeciwko państwu członkowskiemu NATO. Pytanie pozostaje bez odpowiedzi, co przyznaje nawet dowódca sił NATO w Europie, gen. Philip Breedlove[12]. Na marginesie niejako można stwierdzić, iż działania Rosji wobec Ukrainy wypełniają znamiona agresji określone w przywołanej powyżej Definicji Agresji (wysyłanie przez lub w imieniu jakiegoś państwa uzbrojonych band, grup, sił nieregularnych lub najemnych, które dopuszczają się aktów zbrojnych o takiej doniosłości przeciwko innemu państwu, że oznaczają akty wyżej wymienione lub oznaczają mieszanie

[9] K. Karolczak, *Terroryzm. Nowy paradygmat wojny*. Warszawa 2010, s. 17.

[10] S. Koziej, *Teoria sztuki wojennej*. Warszawa 2011, s. 9.

[11] B. Balcerowicz, *O wojnie, o pokoju…*, s. 85–86.

[12] http://www.defence24.pl/analiza_nato-nie-ma-strategii-dzialania-na-wojne-hybrydowa (15.10.2014).

się do nich). Czy podjęcie tego typu działań przeciwko np. Estonii oznacza operacjonalizację art. 5 Paktu?[13]

Analizując rosyjskie działania o charakterze hybrydowym na Ukrainie, Krzysztof Wąsowski wymienia wśród atrybutów konfliktu charakterystycznych dla metod hybrydowych także wojnę informacyjną, wskazując jako środki i metody z arsenału działań wojny hybrydowej „zmasowaną kampanię mającą uzasadnić rosyjskie prawa do aneksji Krymu, próby przekonania lokalnej ludności, że istnieją poważne zagrożenia ze strony władz centralnych Ukrainy, które faktycznie nigdy nie pojawiły się w polityce Kijowa wobec Krymu. Przekaz zewnętrzny rosyjskich mediów na temat faktycznego udziału Rosji w konflikcie"[14]. Co ciekawe, przywołany autor jako odrębne atrybuty wskazuje wojnę psychologiczną („Intensywne manewry i gromadzenie regularnych wojsk rosyjskich przy granicach z Ukrainą stosownie do przebiegu konfliktu i taktycznych potrzeb") oraz niejednoznaczność („Pierwotnie stanowcze zaprzeczanie bezpośredniej interwencji rosyjskich żołnierzy („zielone ludziki") na Ukrainie, a następnie oficjalne jej potwierdzenie przez Władimira Putina, w momencie, kiedy okazało się to przydatne do osiągnięcia taktycznych celów w polityce wewnętrznej")[15].

Nie sposób przy tym nie zauważyć, że Kreml za wszelką cenę stara się utrzymać ten konflikt poniżej progu wojny, unikając otwartego zaangażowania swoich sił zbrojnych. *De facto* rosyjska interwencja zbrojna na Ukrainie została ograniczona do działań tzw. zielonych ludzików, których pododdziały formalnie i oficjalnie nie były częścią armii rosyjskiej Thimothy Thomas dodaje do tego prowadzenie działań w taki sposób, aby uniknąć ponoszenia za nie odpowiedzialności, podając jako przykład sprawę zestrzelenia nad Ukrainą malezyjskiego samolotu pasażerskiego 17 lipca 2014 r.[16]

---

[13] Zob.: T. Aleksadrowicz, *Gdzie leży czerwona linia? Strategia wobec Rosji*, http://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-strategia-wobec-rosji (15.10.2014).

[14] K. Wąsowski, *Istota i uniwersalność rosyjskiego modelu wojny hybrydowej wykorzystanego na Ukrainie*, „Sprawy Międzynarodowe" 2015, nr 2 (wydanie monotematyczne).

[15] Tamże. Zob. też: M. Trudolyubov, *Russia's Hybrid War*, The New York Times February 24, 2016, http://www.nytimes.com/2016/02/25/opinion/russias-hybrid-war.html (26.02.2016).

[16] Zob. T. Thomas, *Russia's 21st Century Information War: Working to Understand and Destabilize Populations*, Defence Strategic Communications, „The Official Journal of the NATO Strategic Communications Centre of Excellence" Winter 2015, vol. 1, nr 1, s. 18.

Wojny nowej generacji

Analizując rosyjską myśl strategiczną należy zauważyć, iż konflikt ukraiński mieści się w kategorii tzw. nowych wojen lub koncepcji „wojen nowej generacji", której głównym założeniem jest skoordynowane użycie środków dyplomatycznych, wojskowych, humanitarnych, ekonomicznych, technologicznych i informacyjnych. Istotną rolę przypisano w niej służbom specjalnym. W tej koncepcji, jak wskazuje Andriej Monojło, walka informacyjna spełnia trzy podstawowe funkcje:

- po pierwsze, zaciera granicę pomiędzy wojną a pokojem, co pozwala na zaatakowanie państwa bez deklarowania wojny i brak oskarżeń o dokonanie agresji (napaści zbrojnej);
- po drugie, pozwala na wywołanie chaosu w zaatakowanym państwie poprzez prowokowanie konfliktów lokalnych i jego destabilizację;
- po trzecie, pozwala na wprowadzenie „blokady informacyjnej" poprzez izolację utrudnienie/odcięcie zaatakowanego obszaru od dostępu do międzynarodowych źródeł informacji (międzynarodowych mediów[17].

W ocenie szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej gen. armii. Genadija Gierasimowa, środki walki informacyjnej mają być stosowane m.in. w celu wzmocnienia i wykorzystania „potencjału protestu", a więc opozycji wewnętrznej w danym kraju, w tym poprzez stymulowanie ruchów antysystemowych w społeczeństwach danego państwa. Cel ten ma być osiągany za pomocą „miękkiej siły", rozumianej jako technologia walki geopolitycznej pozwalająca na uzyskanie dominacji nad wrogim państwem poprzez niejawne przejmowanie kontroli nad mechanizmami formowania polityki, podejmowania decyzji gospodarczych, uzyskania wpływu na procesy kulturowe. Koncepcja wojen nowej generacji zakłada m.in.:

- prowadzenie działań asymetrycznych w celu osłabienia przeciwnika i stworzenia sprzyjających warunków ułatwiających interwencję poprzez zastosowanie środków informacyjnych, psychologicznych, dyplomatycznych i ekonomicznych;
- dezorientacja władz państwowych za pomocą jawnych i tajnych operacji specjalnych prowadzonych za pośrednictwem mediów, dyplomacji i organizacji pozarządowych; operacje taki polegają na wykorzystywaniu istniejących sprzeczności i konfliktów wewnętrznych, podsycaniu ich i stymulowaniu;

[17] C. Johnston, *Russia's Info-War: Theory and Practice*, Issue Alert 22/2015, European Union Institute for Security Studies, April 2015.

- zastraszanie, oszukiwanie i korumpowanie elit;
- stosowanie środków propagandowych wpływających na wzrost nastrojów niepewności i poczucia zagrożenia w społeczeństwie.[18].

Wojny informacyjne („nowej generacji") toczą się o zasoby społeczne. Według Siergieja Rastorgujewa z Instytutu Problemów Bezpieczeństwa Informacyjnego Uniwersytetu Łomonosowa w Moskwie „kluczem do tych zasobów są elity i media przeciwnika. Ważnym czynnikiem jest posiadanie wśród tych elit i mediów niezbędnej masy agentów wpływu, których agresor rekrutuje spośród osób o egoistycznym bądź niewolniczym światopoglądzie. (…) strategia wojny informacyjnej zawsze łączy mnóstwo powiązanych ze sobą wzajemnie taktycznych operacji informacyjnych. Globalny cel tych operacji nie zawsze jest widoczny. (…) wojna informacyjna oznacza ofensywę, zaś o skuteczności działań decyduje realny potencjał sił i środków oddziaływania lub jego brak"[19].

Rosyjscy teoretycy podkreślają także, iż walka informacyjna powinna „przeformatować mentalną przestrzeń społeczeństwa" i „ma przede wszystkim na celu zdemoralizowanie społeczeństwa oraz stworzenie warunków sprzyjających odrzuceniu religii i wartości duchowych charakterystycznych dla tożsamości narodowej i kultury danego kraju. Konieczne jest także wytworzenie wśród ludności atakowanego kraju negatywnego stosunku do własnego dziedzictwa kulturowego i tradycji historycznych"[20]. Jako cel zasadniczy wskazuje się podważenie międzynarodowego znaczenia danego państwa oraz spowodowanie szkód w najważniejszych dla niego sferach działalności (polityka, gospodarka, obronność, kultura, etc.)[21].

