Chorzowskie Studia Polityczne
Nr 15 rok 2018

Artur Dubiel
Wyższa Szkoła Bankowa w Chorzowie
Instytut Naukowy Bezpieczeństwa
orcid.org/0000-0001-5316-3258
e-mail: artur.dubiel@chorzow.wsb.pl
tel. 608 400 275

Operacje informacyjno-psychologiczne jako zagrożenie bezpieczeństwa państwa

Streszczenie. Artykuł ukazuje zagrożenie operacjami informacyjno-psychologicznymi jako podstawowy element prowadzenia walki informacyjnej. W tekście stawiana jest teza, że katalog prowadzonych wrogich działań staje się głównym narzędziem prowadzonej obecnie geopolityki i będzie zyskiwał na znaczeniu. Autor wskazuje służby specjalne jako fizycznego wykonawcę działań i ukazuje bezpośrednie zagrożenia dla Polski ze strony Federacji Rosyjskiej. Walka informacyjna, operacje informacyjno-psychologiczne i zarządzanie refleksyjne mają niebagatelny wpływ na bezpieczeństwo informacyjne państwa, a przez to na żywotne interesy Rzeczpospolitej Polskiej.

Słowa kluczowe: walka informacyjna, operacje informacyjne, operacje psychologiczne, operacje informacyjno-psychologiczne, psychologia operacyjna, zarządzanie refleksyjne

1. Wprowadzenie

Niniejsze opracowanie jest próbą wskazania powiązań pomiędzy procesami komunikowania [por. Grochowski 2015: 46], perswazją [por. Kubicka, Kołodziejczyk 2007: 63-64], a klasyczną cybernetyką [por. Harrel 2015: 26] jako procesem sterowania społecznego. Artykuł ukazuje, jakie zagrożenia dla bezpieczeństwa państwa [por. Liedel 2008: 19] mogą nieść operacje informacyjne, operacje psychologiczne oraz operacje informacyjno-psychologiczne. Mocno interdyscyplinarny charakter zagadnienia [por. Chodubski 2011: 46] wymaga zastosowania wiedzy nie tylko

z wiodących tutaj nauk o obronności i nauk o bezpieczeństwie, ale także ze wspierających i uzupełniających je psychologii, socjologii, politologii, prawa oraz innych nauk i dziedzin [por. Zieliński 2012: 24]. Na potrzeby tekstu założono, że operacje informacyjno-psychologiczne, stanowiące składową walki informacyjnej, będącej elementem szerokiego wachlarza zagrożeń asymetrycznych, są znacznym zagrożeniem dla bezpieczeństwa państwa. Przyjęto także priorytet służb specjalnych w działaniach defensywnych i ofensywnych na tym polu. W artykule postawiono pytania: co spowodowało i zdeterminowało tak wysoki poziom zagrożenia ze strony walki informacyjnej, jaki jest katalog zagrożeń oraz jakie kroki państwo jako instytucja może podjąć w celu przeciwdziałania zagrożeniom i ku lepszej ochronie własnych struktur oraz obywateli.

2. Nowa rzeczywistość

Koniec XX w. i wejście w wiek XXI kojarzy się głównie z nową wizją świata, opartą na dalszym rozwoju cywilizacyjnym, wynikającą z dominacji Europy, utrzymania globalnego pokoju mimo wielu konfrontacyjnych okresów i postaw od zakończenia II wojny światowej. Pierwszym, skrajnie negatywnym symbolem tych czasów, stała się kolejna, IV fala terroryzmu [Noga 2016]. Należy przez nią rozumieć nie masowość zdarzeń, a pojęcie falowości terroryzmu [Noga 2016]. Dobitnym, wizualnym jej symbolem stały się ataki na wieże World Trade Center.

Powyższe skojarzenia straciły na znaczeniu przez wydarzenia na Ukrainie. Począwszy od *modus operandi* przy aneksji Krymu [por. Kaszuba, Minkina 2016: 99] – stały się one nowym symbolem i portalem do nowej geopolitycznej rzeczywistości oraz związanych z nią zagrożeń, z których większość europejskich elit (i społeczeństw) nie zdawała sobie sprawy.

