Tomasz Aleksandrowicz

Wyższa Szkoła Policji w Szczytnie
ORCID: 0000-0002-3419-5577

MECHANIZMY ATAKU INFORMACYJNEGO. SKUTECZNOŚĆ PRZECIWDZIAŁANIA

Abstrakt

Tekst poświęcony został analizie mechanizmu ataków informacyjnych i warunków ich skuteczności. Autor koncentruje uwagę na wypracowaniu mechanizmów odporności na tego typu ataki oraz postuluje budowę defensywnych i ofensywnych zdolności państwa w obszarze walki informacyjnej. Jednocześnie proponuje podstawowe warunki budowy efektywnie działającego systemu. Autor wychodzi z założenia, iż kluczowym warunkiem skuteczności prowadzonych ataków informacyjnych jest mechanizm opisany w pracach Antoniego Kępińskiego jako metabolizm informacyjny, stąd też system przeciwdziałania również musi być oparty na tym mechanizmie.

W przeprowadzonych badaniach zastosowano analizę systemową, wykorzystując także metodę *case studies*, uogólnienia, abstrahowanie i syntezę.

• Słowa kluczowe: walka informacyjna, atak informacyjny, zdolności defensywne i ofensywne w obszarze walki informacyjnej.

Abstract

This paper is devoted to the analysis of the mechanism of information attacks, the conditions of their effectiveness, and the principles of building resistance into a system. The author focuses his attention on developing mechanisms of resistance

to this type of attacks and postulates the construction of defensive and offensive capabilities of the state in the area of information warfare, proposing the basic conditions for building an effective system.

The author states that the key condition for the effectiveness of information attacks is the mechanism described in the works of Antoni Kępiński as information metabolism. This makes it possible to formulate a postulate about the need to counteract such attacks based on building defensive and offensive capabilities of the state in the sphere of information warfare using mechanisms described by Kępiński.

The conducted research used system analysis, as well as case studies, generalizations, and synthesis. This allowed the author to state that the key condition for the effectiveness of information attacks is the mechanism described in the works of Antoni Kępiński as information metabolism.

• Keywords: information warfare, information attack, defensive an offensive abilities in information warfare.

Wstęp

W warunkach społeczeństwa informacyjnego infosferę należy traktować w kategoriach środowiska bezpieczeństwa, w którym występują szanse, wyzwania, zagrożenia i ryzyko. Z punktu widzenia bezpieczeństwa narodowego należy skupić się na cechach współczesnej infosfery, które umożliwiają powstawanie zagrożeń[1]. Przede wszystkim uwagę zwraca nie tylko powszechna dostępność informacji, lecz także niemal nieograniczona swoboda ich publikowania. Wiąże się to ze wzrostem dostępnych kanałów informacyjnych, których wykorzystanie – zarówno przez odbiorcę, jak i nadawcę –

[1] T. Aleksandrowicz, *Infosfera jako środowisko bezpieczeństwa państwa. Próba konceptualizacji problemu*, [w:] A. Kozera, E. Sadowska (red.), *Nauka i praktyka bezpieczeństwa. Księga pamiątkowa Leszka Fryderyka Korzeniowskiego, profesora Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie*, Kraków 2019, s. 308 i nast.

nie wymaga szczególnych zdolności technicznych i jest stosunkowo tanie, co oznacza ich powszechność. Powoduje to nadmiar informacji, których odbiorca nie jest w stanie poddać stosownej analizie, nie wspominając już o weryfikacji wiarygodności ich źródeł. Sytuację komplikuje dodatkowo to, że coraz więcej osób traci zaufanie do mediów związanych z establishmentem (np. do agencji informacyjnych, tytułów prasowych, telewizji – niezależnie od tego, czy są one odbierane w Internecie, czy w sposób klasyczny), zdecydowanie bardziej ufając mediom społecznościowym, np. Facebookowi czy Twitterowi i treściom tam publikowanym. Coraz większa liczba osób wykorzystuje media społecznościowe jako źródło informacji. Z badań prowadzonych przez *Pew Research Center* wynika np., że 44% Amerykanów korzystało z mediów społecznościowych w celu uzyskania informacji na temat kampanii prezydenckiej w 2016 r. Inni badacze podają, że było to nawet 62%[2]. Inne badanie tego ośrodka wskazuje, że zaufanie do tradycyjnych mass mediów, a więc telewizji, prasy, radia czy agencji informacyjnych, oscyluje na poziomie 50%[3].

Nadmiar informacji powoduje, że odbiorca musi wykształcić swego rodzaju filtr informacyjny, dzięki któremu będzie mógł skupić uwagę na kwestiach go interesujących, tych, które uznaje za ważne oraz – *last but not the least* – nie powodują u niego poczucia dysonansu poznawczego, a więc nie są sprzeczne z jego przekonaniami, wartościami, poglądami.

Taki stan rzeczy powoduje, że we współczesnej infosferze w dość prosty sposób można dokonywać skutecznych ataków informacyjnych, mających skłonić określone grupy społeczne do zachowań zakładanych przez napastnika, np. do głosowania na określonego kandydata w wyborach czy protestu przeciwko polityce rządu. Wiąże się to także ze zmianami, jakie w pierwszym dwudziestoleciu naszego stulecia zaszły w charakterze konfliktów. Celem

[2] K. Pałka-Suchojad, *Wojna na tweety, czyli o weaponizacji mediów społecznościowych*, [w:] A. Kasińska-Metryka, R. Dudała, T. Gajewski (red.), *Słowa jak kamienie. Mowa nienawiści, kłamstwo, agresja w sieci. Kompendium wiedzy o języku w życiu publicznym*, Kraków–Nowy Targ 2019, s. 102–103.

[3] *Global Trends: Paradox of Progress*, January 2017, NIC 2017–001, s. VII, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf [dostęp: 30.01.2017].

uderzeń nie są już siły zbrojne przeciwnika, lecz społeczeństwo – jego świadomość, przekonania, nastawienie do określonych kwestii. Zwycięstwo w takim konflikcie oznacza nie pokonanie sił zbrojnych przeciwnika na polu walki, a dezorganizację jego systemów informacyjnych, społecznych, politycznych czy gospodarczych[4]. Warto w tym kontekście podkreślić, iż narzędzia do prowadzenia takich działań pozostają do dyspozycji nie tylko państw, lecz także podmiotów pozapaństwowych, takich jak firmy komercyjne czy organizacje przestępcze, w tym terrorystyczne. Tworzy to nowe realia środowiska bezpieczeństwa, w których państwo musi zyskać zarówno zdolności defensywne, jak i ofensywne, a więc musi stać się odporne na ataki informacyjne, a równocześnie być w stanie samemu przeprowadzać takie ataki, choćby w postaci kontrdziałań.

