Horyzonty Polityki
2016, Vol. 7, Nº 20

Tomasz Grabowski
Akademia Ignatianum w Krakowie
Instytut Nauk o Polityce i Administracji
e-mail: tomasz.grabowski@ignatianum.edu.pl

DOI: 10.17399/HP.2016.072002

Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)

Streszczenie

CEL NAUKOWY: Celem artykułu jest ukazanie współczesnych form walki informacyjnej.

PROBLEM I METODY BADAWCZE: Główny problem badawczy dotyczy odpowiedzi na pytanie o rolę zmagań w sferze informacyjnej we współczesnych konfliktach politycznych. Przyjęto hipotezę, iż rola ta wzrasta i skuteczne przeprowadzenie tego typu operacji jest niezbędne do odniesienia pełnego zwycięstwa. W pracy badawczej zastosowano metodę badania literatury przedmiotu i dokumentów źródłowych, metodę obserwacyjną, metodę analizy oraz metodę syntezy.

PROCES WYWODU: W toku wywodu omówiono kolejno takie zagadnienia jak główne cechy współczesnej walki informacyjnej oraz wybrane metody jej prowadzenia (operacje psychologiczne, propagandę, dezinformację, manipulację informacją, cyberataki społecznościowe). Opis każdej z nich poparto przykładami jej zastosowania w konkretnym przypadku, tj. w najnowszym konflikcie rosyjsko-ukraińskim.

WYNIKI ANALIZY NAUKOWEJ: Wyniki analizy pozwalają na sformułowanie oceny, że formy walki informacyjnej ulegają stałej ewolucji i udoskonaleniom. Wynika to głównie z rozwoju

Sugerowane cytowanie: Grabowski, T. (2016). Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016). *Horyzonty Polityki*, *7 (20)*, 27-53. DOI: 10.17399/HP.2016.072002.

technologicznego i powstawania nowych form komunikacji. Ponadto podmioty realizujące zadania w tej sferze tworzą nowe metody i techniki, aby unikać szablonowości i powtarzalności wcześniej zastosowanych rozwiązań. Analiza konfliktu rosyjsko-ukraińskiego z lat 2014-2016 prowadzi do wniosku, że operacje informacyjne miały zasadnicze znaczenie dla jego przebiegu i dotychczasowych wyników. Były istotnym komponentem tzw. wojny hybrydowej i pozwoliły stronie atakującej osiągnąć określone cele bez przekraczania tzw. progu agresji w jego tradycyjnym rozumieniu.

WNIOSKI, INNOWACJE, REKOMENDACJE: Doświadczenia te wskazują, iż wrogie działania informacyjne stanowią coraz większe zagrożenie i wymagają szczególnej uwagi podmiotów odpowiedzialnych za bezpieczeństwo narodowe.

Słowa kluczowe:
wojna informacyjna, operacja psychologiczna, dezinformacja, propaganda, cyberatak społecznościowy

METHODS OF THE INFORMATION WARFARE IN THE ELECTRONIC MEDIA ON THE BASE OF RUSSIAN-UKRAINIAN (2014-2016) CONFLICT

Abstract

REASERCH OBJECTIVE: The aim of the article is showing contemporary forms of the information warfare.

THE REASERCH PROBLEM AND METHODS: The main research problem is about answering a question about the role of competition in the information sphere in the contemporary political conflicts. There was made a hypothesis that this role is growing and carrying an operation in the information sphere is essential to succeed. The research work included the method of investigating a literature and source documents, the method of analysis and method of synthesis.

THE PROCESS OF ARGUMENTATION: There were discussed such issues as the main features of the contemporary information warfare and chosen methods of managing the warfare (psychological operation, propaganda, disinformation, manipulating information, social cyber attacks). The description of each method is supported by examples of using it in a particular case, i.e. in the contemporary Russian-Ukrainian conflict.

REASERCH RESULTS: The results of the analysis allow an evaluation that the contemporary forms of the information warfare are still evolving and are improved. It mainly results from the technological development and appearance of the new communication forms. What is more, the units that carry an activity in this sphere create new methods and techniques to avoid commonplaceness and repeatability of the previously used solutions. The analysis of the Russian-Ukrainian 2014-2016 conflict results in a conclusion that the informational operations have a significant meaning to its course and current results. The informational operations were a significant component of so-called hybrid war and allowed the offence to realize the target without crossing so-called aggression threshold.

CONCLUSIONS, INNOVATIONS AND RECOMENDATIONS: This experience shows that the enemy informational actions have become a more serious threat, and they require special attention of the units responsible for the national safety.

Keywords:
Information Warfare, Psychological Operation, Disinformation, Propaganda, Social Cyber Attack

WSTĘP

Celem artykułu jest ukazanie współczesnych form walki informacyjnej. Główny problem badawczy dotyczy odpowiedzi na pytanie o rolę zmagań w sferze informacyjnej we współczesnych konfliktach politycznych. Przyjęto hipotezę, iż rola ta wzrasta i skuteczne przeprowadzenie tego typu operacji jest niezbędne do odniesienia pełnego zwycięstwa. W pracy badawczej zastosowano metodę badania literatury przedmiotu i dokumentów źródłowych, metodę obserwacyjną, metodę analizy oraz metodę syntezy. Wykorzystano najnowsze dokumenty państwowe (polskie i zagraniczne) o charakterze doktrynalnym i koncepcyjnym, a także literaturę specjalistyczną, w tym najnowsze publikacje dotyczące bieżących konfliktów.

Polem badawczym były dla autora media elektroniczne, przez które rozumieć należy w szczególności media cyfrowe, a więc wszystkie formy (lub formaty) prezentacji i użytkowania treści (np. tekstowych, graficznych, audiowizualnych), które są zapisywane, odtwarzane, dystrybuowane i edytowane przy użyciu urządzeń, nośników

i systemów elektronicznych, działających na podstawie informacji przetwarzanych w systemie cyfrowym. Zapis cyfrowy w przeciwieństwie do analogowego jest nieciągły i niematerialny. Opiera się on na operowaniu wartościami liczbowymi (kodem liczbowym). Taka technologia umożliwia edycję i powielanie opisujących treści danych bez utraty ich jakości. Szczególną uwagę zwrócono na działania w Internecie – głównie z powodu gwałtownego rozwoju tego medium i wpływu, jaki ten proces wywiera na życie społeczeństw.

Pomimo iż problematyka walki informacyjnej nie jest nowa (była intensywnie eksplorowana m.in. w okresie zimnej wojny), to postawiony problem badawczy uznać należy za aktualny. Wynika to głównie z rozwoju technologicznego, wzrostu znaczenia działań w cyberprzestrzeni oraz rozwoju nowych metod działania w tej sferze. Rodzi to potrzebę powstania nowych prac o charakterze opisowym i systematyzującym wiedzę w tej dziedzinie.