Peter Pomerantsev i Michael Weiss, próbując wyliczyć sposoby stosowane przez Kreml we współczesnej walce/wojnie informacyjnej, wymieniają:

- kreowanie stanu zagrożenia i propagowanie wszelkiego rodzaju teorii spiskowych, stawiających Rosję w roli zaatakowanego i zmuszonego przez przeciwników do obrony;

---

[18] Zob.: M. Wojnowski, *Koncepcja wojen nowej generacji w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13 (7), s. 13 i n.

[19] O.Nazarow, *Informacionnyje wojny – ugroza dlia ciwilizacii,* „Litieraturnaja Gazieta" 2013, nr 42. Cyt. za: J. Darczewska, *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, *Wydanie specjalne – Wojna hybrydowa,* s. 62–63.

[20] M. Wojnowski, *Koncepcja wojen nowej generacji…*, s. 19.

[21] Tamże.

- wysokie nakłady finansowe na wykorzystywane w walce informacyjnej środki masowego przekazu: ponad 300 mln USD rocznie, z czego 41% na kanały francusko- i niemieckojęzyczne oraz wykorzystywanie platform mediów społecznościowych;
- wsparcie dla ugrupowań skrajnie prawicowych, autorytarnych w krajach demokratycznych (a więc przeciwnie, niż w latach zimnej wojny, gdy ZSRR finansował partie lewicowe, lewackie i anarchistyczne);
- sprawne wykorzystywanie zasad liberalnej demokracji na Zachodzie;
- wykorzystywanie do własnych działań propagandowych ekspertów z państw demokratycznych, choćby poprzez zaproszenia do udziału w spotkaniach Klubu Wałdajskiego[22];
- wykorzystywanie komercyjnych firm Public Relations i lobbyingowych[23].

W działaniach prowadzonych przez Federację Rosyjską w związku z konfliktem ukraińskim można wyodrębnić wszystkie aspekty walki informacyjnej. James R. Clapper, Director of National Intelligence, przedstawiając 26 lutego 2015 r. ocenę amerykańskiego wywiadu bieżących zagrożeń globalnych sprzed Senackim Komitetem do spraw Sił Zbrojnych podkreślił, że Rosja podniosła walkę informacyjną na nowy poziom, podsycając antyamerykańskie i antyzachodnie sentymenty zarówno w samej Rosji, jak i na całym świecie. Rosyjskie media państwowe publikują fałszywe i mylące informacje w celu zdyskredytowania Zachodu, podważając jego jedność w sprawach rosyjskich i budując poparcie dla rosyjskiego stanowiska[24].

Widoczna jest także aktywność rosyjskich i prorosyjskich trolli w internecie, publikujących komentarze pod artykułami na portalach informacyjnych, aktywnych na portalach społecznościowych.

Z *Raportu z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r.* wynika, że przedsięwzięcia realizowane w Polsce przez rosyjskie służby specjalne były uwarunkowane głównie konfliktem ukraińskim i zostały podporządkowane strategii propagandowej Kremla. Główne kierunki działań w tym zakresie obejmowały, wg. *Raportu*, następujące elementy:

---

[22] Klub Wałtajski to coroczne spotkanie światowej sławy ekspertów ds. Rosji. Powstał w 2004 r. Spotkania organizowane są w Wielkim Nowogrodzie, niedaleko jeziora Wałdaj, stąd też nazwa – Klub Wałtajski.

[23] P. Pomerantsev, M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. A Special Report presented by The Interpreter, a Project of the Institute of Modern Russia, New York 2014, s. 6.

[24] http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (3.06.2015).

- dyskredytację stanowiska Polski i innych państw członkowskich NATO w kwestii kryzysu ukraińskiego;
- akcentowanie skomplikowanych doświadczeń historycznych w stosunkach polsko – ukraińskich w celu wywoływania antagonizmów pomiędzy społeczeństwami obu krajów;
- uwypuklanie i kreowanie podziałów wśród państw członkowskich Unii Europejskiej i NATO;
- eksponowanie, a niekiedy inspirowanie stanowisk polityków eurosceptycznych, krytykujących nałożone na Federację Rosyjską sankcje;
- działania na rzecz konsolidacji środowisk prorosyjskich w Polsce[25].

Do realizacji tych przedsięwzięć Rosjanie wykorzystywali zarówno rosyjskie media, jak i obywateli RP reprezentujących prorosyjską postawę i w niektórych przypadkach opłacanych przez instytucje Federacji Rosyjskiej. Jak stwierdzają Autorzy *Raportu*, „Jednym z aspektów wojny informacyjnej prowadzonej przez Federację Rosyjską jest próba kształtowania prorosyjskich oraz antyukraińskich poglądów wśród polskiej opinii publicznej za pośrednictwem internetowych blogów, portali i serwisów informacyjnych. W tym celu wykorzystywane są osoby, które można przypisać do następujących grup:

- działające na zlecenie i opłacane za wykonaną pracę, tj. zamieszczanie wpisów, komentarzy ukazujących odpowiednie osoby i wydarzenia w pozytywnym świetle, wykorzystując do tego wybrane i przywołane w odpowiednim kontekście zmodyfikowane fakty,
- tzw. *useful idiots*, czyli osoby prowadzące profile na portalach społecznościowych, czy też blogi osobiste, na których zamieszczane są 'pożądane' teksty, oraz inne osoby inspirowane do powielania dezinformacji.

'Pożądane' informacje i komentarze pisane są według podobnego szablonu, zwykle mają obszerną treść i są wysoko oceniane przez innych 'użytkowników'. Opinie stojące w opozycji do treści zleconych są źle oceniane przez innych 'dyskutantów'. Wpisy w znacznym stopniu są kopią poprzednich, zamieszczanych na innych portalach, często w niewielkim, kilkusekundowym odstępie czasu"[26].

Trudno nie zauważyć, iż mamy do czynienia ze starannie przygotowaną i zaplanowaną operacją. Rosja w bardzo umiejętny sposób wykorzystuje różnego rodzaju narzędzia walki informacyjnej. Jeśli dokonamy

[25] Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r. http://www.abw.gov.pl/pl/pobierz/raporty/575,Raporty.html (3.06.2015).

[26] Tamże, s. 15.

analizy choćby wpisów na Twitterze, okaże się, że rosyjskie interesy prezentowane są tam przez cały szereg podmiotów. Po pierwsze, oficjalne konta rosyjskich instytucji, np. ministerstwa spraw zagranicznych FR. Druga linia to konta prowadzone przez rosyjskie media elektroniczne i tradycyjne, choćby sztandarowa agencja propagandy rosyjskiej *Russia Today*. Potem zaczynają się fałszywki, bez żenady podające informacje nieprawdziwe lub przekłamane (jak ta, wedle której samolot z Janukowyczem na pokładzie miał wylądować w Dubaju). Wreszcie – „piechota informacyjna": konta prowadzone przez pojedynczych użytkowników Twittera z różnych krajów, którzy albo twardo trzymają stronę Rosji, albo są zdecydowanie antyukraińscy, albo po prostu antyamerykańscy czy antyunijni.

W Rosji istnieją całe „fabryki internetowych trolli", pracujących w systemie ciągłym, których zadaniem jest publikowanie komentarzy, wpisów i prowadzenie debat na różnego rodzaju portalach społecznościowych, informacyjnych czy blogach[27]. Jeden z badaczy Internetu, Lawrance Alexander, zidentyfikował ponad 20 000 kont na Twitterze prowadzonych właśnie przez tego typu opłacanych przez Kreml trolli. Daje to pojęcie o skali prowadzonej operacji[28]. Powstały też repozytoria zdjęć i rycin wykpiwających polityków zachodnich i ukraińskich, prezentujących antyrosyjskie stanowiska[29].