Mechanizm ataku informacyjnego

Stworzenie przez odbiorcę filtra informacyjnego powoduje, że zaczyna on funkcjonować w swoistej bańce informacyjnej, a więc pozyskuje wyłącznie te informacje, które – z różnych przyczyn – uznaje za wiarygodne i potrzebne. Na tej podstawie podejmuje następnie decyzje, których konsekwencje analizuje także przez pryzmat swoich uprzedzeń i preferencji informacyjnych, umacniając tym samym szczelność swojej bańki informacyjnej. Jest to mechanizm, który polski psychiatra prof. Antoni Kępiński nazwał metabolizmem informacyjnym. Jego zdaniem metabolizm informacyjny składa się z dwóch faz: w pierwszej człowiek dąży do zdobycia orientacji w świecie zewnętrznym, aby ograniczyć tworzone przez siebie modele rzeczywistości i móc podjąć decyzje o własnym działaniu. W fazie drugiej podejmuje działania na podstawie wybranego modelu i odbiera informacje dotyczące własnej działalności. Powstaje zatem pętla sprzężenia zwrotnego:

[4] T. Aleksandrowicz, *Wojna jako narzędzie polityki w XXI wieku. Stare pojęcia – nowe konotacje*, [w:] W. Kostecki, K. Smogorzewski (red.), *Siła we współczesnych stosunkach międzynarodowych*, Warszawa 2017, s. 85 i nast.

odbiór informacji na temat otaczającej rzeczywistości – tworzenie modelu rzeczywistości – działanie – pozyskiwanie informacji o swoich działaniach[5]. Człowiek, postrzegając rzeczywistość, tworzy pewien jej model (a więc z definicji – uproszczenie) i dopiero na tej podstawie podejmuje decyzje. Jeśli postrzeganie rzeczywistości jest w jakikolwiek sposób zakłócone – czy to przez czynniki zewnętrzne, czy to na skutek cech samego obserwatora – model przezeń tworzony, a tym samym podejmowane na jego podstawie decyzje, odbiegają od obiektywnej rzeczywistości[6]. Każdy odbiorca informacji tworzy zatem określony profil informacyjny, który można rozpoznać i wykorzystać.

Podobnie charakteryzuje problem rosyjski psycholog i matematyk Vladimir Lefebvre (wł. Władimir Lefewr), twórca koncepcji zarządzania refleksyjnego. Nie wdając się w tym miejscu w szczegóły, należy wskazać, iż istotą koncepcji zarządzania refleksyjnego jest przyjęcie następującego założenia: każdy obiekt nie tylko tworzy w swojej świadomości 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 itd.) można z zewnątrz wpływać na te procesy m.in. za pomocą procesu przekazania fałszywej informacji o danej sytuacji lub nieprawdziwego obrazu danego obiektu, sformułowania korzystnej dla siebie doktryny i przekazania jej przeciwnikowi tak, by podejmował on na jej podstawie korzystne dla nas działania, czy też za pomocą neutralizacji dedukcji przeciwnika, czyli jego dezorientacji poprzez wykreowanie kilku fikcyjnych celów uniemożliwiających odkrycie celu rzeczywistego. W ten sposób można dokonać głębokiej

[5] A. Kępiński, *Lęk*, Kraków 2007, s. 20 i nast.; idem, *Melancholia*, Warszawa 1974, s. VI–VII, 156–254.

[6] T. Aleksandrowicz, *The Concept of Information Metabolism by Antoni Kępiński and the Mechanism of Information Manipulation. Conditions for Effectiveness and Ways of Counteraction*, „Security Dimensions" 2020, nr 33, s. 150–165, https://securitydimensions.publisherspanel.com/resources/html/article/details?id=205886 [dostęp: 4.01.2021].

transformacji masowej świadomości społeczeństwa i zmienić jego moralno-psychologiczny stan[7].

Planowanie ataku informacyjnego obejmuje kilka stadiów. Krok pierwszy to wybór celów, jakie atakujący chce osiągnąć. Rzecz jasna, cele te muszą wynikać bezpośrednio z przyjętej przez atakującego strategii politycznej i nie powinny być wymyślane *ad hoc*. Jako przykład może służyć dążenie Rosji do zmniejszenia poziomu jedności Zachodu (Unii Europejskiej) tak, by łatwiej móc nawiązywać relacje z poszczególnymi państwami, a nie zjednoczoną Unią jako całością.

Drugi krok to rozpoznanie tych elementów w sytuacji politycznej/społecznej atakowanego, które można wykorzystać w charakterze punktu wyjścia do wrogich działań informacyjnych. Z reguły są to sytuacje prawdziwe, bowiem oparcie się na kłamstwie przynosi zazwyczaj krótkotrwały efekt. Może to być np. wzrost bezrobocia, społeczna obawa przed napływem uchodźców czy też niezadowolenie z nadmiernych regulacji wprowadzanych przez Unię Europejską.

Trzeci krok to rozpoznanie profilu informacyjnego odbiorców, które stwarza szanse na to, że przekaz informacyjny do nich adresowany będzie postrzegany jako wiarygodny. Rzecz jasna, nie chodzi tu o pojedynczego odbiorcę, lecz o całe ich grupy reprezentujące określone, przydatne z punktu widzenia atakującego, cechy. Służy temu tzw. *data mining* – zdobywanie informacji o pojedynczych osobach i agregacja danych znajdujących się w różnych bazach, przy czym część z nich jest dostępna legalnie, zaś dostęp do innych wymaga naruszania prawa[8]. *De facto* jest to *microtargeting*, a więc rozpoznanie profilu odbiorcy tak, aby można było przygotować dla niego ofertę zgodną z jego zainteresowaniami i nie tracić czasu ani pieniędzy na reklamowanie miłośnikowi wędkarstwa akcesoriów do polowania,

[7] Zainteresowany tą problematyką Czytelnik znajdzie je w artykule Michała Wojnowskiego *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12(7), s. 11–36, zob. na ten temat: T. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 163 i nast.