Zaistniała sytuacja sprokurowała pojawienie się kontrowersyjnego pojęcia i koncepcji wojny hybrydowej [por. Kaszuba, Minkina 2016: 99], które to określenie używane jest również w oficjalnych dokumentach i opracowaniach NATO. Już Sowieci praktykowali działania sprowadzające ośrodki studiów i analiz przeciwnika na niewłaściwe tory [Golicyn 2007: 5], a wiele teorii wskazuje właśnie na to, że owa koncepcja przyszła ze Wschodu. Wykorzystując odpowiednie zabiegi, zaszczepiono to pojęcie, zarzucając Zachodowi wcześniejsze stosowanie wojny hybrydowej wobec Rosji. Co ciekawe, w Rosji była to koncepcja tzw. wojny nowej generacji, opisywana m.in. w resortowych wydawnictwach w 2013 r. [Wojnowski 2015a: 13]. Koncepcję tę Zachód zauważył dopiero przy okazji kryzysu ukraińskiego, chrzcząc ją terminem wojny hybrydowej [Wojnowski 2015a: 13]. Tym samym otwarte pozostaje pytanie, czy pojęcia owej wojny hybrydowej

Zachód nie zafundował sobie sam, ku uciesze rosyjskich służb. Pojęcie to stało się narzędziem walki informacyjnej [Wojnowski 2015b: 19], paradoksalnie przez Zachód zapomnianym, choć przecież pierwotnie użyte zostało przez Amerykanów wobec kryzysu na linii Izrael – Hezbollah w 2006 r. [Wojnowski 2015b: 8].

Zadziwiające jest też, że dopiero konflikt w XXI w. przypomniał Zachodowi takie zestawienie form, technik i środków prowadzenia walki. Przeoczono opisaną także, jako techniki manipulacji i sterowania społeczeństwem, teorię zarządzania refleksyjnego Władimira Lefewra z lat 60. XX w. [Wojnowski 2015c: 11-12]

Marcin Kossek w swych wypowiedziach zauważa jednak, że zarządzanie refleksyjne może być sztucznie wykreowanym pojęciem, ponieważ w moskiewskich ośrodkach naukowych i badawczych ono nie funkcjonuje. Pokrywać się za to może z programowaniem neurolingwistycznym znanym jako NLP oraz coachingiem. Według niego pojęcie to może być nową nazwą i koncepcją wynikającą z brutalnych doświadczeń i badań na psach rosyjskiego noblisty Iwana Pawłowa z lat 20. XX w., a dotyczących warunkowania klasycznego i instrumentalnego. Pawłow wspierał swymi badaniami sowieckie służby specjalne.

Nie do końca jasna sytuacja pojęcia zarządzania refleksyjnego wymaga dogłębnych analiz naukowych, gdyż rozmywa obraz działania służb rosyjskich w tym aspekcie, a jest zapewne celowym działaniem ukierunkowanym na „zadaniowanie" ośrodków analitycznych nieprzyjaciela.

Chaos definicyjno-pojęciowy powoduje także, że zarówno specjaliści, a za nimi również dziennikarze mylą i spłaszczają podstawowe pojęcia. W interpretacyjnym nieładzie Zachód popełnia błąd pojmowania przeciwnika przez własny pryzmat i wartości. Przykładem niech będzie zestawianie tak różnych klasyków, jak Carl von Clausevitz i Sun Tzu. Interesujące, że po II wojnie światowej brytyjskie służby wywiadowcze przepowiadały koniec teorii tego pierwszego oraz że Kreml będzie prowadził agresywną politykę, wykorzystując informacje wywiadowcze, szantaż, propagandę oraz dywersję ideologiczną i polityczną" [Brzeski 2014: 16-17]. Forma „zimnej wojny" doprowadziła również do powstania teorii wojen czwartej generacji, czyli konfliktów niskiej intensywności, w tym z wykorzystaniem terroryzmu [Brzeski 2014: 17].

Rosjanie, wprowadzając Doktrynę wojenną Federacji Rosyjskiej (z 2000 r.), podkreślili potrzebę działań defensywnych i ofensywnych w przestrzeni informacyjnej, zauważając także ich psychologiczny charakter [Darczewska 2016: 8]. Tym samym dochodzi tutaj do pewnego ważnego przełamania czy przewartościowania, gdyż na całość zagadnienia walki informacyjnej należy spojrzeć z punktu widzenia psychologii. Tylko odpowiednia wiedza, poparta także innymi naukami, poprzez interdyscyplinarne podejście pozwoli na osiągnięcie przez instytucje państwowe, a dokładniej organy bezpieczeństwa, satysfakcjonującego poziomu bezpieczeństwa państwa, wobec oczywistych zagrożeń z równie oczywistego kierunku.