1. ISTOTA WALKI INFORMACYJNEJ

„Sposobom produkcji odpowiadają sposoby destrukcji" – pisali Alvin i Heidi Toffler w swoim dziele *Wojna i antywojna* (za: Balcerowicz, 2013, s. 174). Zgodnie z ich teorią, struktura współczesnego świata zmienia się wraz z rewolucją metod wytwórczych. Po „falach" agrarnej i industrialnej, cywilizacja wchodzi w epokę informacyjną, w której narzędzia rolnicze i taśmę fabryczną zastępuje komputer. Rewolucji tej towarzyszy powstawanie środków i metod walki typowych dla świata cyfrowego. W 1994 r. Winn Schwartau opublikował książkę, w której po raz pierwszy zdefiniowano walkę informacyjną. Równolegle pojawiły się takie pojęcia jak: wojna/walka sieciowa, wojna/walka wirtualna, wojna/walka cybernetyczna (cyberwojna), cyberterroryzm i inne, próbujące wyjaśnić zjawisko wojny i konfliktu w epoce postindustrialnej. Co ważne, rewolucja informacyjna nie tylko zmieniła i wprowadziła nowe metody prowadzenia walki, ale także odcisnęła swoje piętno na życiu społeczeństw. Wysoko nasycone mediami, a jednocześnie postheroiczne (niezdolne do walki i związanych z nią poświęceń) społeczeństwa zachodnie stały się wyjątkowo wrażliwe na zagrożenia uderzające w sferę psychologiczną i mentalną, takie jak np. operacje informacyjne czy terroryzm (Munkler,

2004). Epoka cyfrowa w nowy sposób zaangażowała w konflikty ludność cywilną. Opinia publiczna potrafi zmienić decyzje rządów, warto więc „uderzyć" w ten czuły punkt państw zachodnich. Walka w niespotykanym dotąd stopniu przeniosła się do noosfery – sfery ludzkiej refleksji i świadomego myślenia. Zdaniem duńskiego analityka zajmującego się konfliktami w sieciach społecznościowych, w dzisiejszych konfliktach bardziej chodzi o uzyskanie kontroli nad zachowaniem ludności, procesem decyzyjnym oraz całą sferą polityczną aniżeli nad przestrzenią geograficzną (Nissen, 2015). Cel ten można zaś osiągnąć środkami pozamilitarnymi i nie przekraczając progu konwencjonalnej wojny. Być może dzięki zdobyczom epoki cyfrowej jeszcze nigdy największe możliwe osiągnięcie, o jakim pisał Sun Tzu (zwycięstwo bez podejmowania fizycznej walki), nie było tak łatwe jak współcześnie.

W 1994 r. Schwartau zdefiniował walkę informacyjną jako

> działanie ukierunkowane na ochronę, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji, albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem (za: Liedel, Piasecka i Aleksandrowicz, 2012, s. 15).

W myśl najnowszej polskiej definicji, pochodzącej z *Projektu Doktryny bezpieczeństwa informacyjnego RP*, walka informacyjna to

> 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 (Biuro Bezpieczeństwa Narodowego, 2015b, s. 4).

Swoją definicję stworzyło też Ministerstwo Obrony Rosji, dla którego jest to

> walka pomiędzy państwami w przestrzeni informacyjnej w celu uszkodzenia systemów informacyjnych, przetwarzania danych oraz zasobów, struktur newralgicznych i innych, zachwianie systemów

> politycznych, ekonomicznych i społecznych, jak również narzucenie danemu państwu podejmowania zadań w interesie strony przeciwnej (Ministerstvo Oborony Rossijskoj Federacii, 2012).

To tylko kilka spośród bardzo wielu definicji powstałych w środowiskach eksperckich, akademickich czy instytucjach państwowych odpowiedzialnych za bezpieczeństwo. W większości z nich powtarza się stwierdzenie, że w tego typu konflikcie informacja jest jednocześnie: 1) zasobem, 2) obiektem ataku i 3) bronią. Dla ekspertów podkreślających militarny wymiar walki informacyjnej szczególnie istotne są dwa pierwsze punkty. Uzyskanie przewagi informacyjnej nad przeciwnikiem zawsze było celem dowódców. Równie istotna była ingerencja w stan wiedzy przeciwnika, np. poprzez podsuwanie mu fałszywych danych. Rozwój technologii informatycznych i uzależnienie od nich funkcjonowania sił zbrojnych oraz infrastruktury krytycznej państwa tylko podniosło rangę tego rodzaju operacji.

O wiele szersze wnioski można wyciągnąć po zastanowieniu się, w jaki sposób informacja stała się bronią. Niektórzy analitycy, jak Dorothy Denning, znacznie rozszerzają zakres pojęciowy wojny informacyjnej i twierdzą, że obejmuje ona

> informacje w jakiejkolwiek postaci, transmitowane za pośrednictwem dowolnych mediów od ludzi i ich otoczenia fizycznego do drukarek, telefonów, radioodbiorników, telewizorów, komputerów i sieci komputerowych (Fryc, 2009, s. 61-62).

Opinia ta zwraca uwagę na znamienny fakt. Otóż uczestnikami walki informacyjnej są już nie tylko podmioty wojskowe i polityczne. Biorą w niej udział także cywile, którzy mogą być zarówno celem oddziaływania, jak i przekaźnikiem określonych treści (np. przez sieci społecznościowe).

Można postawić tezę, że rola wali informacyjnej wzrasta. Cechą słynnej ostatnio wojny hybrydowej jest to, że składają się na nią skomplikowane kampanie łączące operacje konwencjonalne o niskiej intensywności i operacje specjalne, działania ofensywne w cyberprzestrzeni oraz operacje psychologiczne wykorzystujące media społecznościowe i tradycyjne. Celem wojny hybrydowej jest zaś wywarcie wpływu na opinię publiczną, również na poziomie międzynarodowym (Liedel, 2015, s. 53).

Informacyjny komponent wojny hybrydowej jest trudny do przecenienia. Na przykład w przypadku aneksji Krymu przez Rosję działania kinetyczne nie miały być może pierwszorzędnego znaczenia. Ważniejsze było uzyskanie zamętu informacyjnego i utrudnienie adekwatnej odpowiedzi przeciwnikowi i społeczności międzynarodowej (np. poprzez skierowane do działań „zielonych ludzików" bez dystynkcji wojskowych). Tego rodzaju operacje rozpoczynają się i trwają, jeszcze zanim zaatakowany i jego otoczenie zauważą, że doszło do ataku. Dzięki skutecznym operacjom informacyjnym możliwa staje się do przeprowadzenia tzw. agresja podprogowa, czyli

> działanie wojenne, którego rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego (Biuro Bezpieczeństwa Narodowego, 2015a).