[8] T. Aleksandrowicz, *Podstawy walki informacyjnej*, s. 42–44.

oraz unikanie wpadek reklamowych, np. reklamowanie takich akcesoriów zdecydowanemu przeciwnikowi polowań.

Już wykorzystanie tej metody w sferze komercyjnej jest niepokojące, pozwala bowiem na niemal nieskrępowane kreowanie trendów w zachowaniach, modzie, preferencjach zakupowych itd. Znacznie poważniejszego wymiaru nabiera jednak wykorzystanie jej w sferze politycznej. Pozyskiwane dane pozwalają na zbudowanie profilu wyborcy – określenie jego preferencji politycznych i siły, głębokości przekonań, otwartości na argumenty, a więc tego, na kogo chce głosować, dlaczego, jak zdecydowane są jego przekonania i jakie argumenty mogą to zmienić. Oznacza to manipulowanie poglądami politycznymi w celu uzyskania wpływu na decyzje wyborcze obywateli. Z takimi przypadkami już się spotkaliśmy, m.in. w wyborach prezydenckich w Stanach Zjednoczonych w 2016 r. czy w trakcie kampanii referendalnej w sprawie brexitu w Wielkiej Brytanii[9]. Główną rolę w tym procederze odegrała firma Cambridge Analytica, która pozyskała od Facebooka dane ponad 87 milionów użytkowników. Dotyczyły one nie tylko zachowań użytkowników na Facebooku, lecz także danych udostępnionych przez nich podczas korzystania z takich aplikacji, jak *Mafia Wars, Words with Friends* czy *Farmville* – aplikacje te miały dostęp do praktycznie wszystkich danych osobowych użytkowników. Przedstawiając zasady profilowania opracowane przez firmę, jej prezes, Aleksander Nix, stwierdził, że profilowanie psychograficzne, na podstawie którego można precyzyjnie adresować przekaz do konkretnego wyborcy, opiera się na modelu OCEAN. W jego ramach ustala się pięć cech charakteru, a więc: otwartość (*openess*) – na ile

[9] S. Vaidhyanathan, *Anti Social media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2019, s. 235 i nast.; A. Kazimierska, W. Brzeziński, *Strefy cyberwojny*, Warszawa 2018, s. 85 i nast.; T. Snyder, *Droga do niewolności. Rosja. Europa, Ameryka,* Kraków 2019, s. 10; *Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume I of II. Special Counsel Robert S. Mueller, III. Submitted Pursuant to 28 C.F.R. § 600.8(c),* Washington, D.C., March 2019, https://www.justice.gov/storage/report.pdf [dostęp: 4.01.2019.]; M. Wojnowski, *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 13 i nast.

chętnie badany akceptuje nowe doświadczenia, sumienność (*conscientiouness*) – do jakiego stopnia lubi porządek i powtarzalność albo zmianę i płynność, ekstrawersję (*extroversion*) – jak bardzo jest towarzyski, ustępliwość (*agreeableness*) – czy jest skłonny przedkładać potrzeby innych nad własne, oraz neurotyczność (*neuroticism*) – czy bardzo się niepokoi. Jak twierdzi Nix, „jeśli znamy osobowość ludzi, do których chcemy trafić, możemy zniuansować przekaz, żeby skutecznie przemówić do kluczowych grup elektoratu”[10]. Vaidhyanathan przywołuje przy tym raport ówczesnego dyrektora do spraw bezpieczeństwa Facebooka, Alexa Stamosa, zgodnie z którym w okresie od czerwca 2015 r. do maja 2017 r. około 100 tys. dolarów wydanych na reklamy na Facebooku, co przełożyło się na ok. 3 tysięce reklam, pochodziło z ok. 470 fałszywych kont i stron. Konta te były ze sobą powiązane, najprawdopodobniej sterowano nimi z Rosji. Większość reklam nie wymieniała bezpośrednio nazwiska kandydata, ale ewidentnie skupiała się na przekazie pogłębiającym społeczne i polityczne podziały w różnych obszarach ideologicznego spektrum – poruszały zagadnienie praw LGTB, kwestie rasowe, problematykę imigracji, dostępu do broni. Według specjalistów od reklamy przekazy te trafiły do 23–70 milionów osób (precyzyjnej liczby prawdopodobnie nie uda się obliczyć)[11].

Poznanie profilu odbiorcy (a precyzyjnie – dużych grup odbiorców o określonych cechach) pozwala na przygotowanie stosownie spreparowanej informacji. Jej osią – jak już wspomniano – jest fakt czy sytuacja, mające miejsce naprawdę, manipulacja z reguły polega na udramatyzowaniu, przesadzie, wskazaniu przyczyn itd., by ostateczny efekt był korzystny dla atakującego. Można w tym kontekście posłużyć się przykładem zaginięcia w Niemczech 13-letniej Lisy. Celem operacji informacyjnej było osłabienie pozycji politycznej kanclerz Angeli Merkel przy wykorzystaniu narastających w Niemczech obaw przed napływem imigrantów muzułmańskich i forsowanej przez Merkel polityki otwartych drzwi, osią był fakt zaginięcia dziewczynki. W styczniu 2016 r. w Berlinie rodzice zgłosili policji zaginięcie

[10] S. Vaidhyanathan, op. cit., s. 240–243, 248, 255.
[11] Ibidem, s. 282.

13-letniej dziewczynki pochodzącej z mieszkającej w Niemczech rodziny rosyjskiej; miała ona zostać uprowadzona i zgwałcona przez dwóch mężczyzn pochodzących z Bliskiego Wschodu. W sprawie tej wypowiadał się publicznie sam minister spraw zagranicznych Federacji Rosyjskiej Siergiej Ławrow, który wyrażał nadzieję, iż problemy z imigrantami w Niemczech nie doprowadzą do zatuszowania sprawy z przyczyn politycznych. O sprawie w bardzo emocjonalny sposób informowały rosyjskie media; niemiecka diaspora w Niemczech zorganizowała pod wpływem tych doniesień demonstrację uliczną. Ostatecznie okazało się, że 13-letnia Lisa spędziła noc u swojego przyjaciela, nikt jej nie uprowadził i nie zgwałcił[12]. Brak szczegółowych badań na ten temat, trudno więc odpowiedzieć na pytanie, jaki procent odbiorców, którzy dali wiarę informacjom preparowanym przez Rosjan, zostało przekonanych o pomyłce po ogłoszeniu przez władze, że dziewczynka wróciła do domu cała i zdrowa oraz do jakiego odsetka tych odbiorców w ogóle dotarła taka informacja.