3. Polskie realia

W polskiej rzeczywistości pojawia się Doktryna bezpieczeństwa informacyjnego RP (z lipca 2015 r.) [Biuro Bezpieczeństwa Narodowego 2015], która niestety jest nadal tylko projektem, ale podejmuje próbę przyjęcia ważnych definicji, pojęć i terminów, m.in. bezpieczeństwa informacyjnego państwa czy komunikacji strategicznej. W nawiązaniu do tematu artykułu pojawiają się także następujące definicje [Brzeski 2014: 4]:

> Operacje informacyjne (walka informacyjna) – czynności polegające na oddziaływaniu na informacje i/lub systemy informacyjne w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika (zautomatyzowanych oraz z udziałem czynnika ludzkiego), przy jednoczesnej ochronie własnych procesów decyzyjnych; w wymiarze wojskowym także działalność mająca na celu wywarcie pożądanego wpływu na wolę, rozumienie i zdolności przeciwników, potencjalnych przeciwników lub innych stron konfliktu, wspierających cele danej misji; w operacjach informacyjnych można wyróżnić działania ofensywne i defensywne:
>
> – do działań ofensywnych należy zaliczyć: operacje psychologiczne, pozorację, destrukcję, walkę elektroniczną, atak informatyczny, działania z zakresu komunikacji społecznej,
>
> – do działań defensywnych należy zaliczyć: bezpieczeństwo informacyjne, osłonę, działania kontrpropagandowe, działania kontrwywiadowcze, walkę elektroniczną, informacyjne działania specjalne.
>
> Operacje psychologiczne – operacje mające na celu wpływanie na emocje, motywacje, obiektywne rozumowanie, a ostatecznie zachowanie rządów państw obcych, organizacji, grup i osób będących celami tych operacji, tak aby osiągnąć efekt w postaci wzmocnienia lub nakłonienia do zachowań korzystnych dla realizacji własnych interesów. Mogą być wykorzystywane zarówno w czasie pokoju (klęsk żywiołowych, stanów kryzysowych i alarmowych), jak i podczas wojny.
>
> Inżynieria społeczna – zespół metod i środków celowego manipulowania społeczeństwem. Propaganda, dezinformacja – rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich) w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń.
>
> Manipulacja informacja – wykorzystanie prawdziwych informacji, ale w taki sposób, żeby wywołać fałszywe implikacje, np. drogą pomijania niektórych, istotnych, ale niewygodnych informacji lub poprzez taki dobór informacji, żeby budziły fałszywe skojarzenia.
>
> Trollowanie (trolling) – antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych, polegające na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów.

Niestety powyższe założenia definicyjne budzą wiele pytań i wątpliwości, a błędne założenia mogą mieć negatywny wpływ na jakość podejmowanych działań: czy operacje informacyjne są tożsame z walką informacyjną [por. Aleksandrowicz 2016: 130-131], czy operacje psychologiczne to element tylko działań ofensywnych operacji informacyjnych [por. Modrzejewski 2015: 3], czy

właściwe jest zerojedynkowe rozdzielenie obu typów operacji, czy nie powinno się wprowadzić trzeciej kategorii czyli operacji informacyjno-psychologicznych [por. Wojnowski 2015c: 15-16], czy definicja inżynierii społecznej nie określa czasem cybernetyki (społecznej), dlaczego tak odległe pojęcia jak propaganda i dezinformacja traktowane są tożsamo, czy nie pomylono dezinformacji z manipulacją, dlaczego w trollingu pomięto ważny element celowości i formy ataku, a skupiono się na typowo aspołecznych aspektach? Oczywiście wymienione pytania wynikają tylko z ogólnej lektury, ale dobitnie wskazują, jak wiele jest w projekcie do dopracowania.

Wspomniano powyżej także o trzeciej kategorii operacji, tj. o operacjach informacyjno-psychologicznych jako hybrydzie operacji informacyjnych i psychologicznych [Wojnowski 2015c]. Ta rosyjska koncepcja wydaje się dość sensowna. Kossek wprowadza też zamiennie pojęcie psychologii operacyjnej bądź psychologicznych operacji specjalnych [Kossek 2016]. Celem takich operacji nie muszą być całe społeczeństwa, niemałe przecież, jak np. polskie, ale tzw. grupy kluczowe [Volkoff 1999: 111].