Rosja prowadzi zatem bardzo aktywne działania w obszarze aktywizmu i haktywizmu; w widoczny sposób przybrały one na sile po rozpoczęciu rosyjskiej agresji na Ukrainę. Stosując programy analityczne NodeXL i Gephi, Lawrence Alexander zidentyfikował ok. 3000 kont na Twitterze, z których prowadzona jest prorosyjska kampania propagandowa, dezinformacyjna i psychologiczna; badacz stwierdza, że mamy do czynienia z prawdziwą „armią trolli"[30]. Badania te potwierdzają słowa Marata Burkharda, opisującego funkcjonowanie „fabryki trolli", mieszczącej się w St. Petersburgu, którego oficjalna nazwa brzmi Internet Research Center. Zatrudnieni tam blogerzy pełnią 12 godzinne dyżury w systemie zmia-

---

[27] Istnienie takich instytucji potwierdził jeden z jej byłych pracowników. Zob.: *One Professional Russian Troll Tells All*, http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html?utm_content=buffer9f046&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer (3.06.2015).

[28] Zob.: *Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign*, https://globalvoicesonline.org/2015/04/02/analyzing-kremlin-twitter-bots (3.06.2015).

[29] Na przykład, http://вштабе.рф/index.php?utm_content=bufferd69d4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer (3.06.2015).

[30] L. Alexander, *Social Network Analysis*…

nowym przez 7 dni w tygodniu, 24 godziny na dobę. Ich zadaniem jest publikowanie wpisów i komentarzy na forach internetowych, prowadzenie kont na portalach społecznościowych, dyskusje z internautami[31]. Oczywiście, treści publikowane przez pracowników Internet Research Center muszą zawierać określone tezy. Z raportu opublikowanego przez NATO Strategic Communication COE wynika, że Rosjanie wykorzystują media społecznościowe jako efektywne narzędzie dezinformacji i wywierania wpływu na atakowane społeczeństwo. Główne kierunki ataku informacyjnego zawierają uzasadnienie polityki Kremla, dyskredytację atakowanego rządu i niszczenie społecznego poparcia dla niego[32].

Nie oznacza to porzucenia przez Rosjan klasycznych metod wywiadowczych, stosowanych przez Kreml od dziesięcioleci. Agentura, agentura wpływu, ideowcy przekonani o rosyjskich racjach, tzw. pożyteczni idioci. To znane od lat, sprawdzone mechanizmy, jak np. wsparcie partii politycznych o nastawieniu prorosyjskim, podsycanie sporów i kontrowersji, wykorzystywanie różnic politycznych i pluralizmu w życiu politycznym państw demokratycznych. W ten sposób rozczarowanie polityką Unii Europejskiej na Węgrzech zaowocowało prorosyjską polityką Victora Orbana; widać grę wykorzystującą narastające w Europie nastroje strachu przed islamizacją. Jasno trzeba powiedzieć: poparcie dla polityki Putina nie jest równoznaczne z byciem agentem rosyjskiego wywiadu. Jednak rosyjski wywiad dyskretnie wspiera ludzi popierających na Zachodzie politykę Putina.

Podstawy doktrynalne rosyjskich wojen nowej generacji

Koncepcje wojen informacyjnych znajdują swoje odzwierciedlenie zarówno w obowiązujących dokumentach strategicznych Federacji Rosyjskiej, jak i realizowanych strategiach oraz w praktyce, czego dowodzą choćby działania FR związane z konfliktem na Ukrainie.

Kwestie wojen informacyjnych Kreml traktuje bardzo poważnie; informacja stanowi wedle ich dokumentów strategicznych skuteczną broń wykorzystywaną wobec przeciwnika zewnętrznego, jak też narzędzie do

[31] *One Professional Russian Troll Tells All* http://www.rferl.mobi/a/how-to-guide-russian-trolling-trolls/26919999.html?utm_content=buffer9f046&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer (11.04.2016).

[32] *Internet Trolling as a hybrid warfare tool: the case of Latvia. Results of the Study*, NATO STRATCOM Centre of Excellence, http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0 (11.04.2016).

panowania nad własnym społeczeństwem. Dowodem na to jest podpisana 26 grudnia 2014 r. przez prezydenta Władimira Putina nowelizacja Doktryny wojennej Federacji Rosyjskiej[33]. Uwagę zwraca przede wszystkim fakt, iż o ile w dokumentach zachodnich mowa jest raczej o środkach prowadzenia walki/wojny/konfliktu (*warfare*), to w ich rosyjskich odpowiednikach mówi się wprost o wojnie informacyjnej.

Tak więc, wymieniając niebezpieczeństwa i zagrożenia wojenne dla Federacji Rosyjskiej wśród „głównych zewnętrznych niebezpieczeństw wojennych" Doktryna wymienia „wykorzystywanie technologii informacyjnych i komunikacyjnych w celach wojskowo – politycznych do prowadzenia działań sprzecznych z prawem międzynarodowym, skierowanych przeciwko suwerenności, niezawisłości politycznej, integralności terytorialnej oraz stanowiących zagrożenie dla międzynarodowego pokoju, bezpieczeństwa, stabilności globalnej i regionalnej". Jako jedno z głównych wewnętrznych niebezpieczeństw wojennych Doktryna wskazuje na „działalność w zakresie oddziaływania informacyjnego na społeczeństwo, w pierwszym rzędzie na młodych obywateli, mająca na celu przerwanie historycznych, duchowych i patriotycznych tradycji w zakresie obrony Ojczyzny." Z kolei wśród podstawowych zagrożeń wojennych Doktryna wymienia „zakłócanie pracy systemów państwowego i wojskowego zarządzania Federacją Rosyjską, naruszanie jej strategicznych sił jądrowych, systemów powiadamiania o ataku rakietowym, kontroli przestrzeni kosmicznej, obiektów magazynowania ładunków jądrowych, energetyki atomowej, przemysłu atomowego, chemicznego, farmaceutycznego oraz medycznego, jak również innych potencjalnie niebezpiecznych obiektów."

Charakteryzując współczesne konflikty wojenne, Doktryna wyraźnie odwołuje się do koncepcji wojen hybrydowych oraz wojen „buntowniczych" (por. niżej). Współczesne konflikty zbrojne charakteryzują się m.in. następującymi cechami i właściwościami:

- kompleksowym wykorzystaniem „siły militarnej, politycznych, ekonomicznych, informacyjnych i innych środków o charakterze pozamilitarnym, realizowanych przy wykorzystaniu potencjału protestacyjnego ludności oraz sił prowadzących operacje specjalne";
- jednoczesnym oddziaływaniem na nieprzyjaciela na całej głębokości jego terytorium w globalnej przestrzeni informacyjnej, w przestrzeni powietrzno – kosmicznej, na lądzie oraz na morzu".

W kontekście naszych rozważań należy podkreślić fakt, iż przestrzeń informacyjna nie tylko została oficjalnie za piąte środowisko walki (po

[33] Tekst polski: „Bezpieczeństwo Narodowe" 2015, nr III, lipiec–wrzesień 2015 r.

lądzie, morzu, przestrzeni powietrznej i kosmicznej), ale wręcz wymieniona na pierwszym miejscu, co dodatkowo podkreśla znaczenie, jakie twórcy Doktryny przywiązują do wojny informacyjnej. Konsekwencją takiego ujęcia jest kształt określonej w Doktrynie polityki wojennej Federacji Rosyjskiej. Wśród podstawowych zadań Federacji Rosyjskiej w zakresie odstraszania i zapobiegania konfliktom wojennym w omawianym dokumencie wymienia się m.in.:

- ocenę i prognozowanie rozwoju sytuacji wojskowo-politycznej na szczeblu globalnym i regionalnym, jak również stanu stosunków międzypaństwowych w obszarze wojskowo-politycznym z wykorzystaniem współczesnych środków technicznych i technologii informacyjnych;
- neutralizację potencjalnych niebezpieczeństw wojennych i zagrożeń wojennych przy pomocy środków politycznych, dyplomatycznych i innych środków pozamilitarnych;
- stworzenie warunków zapewniających obniżenie ryzyka wykorzystania technologii informacyjnych i komunikacyjnych do celów wojskowo-politycznych w ramach realizacji działań sprzecznych z prawem międzynarodowym i skierowanym przeciwko suwerenności, niezawisłości politycznej, integracji terytorialnej państw oraz stanowiących zagrożenie dla pokoju międzynarodowego, bezpieczeństwa, stabilności globalnej i regionalnej.