Krok czwarty to odpowiedni dobór kanałów informacyjnych, przede wszystkim pod kątem ich wiarygodności w oczach odbiorców. Odnosząc się do przywołanego powyżej przykładu, można stwierdzić, iż nie każdy odbiorca informacji w krajach zachodnich da wiarę enuncjacjom rosyjskiego ministra spraw zagranicznych czy rosyjskich dziennikarzy. Nieocenioną rolę odgrywają w tym przypadku media społecznościowe, dające niemal nieograniczone możliwości przekazu informacyjnego, szczególnie przy wykorzystaniu jednej z cech sieci, jaką jest efekt kaskadowy, co gwarantuje dotarcie do dużych grup społecznych. Są one wykorzystywane szczególnie wobec tych odbiorców, którzy z nieufnością traktują media oficjalne, uznając je za establishmentowe czy prezentujące punkt widzenia establishmentu, a więc niejako z definicji niewiarygodne. Dodatkowym atutem jest anonimowość w sieci: można publikować informacje jako „naoczny świadek" czy „ekspert" itd., zwłaszcza że jeden człowiek może obsługiwać kilka różnych kont w mediach

[12] *Uprowadzenie i gwałt 13-latki? Ławrow żąda od Niemiec wyjaśnień*, http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosja-siergiej-lawrow-atakuje-niemcy-pyta-o-gwalt-na-13-latce,613989.html [dostęp: 19.02.2017].

społecznościowych. Z reguły przeciętny odbiorca nie będzie zadawał sobie trudu weryfikacji wiarygodności źródła. Ważne jest także wykorzystanie zasady, iż z reguły informacja o danej sytuacji jest traktowana jako wiarygodna, jeśli nie powoduje u odbiorcy dysonansu poznawczego, natomiast jej zaprzeczenie i wyjaśnienie albo nie trafia do odbiorcy z powodu jego funkcjonowania w bańce informacyjnej, albo też nie jest traktowane jako wiarygodne. Możliwa jest też reakcja odbiorcy polegająca na odrzuceniu obu wersji i przyjęcie postawy niechętnie obojętnej (wszyscy kłamią, chcąc wprowadzić społeczeństwo w błąd).

Warunki skuteczności przeciwdziałania atakom informacyjnym

Powyższe konstatacje jednoznacznie wskazują na konieczność uznania ataków informacyjnych za element walki informacyjnej rozumianej jako całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów. Istotą walki informacyjnej jest zniszczenie lub degradacja wartości zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, a z drugiej strony – zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych. Natomiast jako narzędzia wykorzystywane w tej walce można wskazać m.in.:

- dyplomację,
- propagandę,
- kampanie psychologiczne,
- działania podejmowane na poziomie wpływania na procesy polityczne lub kulturowe,
- dezinformację, manipulowanie lokalnymi mediami[13].

[13] T. Aleksandrowicz, *Podstawy walki informacyjnej*, passim.

W opracowanym w Biurze Bezpieczeństwa Narodowego projekcie Doktryny Bezpieczeństwa Informacyjnego RP z 24 lipca 2015 r.[14] bezpieczeństwo informacyjne traktowane jest jako jeden z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, które nosi charakter transsektorowy i wpływa na efektywność funkcjonowania całego systemu bezpieczeństwa. W tym ujęciu bezpieczeństwo informacyjne zdefiniowane zostało jako transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego państwa oraz proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Cele te osiąga się poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Typizując zagrożenia w obszarze wewnętrznym, projekt dzieli je na zagrożenia związane z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego, zagrożenia związane z funkcjonowaniem w cyberprzestrzeni i przestrzeni medialnej oraz – jako wyodrębniony punkt – zagrożenia związane z eksploatowaniem drażliwych kwestii w kontaktach międzynarodowych, w tym bilateralnych, przy wykorzystaniu wsparcia określonych podmiotów i osób. Zagrożeniem płynącym z funkcjonowania w środowisku informacyjnym może być rozpowszechnianie i powielanie treści propagandowych, mające na celu ukazanie polskiej racji stanu w negatywnym świetle, co *de facto* szkodzi interesowi państwa (stosowanie prowokacji, celowe manipulowanie przekazem poprzez wyrwanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru). Precyzując te zagrożenia, w Projekcie zalicza się do nich następujące:

[14] *Doktryna Bezpieczeństwa Informacyjnego RP (projekt)*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3.03.2016].

- występowanie w społeczeństwie deficytów informacyjnych, skutkujących podatnością na wrogą perswazję,
- potencjalna dezinformacja obywateli poprzez agresywne działania propagandowe,
- dywersja ideologiczna – narzucanie obcych idei niezgodnych z interesem państwa,
- pojawienie się i rozwój postaw antypaństwowych, nasilenie się postaw agresywnych, defetystycznych,
- wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych zgodnych z intencjami informacyjnego przeciwnika,
- istnienie (tworzenie) agentury wpływu (inspirowanie do zakładania oraz wsparcie polityczne i finansowe formacji politycznych lub organizacji społecznych wspierających i realizujących obce interesy w Polsce),
- wpływanie na opinię publiczną przez agentów zmiany sterowanych z zewnątrz, zwłaszcza aktywizacja wybranych grup społecznych przez inne państwo oraz realizacja interesów obcych państw, sprzecznych z interesem RP,
- obniżanie się morale społeczeństwa w przypadku agresji informacyjno-propagandowej, rzutujące negatywnie na polityczno-militarne procesy decyzyjne.

Zdolność do skutecznego przeciwstawienia się atakom informacyjnym przeciwnika jest zatem równoznaczne z osiągnięciem przez państwo zdolności defensywnych i ofensywnych w obszarze walki informacyjnej. Nie jest to sprawa prosta i kwestia podjęcia działań o charakterze systemowym i powstania rozproszonego systemu opartego na partnerstwie publiczno-prywatnym.

Odporność państwa na działania dezinformacyjne musi mieć, siłą rzeczy, charakter rozproszony, bowiem ataki dezinformacyjne kierowane są zarówno przeciwko państwu, jak i społeczeństwu. W gruncie rzeczy mamy zatem do czynienia z koniecznością ochrony przed dezinformacją nie tylko poszczególnych ogniw aparatu państwowego, lecz także opinii publicznej czy też instytucji społeczeństwa obywatelskiego. Nietrudno zauważyć, że te dwie kwestie wzajemnie się warunkują i uzupełniają. Budowanie takiej odporności

wymaga pracy u podstaw, pracy organicznej i – wobec faktu, że zarysowane powyżej tendencje zmian w infosferze będą się nasilać w dającej się przewidzieć przyszłości – obliczonej na lata.