Podsumowując, istotą współczesnej wojny informacyjnej jest to, że informacja jest w niej jednocześnie zasobem, celem ataku i bronią. Walka informacyjna przestaje także być tylko dodatkowym, uzupełniającym komponentem starć zbrojnych. Sfera informacyjna staje się równorzędnym „polem" walki, a działania tego typu mogą decydować o zwycięstwie w konflikcie.

2. WYBRANE METODY WALKI INFORMACYJNEJ

Wśród metod walki informacyjnych wymienić można: operacje psychologiczne, propagandę, dezinformację, cyberatak społecznościowy, a także manipulację informacją.

2.1. Operacje psychologiczne

W projekcie *Doktryny bezpieczeństwa informacyjnego RP* z 2015 r. operacje psychologiczne definiuje się jako

> 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 (Biuro Bezpieczeństwa Narodowego, 2015b, s. 4).

Pierwszym w Polsce oficjalnym dokumentem, który definiował tego rodzaju operacje, był *Regulamin działań Wojsk Lądowych* z 2002 r. W publikacji tej podkreślono, że

> działania psychologiczne to planowe oddziaływanie psychologiczne w czasie pokoju, kryzysu i wojny, skierowane do wrogich, przyjaznych lub neutralnych odbiorców, wpływające na ich postawy i zachowania z zamiarem osiągnięcia pożądanych, z punktu widzenia prowadzącego je, celów politycznych i wojskowych (...) (Modrzejewski, 2015, s. 41).

Zdaniem ekspertów cele operacji psychologicznych można streścić w trzech punktach:

- osłabienie woli działania i agresywnych zamiarów przeciwnika lub potencjalnie przeciwnych obiektów oddziaływania;
- wzmocnienie zaangażowania i wsparcia ze strony przyjaznych obiektów oddziaływania;
- pozyskanie poparcia i współpracy ze strony środowisk niezaangażowanych lub niezdecydowanych (Modrzejewski, 2015).

W trakcie konfliktów zbrojnych działania psychologiczne prowadzone są zwykle przez wyspecjalizowane organa propagandowo-agitacyjne. Współcześnie ich skutki są dodatkowo wzmacniane przez powszechny dostęp do technologii komunikacyjnych i informatycznych. W wojnie psychologicznej wykorzystuje się różnorodne sprzeczności (religijne, narodowościowe, społeczne); inspiruje się ruchy zbrojne, chaos, panikę, sabotaż i dywersję w celu załamania stanu moralnego przeciwnika oraz pozbawienia go woli walki. Stosuje się także obietnice polepszenia warunków życia, swobód i przestrzegania praw człowieka. Organizuje się krytykę wrogiego obozu rządzącego, partii politycznych i ich liderów. Wspiera się

nawet nieprzyjazne im zorganizowane grupy przestępcze i organizacje terrorystyczne (Żebrowski, 2016).

Zgodnie z doktryną NATO wyróżnia się dwa rodzaje operacji psychologicznych:

- operacje psychologiczne zaczepne – mają na celu osłabienie woli walki przeciwnika i jego ludności. Po odnalezieniu słabego punktu w polityce przeciwnika rozpoczyna się skoncentrowany pod względem czasu, miejsca i sposobu atak na wybrany obiekt oddziaływania. Odbywa się to poprzez radio, telewizję, prasę (reportaże, artykuły), kampanię plakatową i ulotkową oraz – co dziś szczególnie ważne – Internet. Skuteczna operacja psychologiczna osłabia morale przeciwnika i wprowadza w jego szeregach wątpliwości co do słuszności realizowanej polityki, zdolności własnych wojsk, wartości zawartych sojuszy itp.
- operacje psychologiczne obronne – mają na celu wzmocnienie morale własnej ludności, a także pozyskanie wsparcia sił neutralnych i niezaangażowanych. Realizowane są poprzez osłabienie prestiżu przeciwnika, podważenie jego autorytetu, uprzedzanie i dyskredytowanie jego przekazu informacyjnego.

Dla przykładu rosyjskie operacje psychologiczne w trakcie konfliktu na Ukrainie, w ocenie fińskiego analityka, opierały się na trzech założeniach:

- dążenie do degradacji możliwości obronnych przeciwnika, podrywanie gotowości i zdolności bojowych jego sił, osłabianie zaufania do przywództwa politycznego i wojskowego, destabilizacja i obniżanie morale personelu sił zbrojnych, zwiększanie zamętu na tyłach przeciwnika;
- organizowanie kontrolowanego chaosu i kryzysu poprzez dyskredytację przywództwa politycznego, osłabianie autorytetu instytucji, inicjowanie niepokojów, paniki i zbrojnych starć wśród ludności;
- skrywanie własnych celów w konflikcie, a potem wojnie, w celu osłabienia krytyki wśród własnych obywateli oraz wykreowanie poczucia zagrożenia skierowanego w stosunku do Rosji (Mattson, 2015).

Ukraińscy analitycy z Narodowego Instytutu Studiów Strategicznych wskazują na następujące filary rosyjskich operacji psychologiczno-informacyjnych w konflikcie o Krym i Donbas:

- demoralizacja społeczeństwa Ukrainy;
- demoralizacja sił zbrojnych i struktur siłowych, a także zachęcanie ich do zdrady i ucieczki na drugą stronę konfliktu;
- promowanie wśród obywateli Rosji i Ukrainy „odwróconego" medialnego obrazu zdarzeń zamiast informowania o ich prawdziwych przyczynach i konsekwencjach;
- kreowanie iluzji masowego poparcia dla działań Federacji Rosyjskiej wśród mieszkańców południowo-wschodniej Ukrainy;
- udzielanie psychologicznego wsparcia zwolennikom radykalnego zbliżenia południowo-wschodnich regionów Ukrainy z Rosją (The National Institute for Strategic Studies, 2014).

2.2. Propaganda

W cytowanym już projekcie *Doktryny bezpieczeństwa informacyjnego RP* propagandę łączy się z dezinformacją oraz manipulacją i tłumaczy jako

> 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 (Biuro Bezpieczeństwa Narodowego, 2015b, s. 4).

Nie jest to ujęcie zbyt precyzyjne, gdyż propaganda i dezinformacja to w istocie różne metody oddziaływania informacyjnego, a manipulacja informacją jest jedną ze stosowanych w nich technik.

W potocznym odbiorze słowo „propaganda" kojarzy się z celowym przekazywaniem nieprawdziwych informacji. W tym kontekście mówi się np. o „propagandzie hitlerowskiej/goebbelsowskiej" czy „propagandzie komunistycznej". W poniższej tabeli ujęto kilka z bardzo wielu dostępnych definicji propagandy.