Realizacji tych zadań służyć ma rozwój systemu wojennego, budowa i rozwój sił zbrojnych oraz innych wojsk i służb oraz zabezpieczenie wojskowo-gospodarcze obrony. W tym kontekście doktryna wymienia następujące zadania:

- doskonalenie systemu bezpieczeństwa informacyjnego sił zbrojnych oraz innych wojsk i służb;
- efektywne zapewnienie bezpieczeństwa informacyjnego sił zbrojnych oraz innych wojsk i służb;
- rozwój sił i środków walki informacyjnej;
- jakościowe doskonalenie środków wymiany informacyjnej na bazie wykorzystania współczesnej technologii i standardów międzynarodowych, jak również jednolitej przestrzeni informacyjnej sił zbrojnych oraz innych wojsk i służb jako części przestrzeni informacyjnej Federacji Rosyjskiej.

Analiza treści Doktryny wojennej Federacji Rosyjskiej uzasadnia pytanie o źródła takiego rozumienia kwestii walki i wojny informacyjnej, widać bowiem wyraźnie, że nie są one traktowane jedynie jako narzędzia czy środki działania, lecz wręcz jako samodzielne, wyodrębnione zjawisko.

Analizując dostępne w rosyjskiej literaturze przedmiotu definicje tego pojęcia Michał Wojnowski zauważa, że charakteryzują się one uniwersalnością i odnoszą zarówno do działań prowadzonych w czasie wojny (rozumianej klasycznie), jak i w czasie pokoju. Co więcej, określenie to nie funkcjonuje w dyskursie wojskowym, w którym pojawiają się terminy „konfrontacja informacyjna" i „walka informacyjna"; pojęcie „wojna informacyjna" jest używane przede wszystkim przez uczonych i analityków cywilnych. Próbując znaleźć wspólne elementy w analizowanych przez siebie definicjach przywołany autor pisze, iż „rosyjska wojna informacyjna stanowi całokształt różnorodnych, czasowo skoordynowanych działań prowadzonych przez wojsko, jak i cywilne służby specjalne na wielu obszarach w celu zneutralizowania przeciwnika przy pomocy narzędzi informacyjno-technicznych i informacyjno-psychologicznych"[34].

Analiza przytaczanych przez Michała Wojnowskiego definicji nakazuje uznać poprawność powyższej konstatacji. Tak np. płk Siergiej Komow jeszcze w latach 90. definiował walkę informacyjną jako całokształt wsparcia informacyjnego, informacyjnego przeciwdziałania oraz informacyjnej ochrony własnych zasobów, prowadzonych według jednolitego planu w celu zdobycia i utrzymania przewagi informacyjnej nad stroną przeciwną. Z kolei cytowany przez jednego z zachodnich badaczy anonimowy oficer Akademii Wojennej Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej definiował pojęcie konfrontacji informacyjnej jako jedną z form rozwiązywania konfliktu pomiędzy stronami, których celem jest osiągnięcie i utrzymanie przewagi informacyjnej nad oponentem; rezultat ten jest możliwy do osiągnięcia przy pomocy środków informacyjno-technicznych i informacyjno-psychologicznych przez wywieranie wpływu na ośrodki decyzyjne danego państwa, jego system dowodzenia i kontroli, ludność oraz zasoby informacyjne. Warta przytoczenia jest też opinia analityka Ministerstwa Obrony Federacji Rosyjskiej Władimira Cymbała, którego zdaniem pojęcie wojny informacyjnej należy rozpatrywać w dwóch aspektach: szerokim i wąskim. Wojna informacyjna *sensu largo* to według Cymbała – zespół działań stosowanych przez jedno państwo przeciwko ludności cywilnej drugiego państwa lub grupie państw w czasie pokoju. Działania te dotyczą uzyskania wpływu na świadomość społeczną przez naukę, sztukę, kulturę, system edukacji, administrację etc. Działania mieszczące się w tej definicji zobowiązane

[34] M. Wojnowski, *Terroryzm w służbie geopolityki. Konflikt rosyjsko – ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11 (6), s. 79–80.

są prowadzić cywilne służby specjalne, a więc – w warunkach Federacji Rosyjskiej – Federalna Służba Bezpieczeństwa (FSB) i Służba Wywiadu Zagranicznego (SWR). Zadaniem SWR jest zdobycie kontroli nad zasobami informacyjnymi innych państw, sabotowanie rozwoju technologii informatycznych w państwach uznanych za wrogie oraz neutralizowanie systemów komunikacyjnych i sieci informacyjnych przeciwnika; rolą FSB jest natomiast rozbudowywanie i implementacja systemów gwarantujących bezpieczeństwo własnych zasobów informacyjnych. W zapewnieniu bezpiecznej łączności wiodącą rolę odgrywa Federalna Agencja Łączności Rządowej (FAPSI)[35]. Natomiast wojna informacyjna *sensu stricto* oznacza formę działań militarnych mających na celu uzyskanie przewagi informacyjnej nad przeciwnikiem w zakresie rozpowszechniania, wykorzystania i przetwarzania informacji oraz wdrażania efektywnych decyzji pozwalających na osiągnięcie przewagi na polu walki.

Z kolei zdaniem Andrieja Manojło[36] wojna informacyjna to skrajna metoda konfrontacji pomiędzy państwami realizowana różnorodnymi sposobami i metodami wpływu informacyjnego, mająca za zadanie realizację ich strategicznych celów. Podstawową formą prowadzenia wojny informacyjnej są tajne operacje informacyjno-psychologiczne, mające na celu spowodowanie strat w systemach i zasobach informacyjnych przeciwnika oraz psychologiczną obróbkę masowej świadomości danego społeczeństwa, co w konsekwencji ma doprowadzić do destabilizacji państwa i narodu. Wdrażanie różnorodnych czynności przybierających postać operacji informacyjno-psychologicznych ma na celu umożliwienie uzyskania wpływu na system wyobrażeń o świecie charakterystyczny dla narodu lub grup etnicznych danego kraju. Według koncepcji Manojło obiektami ataku informacyjnego mogą być świadomość, wola i emocje społeczeństwa.

---

[35] Uzupełniając wywód Cymbała należy dodać, iż w latach 90. XX stulecia w Federacji Rosyjskiej powołano do życia sieciową strukturę odpowiadającą za prowadzenie wojen informacyjnych, złożoną z cywilnych służb specjalnych, tj. SWR, FSB, FABSI oraz elementy sił zbrojnych, przede wszystkim GRU (wywiad wojskowy). Zob.: T.L. Thomas, *Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, The State Technical Commission and the Military*, „European Security" 1998, nr 7, s. 156–172; zob.: M. Wojnowski, *Terroryzm w służbie geopolityki. Konflikt rosyjsko – ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11 (6), s. 81.

[36] Reasumpcję poglądów tego rosyjskiego politologa, teoretyka walki i wojny informacyjnej i oficera FSB zob.: M. Wojnowski, *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno – psychologicznych w XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12 (7), s. 27–28.

Działania o charakterze informacyjno-psychologicznym należy prowadzić szczególnie podczas takich wydarzeń, jak wybory, referenda, sytuacje kryzysowe, okresy przesileń politycznych i napięć etc. Obiektem ataku staje się infrastruktura informacyjna oraz szeroko rozumiane podmioty odpowiedzialne za kierowanie działaniami w sferze polityki, gospodarki, nauki, i sił zbrojnych danego państwa, co stwarza możliwość niezauważalnego sterowania procesami decyzyjnymi we wszystkich kluczowych sferach. Manojło podkreśla, że operacja informacyjno-psychologiczna składa się z dużej liczby skoordynowanych i zsynchronizowanych w czasie przedsięwzięć, łącznie z cyberatakami; działania te są prowadzone za pomocą broni informacyjnej, a więc takich środków technicznych i technologii informacyjnych, których użycie umożliwia uzyskanie wpływu na przestrzeń informacyjną i zasoby informacyjne przeciwnika, indywidualną i masową świadomość, moralno-psychologiczny i psychofizyczny stan ludności; rosyjski analityk przywołuje w tym miejscu dezinformację, lobbying, propagandę, sterowanie kryzysami, szantaż i kampanie public relations; wszystko to mieści się w ramach zarządzania refleksyjnego[37].