4. Katalog zagrożeń

Niezależnie od tego, jaki ostatecznie zostanie przyjęty podział operacji, podstawowy katalog zagrożeń dla bezpieczeństwa informacyjnego pozostaje ten sam [Aleksandrowicz 2016: 120]:

– brak dostępu do informacji (pustka informacyjna),
– nadmiar informacji (szum informacyjny),
– dostęp do informacji fałszywej i dezinformacji,
– brak ochrony własnych zasobów informacyjnych,
– brak kontroli nad własnymi kanałami informacyjnymi.

Podstawowe zagrożenia bezpieczeństwa informacyjnego w innym ujęciu [Bączek 2005: 85]:

– nieuprawnione ujawnienia informacji, które mogą nosić charakter pomyłkowy, polityczny lub komercyjny (sprzedaż informacji),
– naruszenia przez władze praw obywatelskich (ograniczanie jawności życia publicznego, naruszenia prywatności),
– asymetria w międzynarodowej wymianie informacji (nierównoprawna wymiana pomiędzy sojusznikami),
– działalność grup świadomie manipulujących przekazem informacji (np. sekty),
– niekontrolowany rozwój technologii bioinformatycznych (np. w postaci uzyskania zdolności manipulacji procesami zachodzącymi w ludzkim mózgu),

– przestępczość komputerowa,
– cyberterroryzm,
– walka informacyjna,
– zagrożenia asymetryczne,
– szpiegostwo.

Bardzo ciekawe jest zestawienie zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni (projekt doktryny) [Aleksandrowicz 2016: 122]:

– dezinformacja, trolling, wroga propaganda zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego,
– ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną,
– istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

Projekt omawia także zagrożenia w przestrzeni medialnej [Aleksandrowicz 2016: 122]:

– monopolizacja rynku informacyjnego i jego poszczególnych struktur oraz niekontrolowany rozwój rynku informacyjnego media masowe mogą być narzędziem dezinformacji,
– przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie Polsce,
– pojawienie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z interesem narodowym,
– aktywne uczestnictwo przeciwnika w polskich mediach społecznościowych – propagowanie idei sprzecznych z interesem narodowym,
– nieświadome, niezamierzone powielanie przekazu informacyjnego sprzecznego z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe.

Samo pojęcie walki informacyjnej wynika bezpośrednio z klasycznej cybernetyki (obecnie: społecznej lub socjocybernetyki) [Kossecki 1997: 2], jest to szczególny przypadek procesu sterowania społecznego, którego celem jest niszczenie przeciwnika za pomocą informacji. Mimo że pojęcie pojawiło pod koniec XX w. w efekcie rewolucji informacyjnej, to funkcjonowało od wieków, chociażby w warsztacie służb wywiadowczych (i kontrwywiadowczych) [Liedel, Piasecka, Aleksandrowicz 2012: 15]. Informacja, a za nią walka informacyjna, stała się także narzędziem w ręku terrorystów [Aleksandrowicz 2015: 42-44].

5. Obrona i ochrona

Mając rozpoznany katalog zagrożeń, można dokonać realizacji założeń dotyczących ochrony i obrony przed nimi. Patrząc bardzo krytycznie, trzeba niestety przyznać, że większość literatury i fachowców w swych wypowiedziach wskazuje sensowne pomysły na zapewnienie bezpieczeństwa, błędnie jednak sugerując je jednostce, a nie organom państwa. W dzisiejszym świecie, w natłoku informacji – czyli omawianym wcześniej szumie informacyjnym, jako jednym z zagrożeń bezpieczeństwa informacyjnego – przeciętny obywatel nie jest w stanie się rozeznać, gdyż nie ma czasu i/lub chęci na weryfikowanie bombardujących go hurtowo informacji. Poprawna weryfikacja informacji musi polegać na sprawdzeniu źródła i autora przywoływanych materiałów, detali, dat, czytaniu między wierszami, wymaga więc umiejętności analitycznych. Jak widać, to na instytucjach państwowych winien spoczywać taki obowiązek, bo tylko one są w stanie tego sprawnie dokonać.