Tabela 1
Wybrane definicje propagandy

A. Pratkins, E. Aronson	„Zręczne posługiwanie się obrazami, sloganami i symbolami, odwołujące się do naszych uprzedzeń i emocji; jest komunikowaniem pewnego punktu widzenia, mającym na celu skłonienie odbiorcy do dobrowolnego przyjęcia tego punktu widzenia za swój".
B. Dobek-Ostrowska	„Technika wpływania na zachowania obywateli, kierowania opinią publiczną i manipulowania. Opiera się na najnowszych osiągnięciach naukowych i wynikach badań empirycznych w zakresie psychologii społecznej, socjologii, politologii, teorii komunikowania i innych naukach społecznych".
H. Kula	„Celowe upowszechnianie wiadomości, opinii, poglądów, teorii, wyjaśniających otaczającą rzeczywistość i zjawiska życia społecznego".
R. Brzeski	„Proces intencjonalnego rozpowszechniania poglądów i przekonań, specyficzny proces komunikowania się, w którym nadawca stara się manipulować odbiorcami drogą rozbudzania emocji oraz zwodniczą lub pokrętną argumentacją".
L. Fraser	„Sztuka skłaniania innych do działań odmiennych od zachowań, które poczyniliby bez propagandy".
Ł. Szurmiński	„Umotywowana politycznie, celowa i systematyczna próba kształtowania percepcji i ludzkich postaw, realizowana głównie za pomocą środków masowej komunikacji w celu zapewnienia sobie poparcia opinii publicznej dla podejmowanych działań".

Źródło: opracowanie własne na podstawie: Kacała, 2015, s. 53-54; Brzeski, 2014, s. 193-194; Szurmiński, 2016, s. 5.

Z powyższych cytatów wynika, iż to nie kryterium prawdziwości odgrywa najważniejszą rolę w definiowaniu propagandy. Tym, co zwraca szczególną uwagę w tej metodzie oddziaływania informacyjnego, jest jego forma – wyjątkowo zręczne posługiwanie się słowami i substytutami słów, takimi jak fotografie, rysunki, obrazy, nagrania wideo, a także pieśni, defilady, manifestacje, wiece i inne środki. Propaganda skierowana jest do odbiorcy masowego i wykorzystuje wiedzę naukową o tym, jak poprzez kreowane emocje wpływać na ludzkie zachowania. Oprócz funkcji informacyjnej (propagowanie idei, wyjaśnianie, instruktaż) zawiera zatem w sobie komunikowanie perswazyjne (wpływanie na zachowanie, wzmacnianie postaw, zmiana zachowań i postaw).

Istnieje wiele typologii propagandy. Ze względu na rodzaj źródła wymienia się propagandę „białą" (gdy nadawca jest znany), „szarą" (źródło przekazu może, ale nie musi być poprawnie identyfikowane, a podawane przez nie informacje nie są zbyt precyzyjne) oraz „czarną" (fałszywe źródło przekazu, ukrywające rzeczywistego nadawcę oraz sfabrykowane, nieprawdziwe informacje). Ze względu na kierunek oddziaływania wymienia się propagandę zewnętrzną oraz wewnętrzną. Wreszcie ze względu na zależność w czasie mówi się o propagandzie poprzedzającej, towarzyszącej oraz następczej.

Propaganda posługuje się ogromnym spektrum środków i wyrafinowanych metod. Zostały one omówione w bogatej literaturze przedmiotu (zob. Zwoliński, 2003).

Powstanie i rozwój Internetu otworzył nowy rozdział w historii propagandy. Trudno wymienić wszystkie „zalety" Sieci dla działań tego typu. Przede wszystkim należy zwrócić uwagę na to, jak silną – znacznie większą niż w przypadku radia czy telewizji – stymulację zapewnia „obcowanie" z Internetem. Dla propagandy, która odwołuje się do emocji i podświadomości, ma to kolosalne znaczenie. Co więcej, korzystanie ze źródeł internetowych nie sprzyja głębszej refleksji (mózg jest „roztrzepany", uwaga ciągle przeskakuje na coraz to nowy, bardziej frapujący *content*) – a więc także weryfikacji, refleksji i krytycznej interpretacji podawanych treści (Carr, 2010, *passim*).

Kolejną rewolucję przyniósł rozwój tzw. Sieci 2.0 (*Web 2.0*), w której dominuje interakcja i treści tworzone przez samych użytkowników. W tym kontekście mówi się już także o Propagandzie 2.0 (zob. Rieger, Frischlish i Bente, 2013). Jeszcze nigdy tak łatwe nie było zaangażowanie do walki informacyjnej szerokiej rzeszy własnych działaczy czy sympatyków. Każdy użytkownik Sieci może zamieszczać i udostępniać materiały propagandowe. Znikają ograniczenia geograficzne i czasowe, a decentralizacja i anonimowość nadawców utrudnia zlokalizowanie oraz ewentualne zneutralizowanie źródła propagandy. Internet daje wyjątkowe możliwości operowania tekstem, dźwiękiem i obrazem. Unikalnym w całym Internecie narzędziem jest serwis YouTube. Z powodzeniem zastępuje on, szczególnie wśród młodych ludzi (czyli tzw. *digital natives*), telewizję i radio, omijając jednocześnie ich największe ograniczenia i wady (Lakomy, 2013).

Nikogo już nie dziwi fakt, że do Internetu przenoszą się największe telewizje, w tym rządowe. Na przykład Russia Today stale

prowadzi swój serwis internetowy (w pięciu językach) oraz kanał na YouTube, gdzie dostępna jest nie tylko transmisja *live* i powtórki programów, ale także np. zapisy z wydarzeń z różnych części globu, których publikacja z jakichś powodów uznana została za korzystną z punktu widzenia rosyjskiej polityki informacyjnej. Russia Today dosłownie zasypuje Internet swoimi nagraniami. Są to najczęściej krótkie klipy, doskonale „skrojone" na potrzeby odbiorcy internetowego: nie nazbyt długie (od kilkudziesięciu sekund do kilku minut), przedstawiające emocjonalny przekaz oraz nierzadko sceny przemocy (np. zamieszki z udziałem imigrantów w krajach europejskich, gwałtowne demonstracje w Kijowie itp.). Są także pozbawione narracji lektora, tak aby uniknąć wrażenia, że odbiorcy narzuca się interpretację.