Twórcą koncepcji zarządzania refleksyjnego jest Władimir Lefewr (Vladimir Lefebvre), rosyjski psycholog i matematyk, od lat 70. mieszkający w Stanach Zjednoczonych. Koncepcja powstała w latach 60. XX wieku, a obecnie jest rozwijana na potrzeby rosyjskiej teorii i praktyki walki informacyjnej. Nie wdając się w tym miejscu w szczegóły[38] należy wskazać, iż istotą lefewrowskiej koncepcji zarządzania refleksyjnego jest przyjęcie założenia, iż każdy obiekt tworzy w swojej świadomości nie tylko własny obraz świata materialnego, lecz także posiada zdolność do analizowania własnych myśli i wyobrażeń (autorefleksja lub refleksja pierwszego stopnia). Przy pomocy odpowiednich instrumentów (np. prowokacji, intrygi, kamuflażu etc) można z zewnątrz wpływać na te procesy:

- za pomocą procesu przekazania fałszywej informacji o danej sytuacji lub nieprawdziwego obrazu danego obiektu;
- wykreowania celu dla oponenta;
- sformułowania korzystnej dla siebie doktryny i przekazania jej przeciwnikowi tak, by podejmował on na jej podstawie korzystne dla nas działania;

[37] Tamże, s. 27–28.

[38] Zainteresowany tą problematyką Czytelnik znajdzie je w artykule M. Wojnowskiego *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12 (7), s. 11–36.

- za pomocą neutralizacji dedukcji przeciwnika, czyli jego dezorientacji poprzez wykreowanie kilku fikcyjnych celów uniemożliwiających odkrycie celu rzeczywistego.

Jak wyjaśniał Lefewr (a raczej już Lefebvre) w 2003 r. „Zarządzanie refleksyjne to informacyjny wpływ na obiekty, do których opisania wymagane jest użycie takich terminów jak świadomość i wola. Obiektami tego rodzaju są zarówno pojedynczy ludzie, jak i wspólnoty ludzkie: rodzina, grupa, naród, społeczeństwo, cywilizacja. Termin zarządzanie refleksyjne można rozumieć w dwóch znaczeniach. Po pierwsze, jako sztuka manipulacji ludźmi i wspólnotami ludzkimi. Po drugie, jako specyficzna metoda sterowania społecznego (…) zarządzanie refleksyjne pojawiło się na początku lat sześćdziesiątych, w czasie kiedy powstawała koncepcja wojny informacyjnej. Specyfika tej metody polega na tym, że generowanie informacyjnych efektów jest oparte nie tyle na naturalnej ludzkiej intuicji, ile na specjalnym modelu poddanego kontroli podmiotu (…) Powodzenie zarządzania refleksyjnego w znacznej mierze zależy od jakości modelu podmiotu, który zastosowano. Modele psychologiczne, oparte na tradycyjnych, behawioralnych, a nawet psychoanalitycznych pojęciach, okazały się mało efektywne. Rzecz w tym, że model podmiotu powinien odzwierciedlać nie tylko sferę jego zachowania, lecz także zdolność do pojmowania samego siebie i drugich podmiotów, włączając i te, które próbują uzyskać kontrolę nad jego działaniem, tzn. model powinien być refleksyjny (…). Modele refleksyjne wniosły nowe spojrzenie na wiedzę o człowieku, związane z takimi kategoriami, jak moralność, sumienie i poczucie sprawiedliwości. Pozwalają one na odzwierciedlenie sytuacji, w których ludzie chcą nie tylko uzyskać materialną korzyść, ale także mają nieutylitarne cele, spełniają akty ofiarne, pragnąc wyglądać godnie w oczach własnych, jak i w oczach innych osób”[39].

Szczegółowa analiza przeprowadzona przez Michała Wojnowskiego jednoznacznie wskazuje na poziom recepcji zarządzania refleksyjnego przez rosyjski wywiad wojskowy (GRU), który potraktował koncepcję Lefewra jako narzędzie walki informacyjnej prowadzonej w wymiarze strategicznym dotyczącym sytuacji konfliktowej o charakterze geopoli-

[39] Cyt. za: M. Wojnowski, *Zarządzanie refleksyjne*…, s. 20–21. Warto w kontekście naszych rozważań zaznaczyć, że zacytowany fragment tekstu Lefewra został opublikowany w Moskwie w 2000 r. w zbiorze „Reflieksja” pod redakcją W.J. Lepskija. Sam Lefebvre, pracownik naukowy Uniwersytetu Kalifornijskiego, zajmuje się tworzeniem refleksyjnych modeli sprawców przestępstw, struktur przestępczości zorganizowanej, sekt i organizacji terrorystycznych, prowadzi też badania nad etyką i motywacjami ludzkich zachowań.

tycznym[40]. Zdaniem rosyjskich teoretyków za pomocą technik zarządzania refleksyjnego można dokonać głębokiej transformacji masowej świadomości społeczeństwa i zmienić moralno – psychologiczny stan narodu; wśród metod wywierania wpływu na przeciwnika tak, by spowodować jego reakcje korzystne dla Federacji Rosyjskiej wymienia się:

- metodę nacisków siłowych poprzez demonstracje siły militarnej, tworzenie sojuszy wojskowych, groźby polityczne i gospodarcze, wsparcie dla wewnętrznych sił antyrządowych etc;
- metodę kreowania i przekazywania fałszywych informacji o danej sytuacji, stosowanie dezinformacji, prowokowanie przeciwnika do eskalacji konfliktu i przeniesienia go na obszary nieobjęte destabilizacją, zmuszenie go do podejmowania czasochłonnych i energochłonnych działań represyjnych, wiążących jego siły i środki;
- metodę wywierania wpływu na algorytm podejmowania decyzji przez przeciwnika poprzez np. publikację rozmyślnie zniekształconej doktryny prowadzenia operacji, uzyskiwanie wpływów na systemy zarządzania i kontroli w państwie oraz postaci pełniące kluczowe funkcje polityczne, neutralizacja strategii i myślenia operacyjnego przeciwnika, jego dezorientacja;
- metodę wpływania na czas decyzji przeciwnika poprzez wywoływanie niespodziewanych działań wojennych, prowokowanie do podejmowania irracjonalnych, pochopnych decyzji skutkujących nieadekwatnymi do sytuacji reakcjami.

Zarządzanie refleksyjne w kategoriach geopolitycznych definiowane jest przez rosyjskich analityków wojskowych jako kompleks technik i sposobów manipulacji emocjami, percepcją i świadomością sił zbrojnych, elit przywódczych i poszczególnych grup społecznych w państwie nieprzyjacielskim; wśród nich wymienia się:

- metodę odwracania uwagi, w więc wdrożenie przedsięwzięć, których celem jest stworzenie prawdziwego lub fikcyjnego zagrożenia dla przeciwnika;
- metodę przeciążenia, polegającą na przekazywaniu przeciwnikowi dużej ilości sprzecznych informacji, co powoduje przeciążenie systemów informacyjnych, tworząc szum informacyjny, co powoduje dezorientację i wzrost niepewności w procesie decyzyjnym;
- metodę paraliżowania, polegającą na wzbudzaniu u przeciwnika strachu na skutek umacniania w nim przekonania o zagrożeniu jego interesów politycznych, gospodarczych, militarnych etc;

[40] M. Wojnowski, *Zarządzanie refleksyjne…*, zwłaszcza s. 21–26.

- metodę wyczerpania oponenta poprzez stymulowanie go do przeprowadzania dużej ilości bezużytecznych, czasochłonnych, energochłonnych i kosztownych operacji;
- metodę inscenizacji, a więc działania informacyjne w stosunku do przeciwnika polegające na stworzeniu fikcyjnego zagrożenia dla niego, ale w taki sposób, aby oponent odkrył to oszustwo; jest to metoda na osłabienie czujności nieprzyjaciela;
- metodę dezintegracji – zmuszenie wrogiego państwa do podejmowania czynności sprzecznych z interesami sojuszu, w którym się znajduje, np. poprzez kreowanie i wzmacnianie wewnętrznych konfliktów społecznych, co może prowadzić do wewnętrznej destabilizacji i zmniejszenia potencjału politycznego, gospodarczego i militarnego przeciwnika;
- metodę uspokojenia obiektu agresji poprzez wywołanie w świadomości przeciwnika przeświadczenia o neutralności lub przyjaznej postawie przyszłego agresora, co może skutkować np. odstąpieniem od planów rozbudowy sił zbrojnych, obniżenia nakładów na obron i bezpieczeństwo etc;
- metodę zastraszania wroga poprzez przekazanie pakietu informacji zawierających dane (niekoniecznie prawdziwe) o dużej przewadze przyszłego agresora;
- metodę prowokacji, a zatem stymulowanie przeciwnika do podejmowania działań korzystnych dla drugiej strony;
- metodę sugestii, rozumianą jako tworzenie i transmisję do świadomości wrogiego społeczeństwa stereotypów informacyjnych stanowiących prawne, moralne i ideologiczne bodźce mające na celu spowodowanie korzystnego działania poszczególnych grup społecznych zaatakowanego państwa na rzecz agresora;
- metodę nacisku czyli dyskredytowanie przeciwnika w oczach opinii publicznej poprzez ujawnienie kompromitujących go informacji (prawdziwych bądź zmanipulowanych).