Punktem wyjścia w tym zakresie musi stać się edukacja. Jak zauważa Witold Sokała, w warunkach jednoczesnego serwowania przez media zbyt wielu interdyscyplinarnych informacji ich krytyczna analiza przekracza możliwości jednostki, a systemy edukacji nie znajdują na to wyzwanie odpowiedzi[15]. Oznacza to konieczność zmian zarówno w systemie edukacji, jak i szkolnictwa wyższego. Programy szkolne muszą przyjąć jako punkt wyjścia fakt, iż Internet, a w tym media społecznościowe, stanowi obecnie dla młodzieży podstawowe źródło informacji i wiedzy, znacznie bardziej atrakcyjne niż obowiązkowe podręczniki i lekcje z nauczycielami, z jakimi stykają się w szkole. Pod tym względem szkoła nie pozwala nie tylko na nauczenie się krytyki źródeł, ale też na ich weryfikację – obowiązuje jedna interpretacja i jedno jej źródło, czyli podręcznik. Jest to zaprzeczenie krytycznego myślenia, które – wobec nasilających się zagrożeń w infosferze – absolwent musi wynieść ze szkoły jako swoje intelektualne wiano na resztę życia. Umiejętność weryfikacji – choćby pobieżnej – źródeł informacji, konfrontacji różnych opinii, a przede wszystkim odróżnienia informacji od opinii jest niezbędna do funkcjonowania w dzisiejszej infosferze. Lekcje informatyki nie mogą ograniczać się do bezpiecznego surfowania po Internecie (choć oczywiście jest to umiejętność konieczna), lecz także muszą obejmować nauczanie krytycznej oceny źródeł internetowych i analizy informacji. Takie elementy wykształcenia szkolnego bez żadnej wątpliwości będą nie tylko przydatne, ale wręcz wskazane dla zachowania bezpieczeństwa informacyjnego społeczeństwa poprzez budowanie odporności na dezinformację. Nie trzeba dodawać, że znacząco wpłynie to na poziom bezpieczeństwa informacyjnego państwa.

[15] W. Sokała, *Współczesna edukacja – tarczą przeciwko BMM (Broni Masowej Manipulacji)?*, [w:] K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014, s. 48.

Drugi element to zwiększenie poziomu zaufania i wiarygodności źródeł oficjalnych (komunikatów władzy) i establishmentowych (mediów masowych, tzw. mainstreamu). Taką wiarygodność łatwo jest utracić, znacznie trudniej odbudować czy zbudować. Nie będzie wszakże przesadą stwierdzenie, iż społeczeństwo musi mieć poczucie, że istnieją takie źródła informacji, które są wiarygodne i przekazują informacje prawdziwe, w oczywisty dla odbiorcy sposób oddzielone od opinii czy sugestii. Podobne uwagi należy sformułować pod adresem źródeł naukowych – tu wielka, nie do przecenienia jest rola czasopism naukowych, portali internetowych dotyczących różnych dziedzin wiedzy, wreszcie mediów propagujących wiedzę naukową w sposób popularny, zrozumiały dla przeciętnego odbiorcy, zawierający wyjaśnienia i interpretacje. W rezultacie spadnie poziom wiary w różnego rodzaju teorie spiskowe, co jest szczególnie istotne w sytuacjach zagrożeń i niepokojów.

Trzeci element to stworzenie instytucji (zarówno na poziomie państwa, jak i społeczeństwa obywatelskiego czy mediów masowych) zajmujących się demaskowaniem nie tylko poszczególnych przykładów dezinformacji, lecz także całych kampanii dezinformacyjnych obliczonych czy to na uzyskanie wpływu na społeczeństwo, czy też na podejmowanie przez różne ogniwa aparatu państwowego decyzji na podstawie zmanipulowanych informacji. Pozostaje faktem, że w środowisku dziennikarskim podejmowane są już udane próby prowadzenia działalności typu *fact checking* (sprawdzanie wiarygodności informacji podawanych przez różne źródła) i demaskowania informacji nieodpowiadających prawdzie. Jest to także swoisty bat na polityków różnych szczebli, którzy w ferworze walki politycznej i motywowani chęcią przeforsowania swojego stanowiska częstokroć sami mijają się z prawdą.

Z punktu widzenia bezpieczeństwa informacyjnego państwa kluczowe jest jednak powołanie instytucji zajmującej się takimi kwestiami na poziomie rządowym oraz jej odpowiedników w departamentach poszczególnych ministerstw. Powinny one pełnić funkcję swoistego dzwonka alarmowego ostrzegającego decydentów przed podejmowaniem decyzji na podstawie zmanipulowanych, nierzetelnych informacji. Nieco odrębna wydaje się być

w tym kontekście rola służb specjalnych rozumianych jako służby informacyjne państwa. Ich rolą powinno być zdobywanie wiedzy o tym, czy źródła upowszechniające nieprawdziwe, zmanipulowane informacje nie są częścią aparatu obcego państwa bądź też nie pracują na jego zlecenie (np. w roli agentury wpływu). To bardzo złożona i trudna kwestia; nie sposób bowiem oskarżać pojedynczego użytkownika mediów społecznościowych o współpracę z obcym wywiadem i udział w operacji dezinformacyjnej tylko dlatego, że powielił i upowszechnił on zmanipulowaną informację podaną przez inne źródło – z tego punktu widzenia jest on raczej ofiarą kampanii dezinformacyjnej. Wszelako trudno zaprzeczyć, iż istnieją i działają takie podmioty, które powielają dezinformację czy też opracowują jej własne, „autorskie" wersje, czyniąc to na zlecenie przeciwnika. Rola kontrwywiadu – już choćby w zakresie zdobywania w tej materii wiedzy operacyjnej, niekoniecznie procesowej, a więc prowadzącej do oskarżenia o współpracę z obcym wywiadem – wydaje się być oczywista.