Strona ukraińska w nadciągającym i eskalującym potem konflikcie zaczynała z nieporównanie niższego poziomu organizacyjnego. Słabością ukraińskiej polityki informacyjnej od początku były: brak systemowego podejścia do polityki informacyjnej państwa, niedocenienie zagrożeń bezpieczeństwa informacyjnego, brak działań informacyjnych wzmacniających tożsamość wszystkich obywateli Ukrainy, oligarchizacja rynku medialnego, nieefektywność (a czasem zupełny brak) rządowej polityki informacyjnej (Dutsyk, 2015). Na arenie międzynarodowej niedostatki te w pewnym stopniu niwelowała powszechna sympatia do Ukrainy. Sami Ukraińcy także potrafili ominąć piętrzące się przeszkody, czego przykładem mogą być telewizje internetowe: Espresso TV i Hromadske TV – zorganizowane naprędce w okresie Majdanu, kiedy to kontrolowane przez ówczesne władze największe kanały emitowały opery mydlane. Dysponowały one prowizorycznym studiem oraz szeregiem kamer przesyłających transmisję z wielu miejsc Kijowa. Poza ważną funkcją informacyjną (każdą ze stacji w szczytowych momentach oglądało nawet 100 tys. osób) ugruntowywały one obraz Majdanu jako zrywu obywatelskiego.

Ukraińcy zastosowali także kilka znakomitych chwytów propagandowych. Dzięki prezentacji odpowiednich, odwołujących się do emocji i swego rodzaju romantyzmu treści, umocnili przekaz przedstawiający Majdan jako szeroki, bohaterski zryw przeciw nadużyciom władzy. W rzeczywistości Majdan nie byłby możliwy bez organizacyjnego wsparcia niektórych oligarchów (Hypki i Szulc,

2014), a w najważniejszych momentach kluczową rolę na kijowskim placu Niepodległości odgrywali nie romantyczni rewolucjoniści, tylko zorganizowane grupy neobanderowskie i neonazistowskie.

Po obaleniu Wiktora Janukowycza, kiedy to wielu zagranicznych obserwatorów zastanawiało się nad zasadnością siłowej zmiany władzy, genialnym posunięciem było pokazanie zdjęć z epatującej bogactwem i kiczem rezydencji byłego już ukraińskiego prezydenta. Nieważne okazało się, że część pokazywanych „eksponatów" z domu Janukowycza (np. zdjęcie klozetu w kształcie tronu faraona) okazało się potem fałszywkami. Przesunięcie opinii, szczególnie światowej, stało się faktem.

W sferze propagandy kulturalnej na zauważenie zasługuje znakomity wiersz Ukrainki Anastazji Dmitruk pt. *Nigdy nie będziemy braćmi*, do którego później piosenkarze z Litwy dołożyli równie udane wykonanie muzyczne. Emocjonalnym, oskarżycielskim i pogardliwym zwrotom w kierunku Rosjan (np. „nie ma w was ducha, by być wolnymi", „wszyscy od dziecka jesteście zakuci w łańcuchy", „wolność to słowo dla was nieznane", „udławcie się swoją zawiścią") odpowiada pochwała ostatnich zmian na Ukrainie („powstaliśmy i wszystko naprawiliśmy", „patrzcie, kryją się szczury", „u was car – u nas demokracja"). Paradoksalnie wielką zaletą tego utworu okazało się to, iż powstał w języku rosyjskim, dzięki czemu bez trudu – oczywiście przez YouTube – trafił do rosyjskich odbiorców, wśród których mógł burzyć wiarę w państwową narrację. Powstające w rosyjskim Internecie próby odpowiedzi na ukraińską piosenkę żenowały swoim prymitywizmem i tylko potęgowały pierwotny efekt.

2.3. Dezinformacja

W literaturze anglojęzycznej termin *disinformation* pojawił się po raz pierwszy w roku 1926 w opisie działań sowieckich służb specjalnych. Rok później ukazujące się w Rydze pismo „białych" Rosjan „Siegodnia" stwierdziło, że podsuwanie obcym służbom dezinformacji należy do głównych zadań Głównego Zarządu Politycznego (GPU). W tym kontekście uznać można, że mimo iż praktyka podsuwania przeciwnikowi sfabrykowanych informacji towarzyszyła polityce i wojnie od zawsze, to właśnie sowieckie służby wprowadziły termin

„dezinformacja" oraz opanowały tę metodę do perfekcji (Brzeski, 2014).

W słowie „dezinformacja" uwagę zwraca przedrostek „dez", który oznacza przeciwieństwo, odwrotność i brak akceptacji. Dezinformacja, po pierwsze, oznacza więc informację fałszywą, kłamliwą lub rzekomą, a wiec nieposiadającą tych cech typowej informacji, które podnoszą poziom wiedzy odbiorcy (Modrzejewski, 2015). Po drugie, dezinformacja jest określoną metodą działania. Praktykę dezinformacji *Wielka Encyklopedia Radziecka* tłumaczyła jako „rozpowszechnianie za pomocą prasy i radia wiadomości fałszywych, celem wprowadzenia w błąd opinii publicznej" (Brzeski, 2014, s. 104). Współczesny *Słownik języka polskiego* definiuje dezinformację jako „wprowadzenie kogoś w błąd poprzez podanie mylących bądź fałszywych informacji". Należy podkreślić, że dezinformacja jest zawsze działaniem celowym. Równie ważny jest fakt, iż dezinformator (w przeciwieństwie np. do propagandzisty) może formułować negatywny przekaz na swój temat (np. przekonywać o niskim potencjale własnych wojsk w celu ukrycia rzeczywistych zdolności).

Znawca sowieckiej dezinformacji i autor znanej w Polsce książki na ten temat, Vladimir Volkoff zauważa, że „dezinformacja jest prowadzona w sposób systematyczny, fachowy, zawsze za pośrednictwem *mass mediów* i jest adresowana do opinii publicznej, a nie sztabów krajów-obiektów działań" (Volkoff, 1991, s. 8). Celem prowadzenia dezinformacji jest wywołanie pożądanego zachowania u przeciwnika, stałe utrzymywanie go w niepewności, wprowadzanie w błąd co do faktycznych zamierzeń, planów kierownictwa politycznego i wojskowego oraz przedsięwzięć realizowanych w państwie i siłach zbrojnych. W sferze wojskowej dezinformacja pozwala na uzyskanie efektu zaskoczenia na polu walki (Żebrowski, 2016).

Ze względu na sferę oddziaływania wyróżnia się cztery rodzaje dezinformacji.

- Dezinformacja polityczna – prowadzona w sferze wewnętrznej i zewnętrznej przez centralne kierownictwo państwa. W wymiarze wewnętrznym obiektem jest własne społeczeństwo i służy kształtowaniu pożądanych postaw, opinii i zachowań współobywateli. Dezinformacja w polityce zagranicznej ma za zadanie tworzenie pozytywnego wizerunku własnego państwa na arenie międzynarodowej. W przypadku gdy prowadzona polityka

wywołuje krytykę i sprzeciw społeczności międzynarodowej, celem dezinformacji jest ukrycie swoich prawdziwych celów i intencji oraz dążenie do uzyskania akceptacji i wsparcia dla swojej działalności.