Thimothy Tomas, próbując uogólnić tego typu działania, wprowadza pojęcie „broni poznawczej" (*cognitive weapon*), rozumiejąc pod tym pojęciem wprowadzanie to intelektualnego środowiska zaatakowanego społeczeństwa fałszywych teorii naukowych, paradygmatów, koncepcji i strategii, które wpływają na administrację państwową w sposób znacząco osłabiający narodowy potencjał obronny[41].

[41] T. Thomas, *Russia's 21st Century Information War: Working to Understand and Destabilize Populations, Defence Strategic Communication*s, „The Official Journal of the NATO Strategic Communications Centre of Excellence" Winter 2015, vol. 1, nr 1, s. 18.

Strategia rosyjska w tym zakresie nawiązuje do opracowanej jeszcze w latach 60. XX wieku przez Jewgienija Messnera koncepcji wojen buntowniczych. Koncepcja Messnera opiera się na stymulowaniu powstawania we wrogim państwie ugrupowań antyrządowych, rewolucyjnych, nie cofających się przed przemocą, podejmującymi działania typu partyzanckiego czy terrorystycznego. Celem wojny buntowniczej jest nie tylko neutralizacja sił zbrojnych przeciwnika, lecz także destabilizacja państwa za pomocą czynników psychologicznych (demoralizacji, strachu, poczucia zagrożenia). Dlatego też sam Messner określał tak rozumianą wojnę buntowniczą jako „półwojnę" – przemoc zbrojną nie będącą klasycznymi działaniami wojennymi. Głównym celem wojny buntowniczej jest „zdobycie duszy wrogiego narodu", stąd istotną rolę odgrywają w niej dziennikarze, dywersanci, prowokatorzy, propagandyści, a pojęcie linii frontu w takiej wojnie odnosi się do poszczególnych sfer aktywności danego społeczeństwa (polityka, gospodarka, kultura etc)[42].

W swoich rozważaniach Messner sprecyzował 9 szczegółowych zasad prowadzenia wojny buntowniczej:

- rozkład morale wrogiego narodu;
- rozbicie aktywnych części państwa (sił zbrojnych, ruchów społecznych);
- zajęcie lub unieszkodliwienie obiektów mających wartość psychologiczną;
- zajęcie lub unieszkodliwienie obiektów mających wartość materialną;
- wdrożenie działań mających na celu pozyskanie sojuszników i osłabienie sprzymierzeńców nieprzyjaciela;
- ochrona morale własnego narodu;
- oszczędzanie własnych sił zbrojnych;
- zabezpieczenie swoich obiektów stanowiących wartość psychologiczną oraz materialną;
- ograniczenie oddziaływania czynników, które mogą spowodować negatywną dla strony prowadzącej wojnę buntowniczą reakcję w państwach neutralnych, nie tylko w sferach rządowych, lecz także w szerokich grupach społecznych[43].

---

[42] Zob.: M. Wojnowski, *Terroryzm w służbie geopolityki. Konflikt rosyjsko – ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11 (6), s. 73–77; J. Tomasiewicz, *Od skrytobójstwa do miatieżowojny. Ewolucja terroryzmu politycznego w Europie – aspekty ideologiczne, taktyczne i organizacyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11 (6), s. 133–134.

[43] M. Wojnowski, *Terroryzm w służbie geopolityki*…, s. 76–77.

Jak zauważa Joanna Darczewska, „podczas operacji krymskiej Rosja zademonstrowała światu możliwości i potencjał prowadzenia wojen informacyjnych. Ich celem jest podporządkowanie elit i społeczeństw innych państw w sposób niezauważalny, przy wykorzystaniu różnych tajnych i jawnych kanałów (służb specjalnych, dyplomatycznych, medialnych), oddziaływania psychologicznego, dywersji ideologicznej i politycznej. Batalie informacyjne rosyjscy politycy i dziennikarze uzasadniają koniecznością przeciwdziałania 'infoagresji cywilizacji atlantyckiej pod przywództwem USA' na 'cywilizację rosyjsko/eurazjatycką', tj. wykorzystywanym od lat argumentem z arsenału geopolityki stosowanej"[44]. Zasadny wydaje się zatem być wniosek, iż doktryna wojenna Federacji Rosyjskiej oraz towarzysząca jej akcja informacyjno – interpretacyjna są elementami ogólnej strategii informacyjnej Rosji, której aspekt funkcjonalny odzwierciedla koncepcja walki informacyjnej. Joanna Darczewska zauważa przy tym, że „koncepcja ta jest przejawem militaryzacji polityki Kremla; pozwala mobilizować społeczeństwo, a poprzez manipulację własną i zagraniczną opinią publiczną legitymizować działania Rosji na arenie wewnętrznej i międzynarodowej. Z tego względu doktryna ma istotny walor praktyczny: przygotowuje grunt pod potencjalne interwencje zbrojne i tworzy preteksty do użycia rosyjskiej armii"[45]. Autorka zauważa przy tym, że rosyjscy teoretycy uznają wojnę informacyjną za oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej przez wykorzystanie poszczególnych sposobów kontroli nad zasobami informacyjnymi, używanych jako „broń informacyjna"; podstawowe znaczenie ma w tym kontekście nie wymiar technologiczny, lecz czynniki kulturowe i ideologiczne[46].

Rosyjska doktryna i praktyka wojen nowej generacji ma zatem solidną, starannie wypracowaną podbudowę teoretyczną, metodologia opiera się na koncepcji walki informacyjnej, zarządzania refleksyjnego i tzw. wojnach buntowniczych. Istotą rosyjskich wojen informacyjnych jest oddziaływanie na społeczeństwo zaatakowanego państwa, osiągnąć zakładany cel (zwycięstwo) bez bezpośredniego i otwartego angażowa-

---

[44] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, „Punkt widzenia", Ośrodek Studiów Wschodnich, nr 42, Warszawa maj 2014 r.

[45] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, „Punkt widzenia", Ośrodek Studiów Wschodnich, nr 50, Warszawa maj 2015, s. 7.

[46] Zob.: J. Darczewska, *Anatomia…*

nia sił zbrojnych Federacji Rosyjskiej w klasycznie rozumiany konflikt zbrojny (wojnę).

Podsumowując swoją analizę Michał Wojnowski podkreśla dwie kardynalne kwestie. Po pierwsze, sterowanie refleksyjne to proces przekazania do wrogiego ośrodka specjalnie spreparowanych i uprawdopodobnionych informacji, które mają na celu podjęcie przez przeciwnika korzystnej dla agresora decyzji. *Conditio sine qua non* takiej operacji jest nieświadomość przeciwnika, że przesłanki, na podstawie których podejmuje decyzje, są rezultatem zewnętrznej manipulacji. Konieczne jest zatem nie tylko zachowanie w tajemnicy samej operacji, lecz także transmisja informacji w taki sposób, aby przeciwnik nie zorientował się, ze pada ofiarą manipulacji. Po drugie – co jest naturalną konsekwencją – konieczne jest zbudowanie maksymalnie precyzyjnego modelu refleksyjnego przeciwnika, który będzie umożliwiał symulację (imitację) jego zachowania w konkretnej sytuacji i na tej podstawie dobór odpowiednich środków działania. W tym kontekście kluczową rolę odgrywa działanie wywiadu. Jak podkreśla w swoim wywodzie przywołany Autor, „do głównych zadań wywiadu należy przede wszystkim gromadzenie, analiza i przetwarzanie informacji dotyczących moralno – psychologicznych cech strony przeciwnej, jej mentalności, kultury, w przypadku zaś państw i narodów dodatkowo organizacji społecznej i tożsamości historycznej (podkreślić w tym miejscu wypada, że są to informacje możliwe do zdobycia metodami białego wywiadu, a więc operującego źródłami otwartymi, legalnymi i analizą informacji – T.A.). Szczególnego uwzględnienia wymagają biografie, cechy charakteru, przyzwyczajenia, upodobania i słabości członków elity przywódczej, dowództwa sił zbrojnych, prominentnych przedstawicieli mediów i dziennikarzy, czyli osób mających zdolności i możliwości opiniotwórcze. Ważnym elementem jest także rozpoznanie Internetu jako środka służącego do ewentualnej transmisji informacji, monitoring społeczno – politycznej sytuacji w danym kraju oraz ocena reakcji społeczeństwa na konkretne działanie informacyjne. Zebranie tych danych umożliwia stworzenie modeli poszczególnych aktorów konfliktu oraz zaplanowanie szczegółowego przebiegu operacji uwzględniających różne warianty rozwoju sytuacji, scenariusze zachowania stron itp. Głównym celem jest uzyskanie informacji umożliwiających skuteczne wywieranie wpływu na poszczególne elementy organizacji społecznej (tzw. audytoria) wrogiego państwa lub koalicji przez zastosowanie specjalnych technik”[47].