Na dzień dzisiejszy należy przyjąć i zaufać, że polskie służby specjalne monitorują zagrożenia, dokonują ich analizy, analiz ryzyka, analiz strategicznych, dokonują modelowania i symulacji procesów, planowania scenariuszowego [Nowakowska-Krystman i in. 2015: 20], wraz z mapowaniem i opracowywaniem odpowiednich algorytmów.

6. Wnioski końcowe

Zdaniem autora niniejszego opracowania, najważniejsze jest powołanie międzyresortowego zespołu (bądź rozbudowa i przekształcenie zespołu wyłączonego ze struktur Agencji Bezpieczeństwa Wewnętrznego Centrum Antyterrorystycznego) zajmującego się zagrożeniami asymetrycznymi. Zespół taki m.in. prowadziłby serwis internetowy (oraz profile społecznościowe), gdzie znalazłyby się (wybrane) ujawnione przypadki i elementy prowadzonych przeciwko polskim interesom operacji informacyjno-psychologicznych. W celu właściwego dostarczenia informacji do weryfikacji należałoby stworzyć skryptozakładki do przeglądarek internetowych, tak by w prosty sposób każdy obywatel mógł zgłosić i zweryfikować swoje wątpliwości co do treści w Internecie. Preferowana byłaby współpraca z producentami przeglądarek oraz bezpośrednio z firmą Microsoft. Na stronach instytucji państwowych powinny pojawić się także widgety wyświetlające najważniejsze informacje z opisanego serwisu. Wskazana byłaby także aplikacja na urządzenia przenośne, na wzór aplikacji Regionalnego Systemu Ostrzegania.

Ponadto zacieśnienie współpracy w trójkącie obywatel – służby specjalne – ośrodki akademickie, poprzez np. szkolenia czy warsztaty, w znaczny sposób podniosłyby społeczną świadomość zagrożeń oraz właściwego i preferowanego reagowania na nie.

Bezsprzecznie to służby specjalne, cywilne i wojskowe, bez sztywnego podziału na wywiad i kontrwywiad, a jako służby typu *intelligence*, mają priorytet związany z działaniami defensywnymi i ofensywnymi w zakresie walki informacyjnej, niezależnie od czasu i sfery [por. Dudzik 2016: 33-42]. Kossecki co prawda wskazuje wprost wywiad jako wyspecjalizowaną służbę prowadzącą walkę informacyjną, a kontrwywiad jako służbę zwalczającą działania obcego wywiadu [Kossecki 1997: 2], jednakże w dzisiejszych czasach te różnice zacierają się, tak między służbami, jak i charakterem działań.

Rozważania na temat walki informacyjnej, w tym operacji informacyjno-psychologicznych, powinny stać się przyczynkiem do prawdziwej dyskusji, tak na poziomie służb i instytucji odpowiedzialnych za zabezpieczenie żywotnych interesów państwa, jak i na specjalistycznym poziomie akademickim. Zarówno na uczelniach resortowych, jak i prywatnych, gdzie najczęściej odnajdują się w swej nowej rzeczywistości byli funkcjonariusze i żołnierze, często o niemałym potencjale i kompetencjach.

Zadziwiać może – mimo wszystko – skromność i rozdrobnienie fachowej literatury, nie tylko polskiej, ale i zachodniej, zwłaszcza w stosunku do literatury traktującej o innych zagrożeniach asymetrycznych. Owszem, może to wynikać z faktu, że tematyka jest mocno interdyscyplinarna oraz że pewne zagadnienia, wiedzę i umiejętności organy bezpieczeństwa państwa chcą jak najdłużej zatrzymać dla siebie. Tak było z siłami i służbami specjalnymi, z antyterroryzmem (nie mylić z kontrterroryzmem), wywiadem i kontrwywiadem. Obecnie opracowań polskich jest coraz więcej, ale i tak nie tyle, ile na Zachodzie. Niektórzy podnoszą, że dobrym obyczajem i warunkiem demokracji jest otwarcie warsztatu służb na rynek cywilny, tak by mógł on ich specyfikę zrozumieć i rozwiać swe wątpliwości. Niekonieczne trzeba się z tym zgadzać, jednakże faktem jest, że *stricte* naukowo zagadnienie walki informacyjnej jest obecnie w tym miejscu, gdzie znajdowało się dobrych parę lat temu.

Literatura

Aleksandrowicz T.R., 2015, *Terroryzm międzynarodowy*, Warszawa: Editions Spotkania.