- Dezinformacja ekonomiczna – ma na celu wprowadzenie przeciwnika w błąd co do stanu rzeczywistych osiągnięć ekonomiczno-gospodarczych, dotyczących możliwości obronnych państwa.
- Dezinformacja naukowo-techniczna – ma na celu ukrycie przed ewentualnym przeciwnikiem faktycznego stanu osiągnięć, odkryć naukowych, zgromadzonych doświadczeń, zmian w teorii sztuki wojskowej, nowych modeli techniki i uzbrojenia, sposobów wykorzystania innowacji oraz perspektyw ich wdrożenia.
- Dezinformacja wojskowa – w której obiektem dezinformacji jest przeciwnik, wojska własne i otoczenie. Oddziaływanie na przeciwnika dotyczy zwykle przekazywania poprzez jego system rozpoznania fałszywych informacji. Istotą dezinformacji w stosunku do wojsk własnych jest spowodowanie takiego ich działania, aby umocniło przekonanie przeciwnika o słuszności wniosków wyciągniętych z rozpoznania. Dezinformacja wojskowa obejmuje więc przekazywanie fałszywych informacji, pogłosek, dokumentów oraz demonstrowanie działań wojsk, w których celem jest wprowadzenie w błąd przeciwnika odnośnie do prawdziwych zamierzeń, planów i przedsięwzięć o znaczeniu militarnym. W przypadku dezinformacji wojskowej wyróżnia się jeszcze działania ofensywne i defensywne. Pierwsze mają pozwolić na uzyskanie zaskoczenia i utrzymanie inicjatywy, drugie – na poprawę bezpieczeństwa działań i stworzenie warunków do ich skutecznej realizacji (Żebrowski, 2016; Modrzejewski, 2015).

Dezinformację prowadzi się na poziomie strategicznym i taktycznym. W przypadku dezinformacji wojskowej można jeszcze mówić o dezinformacji na poziomie operacyjnym. Dezinformację strategiczną prowadzą centralne organy kierownicze państwa. Jej celem jest wprowadzenie w błąd przeciwnika co do podstawowych kwestii jego polityki; wywołanie zamętu w ocenie fundamentalnych zamiarów i ambicji drugiej strony. Prowadzi się ją kanałami politycznymi, dyplomatycznymi, ekonomicznymi, naukowo-technicznymi,

wojskowymi, specjalnymi (wywiad i kontrwywiad cywilny i wojskowy), poprzez służby policyjne, służby do walki z narkotykami, służby do walki z terroryzmem, jednostki walki elektronicznej, jednostki rozpoznania wojskowego. W działaniach wykorzystuje się mniejszości narodowe, religijne i etniczne, organizacje nacjonalistyczne, a nawet organizacje terrorystyczne i przestępcze o charakterze międzynarodowym. Dezinformacja taktyczna obejmuje doraźne działania, których przykładami mogą być: opublikowanie sfabrykowanej notatki wewnętrznej polityka wyznaczonego do skompromitowania, podsunięcie nieprawdziwych danych technicznych uzbrojenia, „podkolorowanie" danych statystycznych celem wywołania wrażenia, że stan gospodarki państwa jest lepszy (albo gorszy) od rzeczywistego. Rozsiewane są pogłoski i plotki obliczone na uśpienie społeczeństwa przeciwnika lub jego zastraszenie, zdemoralizowanie oraz odebranie woli oporu (Brzeski, 2014; Żebrowski, 2016).

Współcześnie najszersze pole oddziaływania ma dezinformowanie poprzez środki masowego przekazu, polegające na wykorzystaniu oficjalnych publikacji w celu wprowadzenia przeciwnika w błąd, np. co do zamiaru użycia wojsk własnych i planowanych operacji. W literaturze przedmiotu wymienia się jeszcze dezinformowanie agenturalne (bezpośredni lub pośredni kontakt z wywiadem przeciwnika i przekazywanie mu tą drogą odpowiednich materiałów dezinformacyjnych), dezinformowanie radioelektroniczne (przekazywanie drogą radiową fałszywych komend, rozkazów, meldunków), dezinformowanie poprzez inspirację otoczenia (wprowadzanie w błąd rozpoznania przeciwnika poprzez wykorzystanie ludności/osób do rozpowszechniania fałszywych wiadomości) (Modrzejewski, 2014).

Aby dezinformacja była skuteczna, musi być realizowana według określonych zasad: 1) zasada celowości (dezinformacja musi mieć jasno sprecyzowany cel, który określa pożądany rezultat); 2) zasada przygotowania (gwarancja dostępności sił i środków niezbędnych do realizacji i wsparcia dezinformacji, łącznie z planem ich wykorzystania po zaistnieniu określonych skutków pośrednich); 3) zasada kompleksowości (stosowanie różnorodnych form, metod i sposobów, przy całościowym wykorzystaniu dostępnych sił i środków oraz kanałów transmisji dezinformacji); 4) zasada scentralizowanego kierowania (ścisłe rozgraniczenie zadań, koordynacja i współpraca między

zespołami, ograniczenie inicjatywy osobom wykonującym zadania na niższym szczeblu); 5) zasada wiarygodności (prowadzenie dezinformacji w taki sposób, aby miała znamiona informacji prawdziwej; nie może być nieadekwatna do sytuacji czy nielogiczna); 6) zasada dublowania (nieprawdziwe informacje muszą pochodzić z możliwie największej liczby źródeł, tak aby wzajemnie się uwiarygadniały); 7) zasada elastyczności (w przypadku wywołania niepożądanych efektów, albo tylko częściowego sukcesu, należy przerwać działania dezinformujące bez ujawniania ich pierwotnego celu oraz określić nowe zadania, a także zmienić w miarę możliwości ich wykonawców); 8) zasada terminowości (należy wydzielić przeciwnikowi wystarczająco dużo czasu na otrzymanie informacji, zrozumienie jej oraz reakcję, ale zbyt mało na jej gruntowną analizę i odkrycie oszustwa); 9) zasada ciągłości (wysyłanie fałszywych danych powinno przebiegać systematycznie, intensywność dezinformacji nie może narastać tuż przed rozpoczęciem aktywnych działań); 10) zasada spójności (zgodność celu dezinformacji z celem polityki zagranicznej państwa i działalnością sił zbrojnych oraz logiczny związek między formułowanymi przekazami); 11) zasada nieszablonowości (unikanie wcześniej użytych technik i zmiana sposobu ich stosowania); 12) zasada skrytości (utrzymanie swoich przedsięwzięć w tajemnicy przed przeciwnikiem, otoczeniem zewnętrznym oraz własnymi siłami, a nawet osobami wykonującymi konkretne zadania szczegółowe) (Modrzejewski, 2014; Żebrowski, 2016).