W tym kontekście musimy powrócić do kwestii wykształcenia, tym razem na poziomie wyższym i specjalistycznym. Praca w tego typu instytucjach wymaga wiedzy i umiejętności z zakresu analizy informacji. Instytucje takie muszą być wyłączone z bieżącej gry politycznej, a osoby przygotowujące analizy na temat rozpoznawanych kampanii dezinformacyjnych nie mogą doświadczać syndromu posłańca przynoszącego złe wieści. To również jest bardzo trudne zadanie, gdyż biurokracja rządowa, a mówiąc precyzyjnie, jej aparat polityczny, ma naturalne w swojej istocie tendencje do włączania wszystkich ogniw aparatu państwowego do bieżącej walki politycznej. Jest to szczególnie widoczne w okresie kampanii wyborczych. Praca analityka w administracji rządowej charakteryzuje się specyfiką wynikającą z samego charakteru i istoty aparatu administracyjnego. Jest to struktura biurokratyczna, hierarchiczna, z reguły wysmukła, działająca według schematów pionowego podporządkowania. Analityk jest zatem – z tego punktu widzenia – elementem procesu zarządzania w strukturach biurokratycznych. Innymi słowy, jest urzędnikiem zajmującym określone w pragmatyce służbowej stanowisko, posiada zakres obowiązków i kompetencji, podlega dyscyplinie służbowej itd., a więc – z formalno-prawnego punktu widzenia – niczym

nie różni się od innych urzędników. Ideałem jest tu postawa wskazująca na pełną niezależność intelektualną analityka. Można w tym kontekście zacytować słowa brytyjskiego historyka, Christophera Andrew, który rozważając rolę służb specjalnych w państwie demokratycznym, przywołał wypowiedź jednego z szefów brytyjskiej *Secret Intelligence Service*, opisującego swoje obowiązki krótkim, ironicznym stwierdzeniem: „[...] moim zadaniem jest mówienie premierowi tego, czego on nie chce usłyszeć”[16]. Parafrazując te słowa, można powiedzieć, iż rolą analityka jest mówienie decydentowi tego, czego decydent nie chce usłyszeć; jest to sytuacja modelowa (idealna), której osiągnięcie wymaga zaangażowania się i odpowiednich postaw zarówno ze strony decydenta, jak i analityka. Można też powiedzieć, że konieczne jest stworzenie takiego systemu, który w jak największym stopniu gwarantuje analitykowi intelektualną niezależność[17]. Służyć może temu także wykorzystanie przez struktury rządowe efektów pracy podmiotów niezależnych.

Skuteczność przeciwdziałania atakom dezinformacyjnym i zbudowanie odporności państwa i społeczeństwa na nie wymaga zatem spełnienia szeregu warunków i przyjęcia strategii i polityki państwa w tym zakresie.

Punktem wyjścia jest rozpoznanie celów strategicznych potencjalnego przeciwnika, co pozwoli na określenie możliwych linii ataku. Do tego celu niezbędne jest stworzenie silnych ośrodków analitycznych stosujących metody białego wywiadu i analizy informacji; przykładem może służyć Ośrodek Studiów Wschodnich. Do zdobycia tej wiedzy nie są konieczne (choć na pewno przydatne) informacje pochodzące z twardego wywiadu operacyjnego; znaczenie źródeł otwartych zawsze było bardzo silnie akcentowane. Już w 1947 r. jeden z założycieli Centralnej Agencji Wywiadowczej i twórca amerykańskiej szkoły analizy wywiadowczej, Sherman Kent, szacował, że w czasie pokoju

[16] Ch. Andrew, *Twenty-First Century Intelligence in Long-Term Perspective*, maszynopis powielony, w posiadaniu autora.

[17] T. Aleksandrowicz, *Analityk w administracji rządowej*, [w:] K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), *Analiza informacji w zarządzaniu bezpieczeństwem*, Warszawa 2013, s. 11 i nast.

ok. 80% informacji niezbędnych politykom do podejmowania decyzji należy do kategorii ogólnodostępnych[18]. „Informacje wywiadowcze zdobywa się w różny sposób, nie wszystkie z nich stanowią tajemnice i sekrety. W szczególności dotyczy to białego wywiadu (*overt intelligence*), w ramach którego wykorzystywane są informacje pochodzące z gazet, książek, publikacji naukowych i technicznych, oficjalnych publikacji rządowych, radia i telewizji. Nawet powieść czy sztuka teatralna może zawierać użyteczne informacje na temat stanu państwa"[19].

Nie ulega wątpliwości, że z biegiem lat, a przede wszystkim ze wzrostem dostępności informacji w rezultacie rewolucji informacyjnej, szacunki ulegały zmianie na korzyść źródeł otwartych. Zdaniem gen. Samuela V. Wilsona, byłego dyrektora *Defence Intelligence Agency*, stosunek ten wynosił nawet 90 : 10[20].

W dalszej kolejności ważne jest rozpoznanie własnych słabych punktów, które mogą zostać wykorzystane przez przeciwnika jako wspomniany wyżej punkt wyjścia (oś) potencjalnego ataku informacyjnego. Jest to szczególnie trudne zadanie, ponieważ zmusza to urzędników/analityków pracujących dla rządu do swoistego samooskarżenia (robimy coś źle), co w strukturach biurokratycznych funkcjonujących w sferze politycznej wymaga odwagi i wiary, że przełożony nie potraktuje tego jako krytykanctwa i ataku na rząd, a wręcz – braku lojalności. Jest to szczególnie prawdopodobne, jeśli listę słabych punktów – potencjalnych osi ataku informacyjnego przedstawią ośrodki pozarządowe. Pewnym osłabieniem tego schematu jest zachowanie owych prac w poufności.

---

[18] *Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for National Defence Establishment, Submitted by Allen W. Dulles*, April 25, 1947, reprinted in U.S. Congress, 80th Congress, 1st session, Senate, Committee on Armed Services, National Defence Establishment (Unification of the Armed Services), Hearings, Part 1, s. 525.

[19] A. Dulles, *The Craft of Intelligence*, New York 1963, s. 55.

[20] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Warszawa 2009, s. 82–83.

Trzeci krok to rozpoznanie kanałów informacyjnych, jakimi może posłużyć się przeciwnik. Jest to praca żmudna, bowiem rzecz nie tylko w rozpoznawaniu np. kont twitterowych publikujących treści związane z atakiem informacyjnym, lecz także w prowadzeniu bieżącego monitoringu, gdyż konta takie pojawiają się i znikają w zależności od sytuacji. Nie sposób robić tego wyłącznie drogą śledzenia aktywności na tych kontach bezpośrednio przez człowieka, konieczne jest stworzenie stosownych algorytmów i automatyzacja tego procesu. Rzecz jasna, kwestia ta nie ogranicza się wyłącznie do mediów społecznościowych, należy wziąć pod uwagę także agenturę wpływu oraz – używając starego określenia – pożytecznych idiotów. To już zadanie dla kontrwywiadu.