Aleksandrowicz T.R., 2016, *Podstawy walki informacyjnej*, Warszawa: Editions Spotkania.

Biuro Bezpieczeństwa Narodowego, 2015, *Doktryna bezpieczeństwa informacyjnego RP (projekt)*, www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 24.08.2018].

Bączek P., 2005, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń: Wydawnictwo Adam Marszałek.
Brzeski R., 2014, *Wojna informacyjna – wojna nowej generacji*, Komorów: Wydawnictwo Antyk Marcin Dybowski.
Brzeziński J., 2012, *Metodologia badań psychologicznych*, Warszawa: Wydawnictwo Naukowe PWN.
Chodubski A.J., 2011, *Wstęp do badań politologicznych*, Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.
Darczewska J., 2016, *Rosyjskie Siły Zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, Warszawa: Wydawnictwo OSW.
Dudzik I., 2016, Wywiad i kontrwywiad w aspekcie walki informacyjnej XXI wieku, w: M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa: Difin: 33-42.
Golicyn A., 2007, *Nowe kłamstwa w miejsce starych*, Komorów: Wydawnictwo Antyk Marcin Dybowski.
Górka M., 2016, *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa*, Toruń: Wydawnictwo Adam Marszałek.
Górka M. (red.), 2016, *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa: Wydawnictwo Difin.
Grochowski R., 2015, Mass media jako enklawy ukrytych przekazów, w: Narożna D. (red.), *Informacja i konteksty społeczno-kulturowe*, Toruń: Wydawnictwo Adam Marszałek: 46-58.
Harrel Y., 2014, *Rosyjska cyberstrategia*, Warszawa: Wydawnictwo DiG.
Kaszuba M., Minkina M., 2016, *Imperialna gra Rosji*, Warszawa: Oficyna Wydawnicza Rytm.
Kossecki J., 1997, *Totalna wojna informacyjna XX wieku a II RP*, Kielce: WZiA WSP.
Kossek M., 2016, *Psychologia operacyjna w praktyce*, https://mil.link/pl/psychologia-operacyjna--w-praktyce [dostęp: 24.08.2018].
Kubicka D., Kołodziejczyk A., 2007, *Psychologia wpływu mediów*, Kraków: Oficyna Wydawnicza Impuls.
Liedel K., 2008, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Wydawnictwo Adam Marszałek.
Liedel K., Piasecka P., Aleksandrowicz T.R., 2012, *Analiza informacji. Teoria i praktyka*, Warszawa: Difin.
Noga M., 2016, *Falowość terroryzmu*, https://mil.link/pl/falowosc-terroryzmu [dostęp: 24.08.2018].
Nowakowska-Krystman A., Zubrzycki W., Daniluk P., Mazur-Cieślik E., 2015, *Terroryzm w ujęciu analiz strategicznych*, Warszawa: Difin.
Przegląd bezpieczeństwa Wewnętrznego, Warszawa: Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia.
Rajczyk R., 2016, *Nowoczesne wojny informacyjne*, Warszawa: Difin.
Volkoff V., 1999, *Psychosocjotechnika, dezinformacja. Oręż wojny*, Komorów: Wydawnictwo Antyk Marcin Dybowski.
Wojnowski M., 2015a, Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, *Przegląd Bezpieczeństwa Wewnętrznego*, nr 13(7): 13-39.
Wojnowski M., 2015b, Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX-XXI wieku, *Przegląd Bezpieczeństwa Wewnętrznego*, wyd. spec. *Wojna hybrydowa*: 7-38.
Wojnowski M., 2015c, „Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w., *Przegląd Bezpieczeństwa Wewnętrznego*, nr 12(7): 11-36.
Zieliński J., 2012, *Metodologia pracy naukowej*, Warszawa: Oficyna Wydawnicza ASPRA-JR.

Information-Psychological Operations as Threat to State Security

Summary. The article presents the threat of information-psychological operations as the key element of information warfare. It's based on the thesis that the portfolio of hostile operations is becoming the main tool in the current geopolitics and its significance will continue to increase. The author indicates the secret service as the party physically executing these operations and points to the Russian Federation as direct threat to Poland. Information warfare, information-psychological operations and reflexive control significantly influence the state's information security and consequently Poland's vested interests.

Keywords: information warfare, information operations, psychological operations, information-psychological operations, operational psychology, reflexive control