Modelowym przykładem dezinformacji polityczno-wojskowej było zachowanie rosyjskiego kierownictwa państwowego w okresie bezpośrednio poprzedzającym aneksję Krymu. Rosjanie do ostatnich dni ukrywali swoje prawdziwe zamiary i wysyłali sygnały mogące świadczyć o tym, że nie planują gwałtownej reakcji na wydarzenia rozgrywające się u sąsiada. Wykorzystano przy tym fakt, iż w tym okresie trwały zimowe igrzyska olimpijskie w Soczi, co ułatwiało np. prezydentowi Putinowi formułowanie nieraz wręcz pacyfistycznego przekazu.

Być może najbardziej charakterystyczną cechą konfliktu ukraińskiego, począwszy od Majdanu, poprzez aneksję Krymu, aż po wojnę w Donbasie, było publikowanie w mediach elektronicznych ogromnej ilości fałszywych informacji, tzw. fake'ów (*fake* – ang. fałszywka). Była to dezinformacja na najniższym poziomie, szczególnie rozlegle

stosowana w mediach internetowych. Jej zadaniem było oddziaływanie na opinię publiczną w celu zmiany panujących w społeczeństwie nastrojów.

2.4. Manipulacja informacją

Mniejszą pod względem skali od dotąd omówionych formą oddziaływania informacyjnego jest manipulacja. Jest ona zwykle nieodłączną częścią propagandy i dezinformacji, jednak techniki manipulowania informacją z pewnością zasługują na osobne omówienie.

A. Lepa pisze, iż „manipulacja to celowe i skryte działanie, przez które narzuca się jednostce lub grupie ludzi fałszywy obraz pewnej rzeczywistości". „Składnikiem elementarnym manipulacji jest informacja" – dodaje ten sam autor (Lepa, 1997, s. 23). W opracowaniu BBN przez manipulację rozumie się „wykorzystanie prawdziwych informacji, ale w taki sposób, aby wywołać fałszywe implikacje, np. drogą pomijania niektórych, istotnych, ale niewygodnych informacji, żeby budziły fałszywe skojarzenia" (Biuro Bezpieczeństwa Narodowego, 2015b, s. 4).

Spektrum możliwych sposobów manipulacji jest znacznie szersze. Niektóre z nich przedstawia tabela 2.

Tabela 2
Wybrane metody manipulacji informacją

Sposoby manipulowania	Charakterystyka sposobów manipulowania
Przekazywanie danych nieprawdziwych	Podanie przedmiotowi oddziaływania danych z gruntu nieprawdziwych, jednak takich, które powinny utkwić w podświadomości jako możliwe.
Preparowanie i przesyłanie do przedmiotu danych nieważnych lub mało ważnych z pominięciem najważniejszych	Przekazanie danych na zasadzie przedstawienia rzeczywistego obrazu w tzw. krzywym zwierciadle.
Przekazywanie danych o dużym znaczeniu jako marginalnych	Każda postać danej, nawet bardzo istotna, przekazana w dalszej kolejności komunikatu informacyjnego staje się mniej ważną, nieznaczącą wiadomością, na którą przedmiot nie zwraca uwagi.

Udostępnianie danych preparowanych w celu wywołania określonych interwencji	Może być sprowadzony do wywoływania tzw. tematów dyżurnych. Permanentne przekazywanie danych może stanowić swoisty impuls do podjęcia działań interwencyjnych, dociekania prawdy, ucieczki z pola walki i innych tego typu zachowań.
Przesyłanie danych wieloznacznych, utrudniających zrozumienie	Może doprowadzić u ich odbiorcy do wytwarzania mylnego obrazu tego, co ważne z punktu widzenia prowadzonych działań.
Generowanie nadmiaru danych, by spowodować tzw. chaos informacyjny	To przekazywanie danych w nadmiarze, które prowadzi do chaosu informacyjnego. Można zasypać przedmiot oddziaływania tak dużą ilością danych o faktach i zjawiskach, że spowoduje to u niego brak wrażliwości na istotne i ważne wiadomości.

Źródło: Żebrowski, 2016, s. 459.

2.5. Cyberataki społecznościowe

Gwałtowny rozwój technologii internetowych stworzył nowe możliwości komunikacji i samoorganizacji międzyludzkiej. Ogromną rolę w ostatnich latach odgrywają tzw. media społecznościowe, które są także wykorzystywane w walce informacyjnej. W literaturze przedmiotu pojawiło się pojęcie społecznościowego cyberataku (ang. *social cyber attack*), definiowanego jako działanie anonimowe lub pod fałszywym pretekstem, polegające na wysyłaniu do mediów społecznościowych zmanipulowanego przekazu, albo też manipulację istniejącego przekazu, w celu uzyskania pożądanego efektu: chaosu, paniki, masowych zamieszek (Lange-Ionotamishvili i Svetoka, 2015).

Mechanizm cyberataku społecznościowego doskonale oddaje zjawisko tzw. trollowania (ang. *trolling*). Według opracowania BBN jest to

> 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 (Biuro Bezpieczeństwa Narodowego, 2015b, s. 4).

Modus operandi internetowego trolla najlepiej rozpoznali sami internauci w działającej na zasadzie serwisu społecznościowego *Wikipedii*. Wśród znaków rozpoznawczych trolla wymienia się: bezgraniczne podporządkowanie się jakiejś idei, udawaną nieznajomość tematu, częste zadawanie tych samych pytań, celowe wyrażanie zdania różnego od grupy, chętne używanie argumentów *ad personam*, skrajną megalomanię i pogardliwy stosunek do innych osób, częste nazywanie innych dyskutantów trollami, wprowadzanie zamieszania w stosunku do własnej osoby, przedstawianie siebie jako ofiary, próby utrudniania innym wypowiedzi, rozpoczynanie wypowiedzi ciągle od tego samego zwrotu (np. pogardliwego powitania), zmienianie własnych danych, tworzenie multikont, aby udawać poparcie dla siebie w dyskusji (Wikipedia, 2016).

Te z pozoru błahe sposoby zaistnienia dla internetowych frustratów mogą się stać bardzo groźne, jeśli: 1) przybierają formę zorganizowaną, 2) dokonują się w czasie sytuacji kryzysowej, 3) zawierają założony przekaz ideologiczny.

Po pierwsze, trolle utrudniają wówczas prowadzenie pracy niezależnym serwisom informacyjnym poprzez zalew krytycznych wpisów na wszystkich możliwych stronach i kontach (komentarze pod artykułem, forum, strona na Facebooku, Twitter). Po drugie, zalewem wpisów trolle starają się zniekształcić wydźwięk podawanej przez serwis informacji lub całkowicie zneutralizować jej wymowę. Często trolle formułują jednocześnie własny przekaz polityczny.