Czwarta kwestia – konieczne jest podejmowanie działań wyprzedzających, a więc zwracanie uwagi na to, co może być osią ataku informacyjnego i narzucenie własnej interpretacji (narracji) w określonych sprawach. Mówiąc wprost, może to być atak informacyjny ukierunkowany na społeczeństwo/kierownictwo polityczne przeciwnika, którego celem jest wytrącenie/neutralizacja argumentów, mogących być wykorzystanymi przeciwko nam.

Sprawa piąta – to stworzenie wiarygodnych dla odbiorców kanałów informacyjnych, z których można korzystać przy prowadzeniu walki informacyjnej. Ten postulat wydaje się być rzeczą oczywistą, bowiem w przypadku skutecznego ataku informacyjnego próby przeciwstawienia się mu w postaci np. oświadczeń rządu czy wystąpień poszczególnych jego członków skazane są na porażkę, trafiają bowiem niemal wyłącznie do już przekonanych.

Punkt ostatni – to neutralizacja skutków skutecznego ataku informacyjnego. To zadanie niezwykle trudne, bowiem – jak wiadomo – skuteczniejsza jest informacja, w której zawarte są określone dane i interpretacje, niż zaprzeczenie jej. Również i w tym wypadku konieczne jest posiadanie wiarygodnych dla odbiorców informacji kanałów informacyjnych.

Nie ulega wątpliwości, iż osiągnięcie przez państwo zdolności ofensywnych i defensywnych wymaga współpracy publiczno-prywatnej, a więc współpracy rządu z szeroko rozumianymi reprezentacjami społeczeństwa obywatelskiego, niezależnymi think tankami i ośrodkami analitycznymi oraz środowiskiem naukowym. Infosfera traktowana w kategoriach środowiska

bezpieczeństwa, walka informacyjna i jej przejawy pozostają przedmiotem badań naukowych o charakterze interdyscyplinarnym, choć przede wszystkim w ramach dyscypliny nauk o bezpieczeństwie. W tym kontekście należy podkreślić, iż nauka nie może ograniczać się tylko do roli deskryptywnej i eksplanacyjnej, musi także – i to jest istotny punkt wspomnianej współpracy ośrodków akademickich i rządowych – wyciągać praktyczne wnioski i proponować stosowne rozwiązania utylitarne. Bez tego trudno będzie mówić o osiąganiu przez państwo zdolności defensywnych i ofensywnych w obszarze walki informacyjnej.

Wreszcie – *last but not the least* – konieczne jest przygotowanie i przeprowadzanie kampanii społecznych wskazujących na zagrożenia związane z dezinformacją, atakami informacyjnymi itd. Dobrym przykładem takich działań mogą służyć np. kampanie związane z bezpieczeństwem antyterrorystycznym[21].

Zakończenie: pigułki Murti Binga 2.0

W wydanej w latach 20. ubiegłego stulecia powieści *Nienasycenie* Stanisław Ignacy Witkiewicz kreśli obraz Polski rządzonej przez chaos, społeczeństwa pozbawionego jakiejkolwiek idei i celu, z powszechnym alkoholizmem, narkomanią, wynaturzeniami seksualnymi, zdegenerowaną i niezrozumianą sztuką – słowem obraz dekadencji, rozpaczy i beznadziei. Obrazu tego dopełniało wiszące nad Polską zagrożenie w postaci chińskiej armii nadciągającej ze wschodu, armii zwycięskiej, silnej, dobrze zorganizowanej, której atak na

[21] K. Jałoszyński, A. Letkiewicz (red.), *Edukacja antyterrorystyczna – konieczność i obowiązek naszych czasów/ Antiterrorism Education – Necessity and Responsibility of Our Times*, Szczytno 2010; A. Furgała, A. Tulej, D. Szlachrer, P. Chomentowski (red.), *Spójna antyterrorystyczna strategia informacyjna*. Tom I. *System ochrony antyterrorystycznej w Polsce ze szczególnym uwzględnieniem aspektów komunikacji ze społeczeństwem za pośrednictwem mediów i organizacji pozarządowych a rozwiązania prawno-organizacyjne w zakresie uprawnień środków masowej komunikacji*, Szczytno 2011.

Rzeczpospolitą nie pozostawiał wątpliwości co do wyniku starcia. Chińczycy jednak nie atakowali, a w Polsce pojawili się potajemnie wyznawcy Murti Binga oferujący chętnym nowy narkotyk – Dawamesk B2. Miał on szczególne działanie: po jego zażyciu delikwent postrzegał dowolną rzecz przedstawioną mu w imię nauki Murti Binga jako prawdę, ba – „Jedyną Prawdę". A „cały świat dawny z tajemnicami i cudami, przedstawiał się teraz jako niebezpieczny i męczący chaos, pełen rozkosznych schowków, ale i plugawych zasadzek, nieznanych możliwości, ale i mąk rozdwojenia i wynikających stąd bardziej realnych inkomodacji"; „taki osobnik zażywał pigułki, a potem już szło jak po maśle". Ludzie zajęli się działalnością społecznie użyteczną; wiersze były zrozumiałe, muzyka słuchana przez masy, życie nabrało sensu i celu. Chińczycy zwyciężyli bez walki – naczelny wódz udał się do chińskiej kwatery i poddał armię polską w imię nowego porządku i przyszłości; został z honorami ścięty. Nastał czas porządku, dobrobytu i społecznego spokoju[22].

Współczesne ataki informacyjne można nazwać swoistymi pigułkami Murti Binga 2.0. Pod ich wpływem ludzie podejmują decyzje korzystne dla atakującego, dokonują wyborów politycznych i komercyjnych, społeczeństwa podlegają – używając języka rosyjskich teoretyków – psychologicznej obróbce masowej świadomości, co w konsekwencji ma doprowadzić do destabilizacji państwa i narodu[23]. Jak stwierdza Siergiej Rastorgujew 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

[22] St.I. Witkiewicz, *Nienasycenie*, Kraków 2019, s. 164, 206, 379, 443, 447–449, 483. Do wątku pigułek Murti Binga sięgnął m.in. Czesław Miłosz, usiłując wyjaśnić fenomen zauroczenia intelektualistów stalinizmem, odwoływał się do niego także Paweł Śpiewak, opisując okres początku lat 90. w Polsce: Cz. Miłosz, *Umysł zniewolony*, Kraków 199, s. 25–27; P. Śpiewak, *Pamięć po komunizmie*, Gdańsk 2005, s. 6.