[47] M. Wojnowski, *Zarządzanie refleksyjne…*, s. 24–25.

Rola służb specjalnych w koncepcji nowych wojen

Jak rozumieć pojęcie służb specjalnych? Termin ten jest daleki od precyzji, wypada w tym miejscu przyznać rację Sławomirowi Zalewskiemu, którego zdaniem obejmuje on zasadzie tylko wywiad i kontrwywiad.[48] Podstawowym zadaniem tych służb jest zdobywanie informacji służących zapewnieniu bezpieczeństwa oraz zapewnienie bezpieczeństwa informacji własnych.

Do zadań o charakterze czysto informacyjnym z czasem dołączyły zadania o charakterze aktywnym, a więc nie tylko zdobywanie informacji, lecz także kreowanie sytuacji korzystnej dla państwa: wprowadzanie w błąd przeciwnika (dezinformacja), pozyskiwanie agentów wpływu, kompromitacja przeciwnika i skrytobójstwa. Za prekursora tego typu myślenia o roli służb specjalnych uchodzi na poły legendarny chiński mędrzec Sun Tzu[49].

Generalnie rzecz ujmując, służby specjalne odgrywając dwie podstawowe role: informacyjno – analityczną oraz kreatywną.

Funkcji informacyjno – analitycznej nie sposób jest sprowadzić wyłącznie do roli źródła informacji dla decydentów. Potencjałem służ specjalnych w tym zakresie jest przede wszystkim zdolność do tworzenia analiz i prognoz (również na poziomie strategicznym) opartych na wszystkich dostępnych źródłach informacji (tzw. *all – source analysis*), które stanowią wkład do tworzenia strategii i polityki bezpieczeństwa narodowego (państwa). Równocześnie materiały analityczne stanowią wsparcie bieżących działań innych organów i instytucji państwowych, np. w postaci obsługi negocjacji prowadzonych przez MSZ (rozpoznanie potencjalnych stanowisk i mandatu negocjacyjnego partnera).

Funkcja ta dotyczy zarówno sfery zewnętrznej, jak i wewnętrznej państwa i wykonywana jest wszędzie tam, gdzie dane państwo ma swoje interesy. W sferze zewnętrznej rozpoznanie może dotyczyć np. konfliktów, które mogą wpłynąć na interesy państwa czy wręcz zagrozić jego bezpieczeństwu. W sferze wewnętrznej można je sprowadzić do identyfikacji zagrożeń, głównych kierunków tych zagrożeń (np. kierunki zainteresowań operacyjnych obcych służb specjalnych) oraz na

---

[48] Zob.: S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2005, wyd. II poszerzone i uaktualnione, s. 7 n.

[49] Zob.: Sun Tzu, Sun Pin, *Sztuka wojny*, Warszawa 2004, szczególnie rozdział *Zatrudnianie szpiegów*.

podstawie identyfikacji zagrożeń prowadzenie działań wyprzedzających i ochronnych, np. w sferze ochrony informacji i zasobów strategicznych państwa.

Funkcja kreatywna służb specjalnych w zarządzaniu bezpieczeństwem strategicznym państwa oznacza stymulowanie przez służby specjalne sytuacji korzystnych z punktu widzenia interesów państwa. Jest to funkcja wykonawcza, bowiem podejmowane przez służby specjalne działania musza mieścić się i wynikać z przyjętej przez państwo strategii bezpieczeństwa narodowego. Termin „sytuacja korzystna z punktu widzenia interesów państwa" należy rozumieć dwojako, tj. w postaci negatywnej i pozytywnej, choć trzeba zwrócić uwagę, że granica pomiędzy nimi jest płynna i niezbyt wyraźnie zarysowana. W postaci negatywnej kreowanie sytuacji korzystnej dla interesów państwa następuje poprzez neutralizację zagrożenia, np. identyfikacja kierunków zagrożeń ze strony obcych służb specjalnych i doprowadzenie do podniesienia poziomu ochrony określonego sektora czy informacji. Natomiast o postaci pozytywnej możemy mówić np. przy skłonieniu innego podmiotu do zawarcia korzystnego dla państwa porozumienia czy też po przewerbowaniu agenta obcych służb specjalnych przeprowadzenie skutecznej operacji dezinformacyjnej[50].

Tak więc, rola służb specjalnych nie kończy się w tym przypadku na zdobywaniu i analizie informacji. Równie istotna jest kwestia przekazania odpowiednio spreparowanej informacji stronie przeciwnej, a przede wszystkim wykorzystaniu takich kanałów informacyjnych i takich źródeł informacji, które będą dla przeciwnika wiarygodne. W znacznej mierze pozostaje to domeną służb specjalnych, choćby przy konieczności wykorzystania agentury klasycznej i/lub agentury wpływu. W literaturze przedmiotu takie działania nazywa się operacjami pozainformacyjnymi wywiadu (*covert operations*). Nazwa ta – choć wydawać się może paradoksalna, bowiem przecież mowa jest o walce i wojnie informacyjnej – związana jest z faktem, iż operacje takie nie mają nic wspólnego ze zbieraniem informacji, ale realizacją określonej polityki poprzez uzyskanie wpływu na działanie przeciwnika. „Na działania tego typu składają się akcje propagandowe, polityczne, militarne, logistyczne, techniczne oraz finansowe wspieranie pewnych ugrupować (najczęściej opozycyjnych) (…) prowadzone są wtedy, kiedy nie ma możliwości osiągnięcia celów

[50] Zob.: na ten temat: T. Aleksandrowicz, *Służby specjalne w strategicznym zapewnianiu bezpieczeństwa państwa*, [w:] J. Gryz (red.), *Strategia bezpieczeństwa narodowego Polski*, Warszawa 2013, s. 254 i n.

militarnie albo użycie siły militarnej wywoła konsekwencje negatywne lub niewspółmierne do uzyskanych efektów, a instrumenty dyplomatyczne są nieskuteczne. Wśród działań dezinformujących i okłamujących przeciwnika, realizowanych m.in. przez służby wywiadowcze państw, możemy wyróżnić wpływanie na instytucje państwowe przeciwnika oraz jego społeczeństwo"[51].

Tego typu działania nie stanowią w stosunkach międzynarodowych żadnego *novum*. Tak np., na mocy dyrektywy 10/2 Rady Bezpieczeństwa Narodowego USA w sprawie projektów specjalnych z 18 czerwca 1948 r.[52], Centralna Agencja Wywiadowcza otrzymała uprawnienie do prowadzenia *covert operations* (tajnych operacji), rozumianych jako „działalność prowadzona przez rząd Stanów Zjednoczonych lub na jego zlecenie przeciwko wrogim państwom lub grupom lub w celu poparcia przyjaznych państw lub grup, które są tak zaplanowane i wykonywane, że odpowiedzialność żadnej agendy rządu Stanów Zjednoczonych nie będzie mogła być udowodniona przez osobę nieuprawnioną, a w przypadku ujawnienia takich operacji rząd Stanów Zjednoczonych będzie mógł w prawdopodobny sposób odrzucić jakąkolwiek odpowiedzialność za nią. Operacje takie mogą polegać na działaniach związanych z propagandą, wrogimi działaniami gospodarczymi (*economic warfare*), prewencyjnymi działaniami bezpośrednimi, takimi jak sabotaż, niszczenie i zabór środków, działalność wywrotową przeciwko obcym państwom, w tym wsparcie dla odziemnych ruchów oporu, partyzantów, uchodźców, grup wyzwoleńczych oraz wsparcie dla lokalnych elementów antykomunistycznych w Wolnym Świecie. Takie operacje nie obejmują konfliktów zbrojnych prowadzonych przez regularne siły zbrojne, szpiegostwa i zwalczania szpiegostwa, osłony i podstępu dla operacji militarnych"[53].