[23] M. Wojnowski, *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI wieku*, s. 27–28.

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”[24].

Skuteczne przeciwdziałanie atakom informacyjnym oznacza zatem – trzymając się tej przenośni – umiejętność stworzenia antidotum na pigułki Murti Binga 2.0, a w sferze ofensywnej – umiejętność wytworzenia własnych, stosowanych w imię racji stanu.

BIBLIOGRAFIA

1. Aleksandrowicz T., *Analityk w administracji rządowej*, [w:] K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), *Analiza informacji w zarządzaniu bezpieczeństwem*, Warszawa 2013, s. 11–27.
2. Aleksandrowicz T., *Biały wywiad w walce z terroryzmem*, [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałaniu terroryzmowi*, Warszawa 2009, s. 81–92.
3. Aleksandrowicz T., *Infosfera jako środowisko bezpieczeństwa państwa. Próba konceptualizacji problemu*, [w:] A. Kozera, E. Sadowska (red.), *Nauka i praktyka bezpieczeństwa. Księga pamiątkowa Leszka Fryderyka Korzeniowskiego, profesora Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie*, Kraków 2019, s. 308–323.
4. Aleksandrowicz T., *Podstawy walki informacyjnej*, Warszawa 2016.
5. Aleksandrowicz T., *The Concept of Information Metabolism by Antoni Kępiński and the Mechanism of Information Manipulation. Conditions for Effectiveness and Ways of Counteraction*, „Security Dimensions” 2020, nr 33, s. 150–165, https://securitydimensions.publisherspanel.com/resources/html/article/details?id=205886 [dostęp: 4.01.2021].

[24] О. Назаров, *Информационные войны – угроза для цивилизации*, „Литературная газета” 2013, nr 42. Cyt. za: J. Darczewska, *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?*, [w:] *Wojna hybrydowa. Przegląd Bezpieczeństwa Wewnętrznego*, wydanie specjalne, Warszawa 2015, s. 62–63, https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html [dostęp: 16.05.2022].

6. Aleksandrowicz T., *Wojna jako narzędzie polityki w XXI wieku. Stare pojęcia – nowe konotacje*, [w:] W. Kostecki, K. Smogorzewski (red.), *Siła we współczesnych stosunkach międzynarodowych*, Warszawa 2017, s. 165–193.
7. Andrew Ch., *Twenty-First Century Intelligence in Long-Term Perspective*, maszynopis powielony w posiadaniu autora.
8. Darczewska J., *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?*, [w:] *Wojna hybrydowa, Przegląd Bezpieczeństwa Wewnętrznego*, wydanie specjalne, Warszawa 2015, s. 59–73, https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPEC_JALNE.html [dostęp: 16.05.2022].
9. *Doktryna Bezpieczeństwa Informacyjnego RP,* https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3.03.2016].
10. Dulles A., *The Craft of Intelligence*, New York 1963.
11. Furgała A., Tulej A., Szlachrer D., Chomentowski P. (red.), *Spójna antyterrorystyczna strategia informacyjna.* Tom I. *System ochrony antyterrorystycznej w Polsce ze szczególnym uwzględnieniem aspektów komunikacji ze społeczeństwem za pośrednictwem mediów i organizacji pozarządowych a rozwiązania prawno-organizacyjne w zakresie uprawnień środków masowej komunikacji*, Szczytno 2011.
12. *Global Trends: Paradox of Progress,* January 2017, NIC 2017–001, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf [dostęp: 30.01.2017].
13. Jałoszyński K., Letkiewicz A. (red.), *Edukacja antyterrorystyczna – konieczność i obowiązek naszych czasów/ Antiterrorism Education – Necessity and Responsibility of Our Times*, Szczytno 2010.
14. Kazimierska A., Brzeziński W., *Strefy cyberwojny*, Warszawa 2018.
15. Kępiński A., *Lęk*, Kraków 2007.
16. Kępiński A., *Melancholia*, Warszawa 1974.
17. *Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for National Defence Establishment, Submitted by Allen W. Dulles*, April 25, 1947, reprinted in U.S. Congress, 80th Congress, 1st session, Senate, Committee on Armed Services, National Defence Establishment (Unification of the Armed Services), Hearings, Part 1.
18. Miłosz C., *Umysł zniewolony*, Kraków 1999.
19. Pałka-Suchojad K., *Wojna na tweety, czyli o weaponizacji mediów społecznościowych,* [w:] A. Kasińska-Metryka, R. Dudała, T. Gajewski (red.), *Słowa jak kamienie. Mowa nienawiści, kłamstwo, agresja w sieci. Kompendium wiedzy o języku w życiu publicznym*, Kraków–Nowy Targ 2019, s. 95–108.
20. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume I of II. Special Counsel Robert S. Mueller, III. Submitted Pursuant*

to 28 C.F.R. § 600.8(c), Washington, D.C. March 2019, https://www.justice.gov/storage/report.pdf [dostęp: 4.01.2019].
21. Snyder T., *Droga do niewolności. Rosja. Europa, Ameryka*, Kraków 2019.
22. Sokała W., *Współczesna edukacja – tarczą przeciwko BMM (Broni Masowej Manipulacji)?*, [w:] K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014, s. 63–73.
23. Śpiewak P., *Pamięć po komunizmie*, Gdańsk 2005.
24. *Uprowadzenie i gwałt 13-latki? Ławrow żąda od Niemiec wyjaśnień,* http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosja-siergiej-lawrow-atakuje-niemcy-pyta-o-gwalt-na-13-latce,613989.html [dostęp: 19.02.2017].
25. Vaidhyanathan S., *Anti Social media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2019.
26. Witkiewicz S.I., *Nienasycenie*, Kraków 2019.
27. Wojnowski M., *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 13–43.
28. Wojnowski M., *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12(7), s. 11–36.

1. *Информационные войны – угроза для цивилизации*, „Литературная газета" 2013 2013, nr 42.