---

[51] M. Minkina, B. Gądek, *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015, s. 36.

[52] National Security Council Directive on Office of Special Projects (NSC 10/2), Washington, June 18, 1948, para. 5, https://history.state.gov/historicaldocuments/frus1945-50Intel/d292 (21.03.2016).

[53] Jest to tzw. doktryna prawdopodobnego zaprzeczenia (*plausible deniability*). Wedle obowiązujących definicji normatywnych definicja *covert operation* stanowi, że jest to „działalność Rządu Stanów Zjednoczonych prowadzona w celu wpływania na warunki polityczne, gospodarcze lub militarne za granicą, która zakłada, iż rola Rządu Stanów Zjednoczonych nie będzie widoczna lub znana publicznie", Executive Order 12333. United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), para. 3.5. b), http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf (21.03.2016). Również i w tym przypadku takie operacje nie obejmują otwartych działań wojskowych.

Podsumowanie

Koncepcja „wojen nowej generacji" („nowych wojen") stanowi rozwinięcie znanych od dawna koncepcji informacyjnych, buntowniczych i zarządzania refleksyjnego. Jej podstawowym elementem jest informacja wykorzystywana jako broń, a podstawową zasadą unikanie zaangażowania Federacji Rosyjskiej w konflikty powyżej progu otwartej wojny, a więc takich, w których Rosja byłaby stroną konfliktu militarnego (wojny) prowadzonego przeciwko innemu podmiotowi państwowemu. Istotnym elementem wojen nowej generacji są służby specjalne, których zadaniem jest nie tylko pozyskiwanie informacji o przeciwniku, lecz także przekazywanie mu informacji za pośrednictwem wielu kanałów informacyjnych w taki sposób, aby spowodować jego działania korzystne dla Rosji. Analiza konfliktu rosyjsko-ukraińskiego wyraźnie wskazuje, iż omawiana koncepcja znalazła w tym przypadku pełne zastosowanie.

Ocena tego typu działań pod kątem zastosowania wobec nich dychotomicznego kryterium wojna – pokój ma nie tylko istotny wymiar teoretyczny, jak i praktyczny. Jego rozstrzygnięcie wiąże się bowiem z reakcją państw i sojuszy wojskowych na tego typu zagrożenia, które z trudnością (o ile w ogóle) mieszczą się w pojęciu wojny.

Jako punkt wyjścia można przyjąć propozycję Stanisława Kozieja wprowadzającego pojęcie konfliktu niezbrojnego w związku z rosnącą rolą pozazbrojnych środków przemocy w osiąganiu celów wojennych. W jego ujęciu konflikt niezbrojny stanowi trzeci, pośredni stan pomiędzy wojną a pokojem. „Współcześnie w naukach wojennych mamy więc do czynienia z problemem natury pojęciowej, który można ująć w postaci następującej alternatywy: albo poszerzyć pojęcie wojny tak, aby objąć nim także stosowanie samych pozazbrojnych form przemocy politycznej, albo – zachować jej dotychczasowe pojmowanie, a stosowanie wyłącznie niezbrojnej przemocy do narzucania swej woli stronie przeciwnej uważać za jakościowo inne zjawisko i nazwać je inaczej"[54].

[54] S. Koziej, *Teoria*…, s. 12–13.

Streszczenie

Analizując rosyjską doktrynę, myśl strategiczną i działania podejmowane przez Federację Rosyjską przeciwko Ukrainie nie sposób nie zauważyć, iż Kreml wdraża w życie koncepcję „nowych wojen" („wojen nowej generacji"). Koncepcja ta obejmuje zarówno wojnę informacyjną, jak i „zarządzanie refleksyjne" i „wojny buntownicze". Wiele wskazuje na to, że wypracowana przez Rosjan koncepcja „nowych wojen" jest odpowiedzią na zachodnie koncepcje wojny informacyjnej (*information warfrare*) i wojen hybrydowych. Konflikt ukraiński można traktować ja swoisty poligon dla rosyjskich służb specjalnych, tak wojskowych jak i cywilnych, które w ramach „nowych wojen" odgrywają kluczową rolę.

Tomasz R. Aleksandrowicz

Foreign Intelligence as a Tool in the Concept of New Wars. The Ukrainian Conflict Case

Analysis of the Russian doctrine, strategic thought and practice in the Ukrainian conflict shows that the Kremlin has developed the concept of "new wars" or "new generation of wars". In this concept one can find the "information wars", "reflective governance" and "mutiny wars". In the matter of fact it is the reaction to the western concept of "information warfare" and "hybrid war". The Ukrainian conflict is probably kind of a training ground of the Russian special services, both military (GRU) and the SVR. In the concept of "new wars" special services has to play the main role as a useful tool but also as an intellectual background.

Key words: *information war, new wars, Russian doctrine, foreign intelligence, Ukrainian conflict*

Bibliografia

Aleksadrowicz T., *Gdzie leży czerwona linia? Strategia wobec Rosji*, http://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-strategia-wobec-rosji (15.10.2014).

Aleksandrowicz T., *Służby specjalne w strategicznym zapewnianiu bezpieczeństwa państwa*, [w:] J. Gryz (red.), *Strategia bezpieczeństwa narodowego Polski*, Warszawa 2013.

Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.

Balcerowicz B., *O pokoju. O wojnie. Między esejem a traktatem*, Warszawa 2013.

Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Warszawa 2010.

Brudelein C., *The Role of Non – State Actors in Building Human Security: the Case of Armed Groups in Infra – State Wars*, Geneva Center for Human Dialog, May 2000, http://www.hdcentre.org/files/the%20role%20of%20non-state%20actors.pdf (28.03.2012).

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, „Punkt widzenia", Ośrodek Studiów Wschodnich, nr 42, Warszawa maj 2014.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, „Punkt widzenia", Ośrodek Studiów Wschodnich, nr 50, Warszawa maj 2015.

Darczewska J., *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, *Wydanie specjalne – Wojna hybrydowa*.

Dudziak M.L., *War Time. An Idea, It's History, It's Consequences*, Oxford 2012.

Hobsbawm E., *Globalization, Democracy and Terrorism*, London 2007.

Johnston C., *Russia's Info-War: Theory and Practice*, Issue Alert 22/2015, European Union Institute for Security Studies, April 2015.

Karolczak K., *Terroryzm. Nowy paradygmat wojny*, Warszawa 2010.

Koziej S., *Teoria sztuki wojennej*, Warszawa 2011.

Minkina M., Gądek B., *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015.

Nazarow O., *Informacionnyje wojny – ugroza dlia ciwilizacii*, „Litieraturnaja Gazieta" 2013, nr 42.

Pomerantsev P., Weiss M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. A Special Report presented by The Interpreter, a Project of the Institute of Modern Russia, New York 2014.

Sun Tzu, Sun Pin, *Sztuka wojny*, Warszawa 2004.

Thomas T., *Russia's 21st Century Information War: Working to Understand and Destabilize Populations*, Defence Strategic Communications, „The Official Journal of the NATO Strategic Communications Centre of Excellence", vol. 1, nr 1, Winter 2015.

Thomas T.L., *Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, The State Technical Commission and the Military*, „European Security" 1998, nr 7.

Tomasiewicz J., *Od skrytobójstwa do miatieżowojny. Ewolucja terroryzmu politycznego w Europie – aspekty ideologiczne, taktyczne i organizacyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 11 (6).

Trudolyubov M., *Russia's Hybrid War*, The New York Times, February 24, 2016, http://www.nytimes.com/2016/02/25/opinion/russias-hybrid-war.html (26.02.2016).

Wąsowski K., *Istota i uniwersalność rosyjskiego modelu wojny hybrydowej wykorzystanego na Ukrainie,* „Sprawy Międzynarodowe" 2015, nr 2.

Wojnowski M., *Aleksandr Dugin a resorty siłowe Federacji Rosyjskiej. Przyczynek do badań nad wykorzystaniem geopolityki przez cywilne i wojskowe służby specjalne we współczesnej Rosji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10 (6).

Wojnowski M., *Koncepcja wojen nowej generacji w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13 (7).

Wojnowski M., *Terroryzm w służbie geopolityki. Konflikt rosyjsko – ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11 (6).

Wojnowski M., *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno – psychologicznych w XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12 (7).

Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2005.