Problem trollowania w kontekście rosyjskim został omówiony w obszernym, specjalnym raporcie opublikowanym przez NATO Strategic Communications Centre of Excellence. Autorzy tego opracowania rozróżniają dwa rodzaje trolli:

- troll klasyczny – osoba próbująca sprowokować emocjonalną reakcję czytelnika, wywołać szok, doprowadzić do wściekłości, wywołać strach lub poczucie zagrożenia. Także osoba próbująca przyciągnąć do siebie uwagę poprzez sabotowanie zasad korzystania z serwisu (np. mnożenie wątków na forach albo wklejanie wbrew regulaminowi ogromnych partii skopiowanego tekstu). Troll klasyczny nie jest związany żadną ideologią

czy wierzeniem ani też przejęty prawdą czy fałszywością rozpowszechnianych informacji. Wprowadzana przez niego treść ma jeden główny cel – prowokować i wywoływać u innych gwałtowne, emocjonalne reakcje.

- troll hybrydowy – osoba wynajęta, działająca pod kierunkiem i na rozkaz państwa bądź instytucji państwowej, propagująca konkretną ideologię. Troll hybrydowy poza sprowokowaniem emocjonalnej reakcji zawsze ma jakiś cel dodatkowy, np. dezinformację, rozpowszechnianie „teorii spiskowych", kontrowersji itd. (NATO StratCom Centre of Excellence, 2016).

Ogólne metody działania obu typów internetowych trolli są podobne, różnią ich tylko intencje. Szczegółowe badania nad internetowymi trollami działającymi na Łotwie pozwoliły ekspertom NATO na wyróżnienie kilku ich typów, ze względu na formę przekazu i sposób argumentacji:

- troll typu „obwiń o wszystko amerykański spisek" – rozpowszechnia twierdzenia, że wszystko jest winą Stanów Zjednoczonych. Teksty „spiskowego" trolla są bardzo rozbudowane, zawierają długi „logiczny" wywód z szeroką argumentacją. Po bliższym zapoznaniu okazuje się jednak, że jest to pozorna logika, a wynik wywodu jest zawsze ten sam – winne są Stany Zjednoczone. Znakiem rozpoznawczym tego typu trolla jest objętość wpisów – są znacznie dłuższe niż w innych przypadkach;
- troll typu „bikini" – swoją nazwę wziął od zdjęcia profilowego lub avataru, w którym bardzo często pojawia się atrakcyjna kobieta ubrana w strój plażowy. W jego przekazie dominuje uproszczona wizja świata i naiwność. Wpisuje na przykład niewinnie brzmiące pytania: „Czy naprawdę tylko Rosja jest taka zła? Świat chyba nie jest taki prosty. Może powinniśmy spojrzeć na to co robią USA?". Trolle typu bikini wykazują według ekspertów wyjątkowe zdolności adaptacyjne w Internecie i są trudne do rozpoznania. Mimo niewielkiej objętości, naiwności i banalności ich wpisy wywierają ogromny wpływ na społeczność internetową;
- troll agresywny – to typ najbardziej zbliżony do klasycznego trolla, publikuje tylko agresywne i ekspresyjne wpisy i łatwo rozpoznać stanowisko, którego broni. Często straszy swoich czytelników i chce wywołać emocjonalną reakcję. W odróżnieniu od

trolla klasycznego, który żywo reaguje na polemikę, chcąc jak najbardziej przedłużyć konflikt i sprowokować szerszą grupę do reakcji, hybrydowy troll typu agresywnego cechuje się niską reaktywnością. Wynikać to może z bariery językowej i obawy przed dekonspiracją;

- troll „wikipedyjny" – to specyficzny rodzaj trolla, który przekopiowuje informacje z Wikipedii (lub innych źródeł, takich jak np. blogi historyczne), nie dodając do nich żadnych emocjonalnych komentarzy. Przeklejane informacje są zasadniczo prawdziwe, ale wyrwane z kontekstu i prowadzące do błędnych wniosków. W praktyce polega to na tym, że np. pod artykułami o wojskowej agresji Rosji przekopiowywane są ze źródeł otwartych fragmenty tekstów o interwencjach wojskowych USA – ale bez wskazania przyczyn, kontekstu, polityki innych państw w tym samym okresie itd.;
- troll „załącznikowy" – wiadomości tego typu trolli są wyjątkowo zwięzłe, ale zawsze zawierają załączony link, za którym podąża zachęcony czytelnik. W konsekwencji trafia się na np. rosyjski serwis informacyjny, nagranie z YouTube zawierające fragment programu informacyjnego lub amatorsko wyprodukowany klip propagandowy. Należy podkreślić, że hybrydowy troll nigdy nie przekierowuje do płatnych serwisów czy stron zawierających wirusy. Jego misją jest „edukacja" innych internautów. Tego rodzaj troll jest trudny do zidentyfikowania, ponieważ jego wpisy pozbawione są specyficznego stylu (NATO StratCom Centre of Excellence, 2016).

Instrukcję, jak rozpoznać i neutralizować hybrydowego trolla, zawiera tabela 3.

Tabela 3
Sposoby rozpoznania i neutralizacji hybrydowego trolla

Etap	Działanie
Krok pierwszy Rozpoznaj hybrydowego trolla	• komentarz jest zbyt długi (więcej niż 4 linijki), • komentarz nie pasuje do kontekstu, • komentujący został rozpoznany jako troll przez innych komentujących, • komentujący jest otwarcie agresywny i wrogi, • komentujący jest półanalfabetą, • jeśli odkryłeś jednego trolla hybrydowego, rozejrzyj się za innymi – zazwyczaj publikują posty w grupie (albo też jeden troll używa kilku tożsamości), Notabene: nawet jeśli wszystkie te czynniki są obecne, to nie przesądza to ostatecznie, że komentujący jest trollem hybrydowym.
Krok drugi Sprawdź hybrydowego trolla	• zadaj mu pytanie – klasyczny troll zazwyczaj odpowiada, odpowiedź od trolla hybrydowego jest mniej prawdopodobna z powodu bariery językowej, • „Wygugluj" go: • ten sam komentarz z różnych profil, • takie same komentarze, częste powtórzenia, (takie same komentarze zamieszczane pod artykułami na różne tematy, przez dłuższy czas, nawet przez rok).
Krok trzeci Oznacz hybrydowego trolla	• oznacz trolla poprzez komentarz dla uświadomienia bardziej podatnych użytkowników Internetu, • po oznaczeniu trolla przejdź do kroku 4.
Krok czwarty Zignoruj!	Jest bardzo ważne, aby ignorować trolla internetowego i nie wchodzić z nim w dalszą interakcję. Z kilku powodów: • kolejni użytkownicy zainteresują się nim, stanie się bardziej wiarygodny w oczach mniej doświadczonych internautów, • im więcej odpowiedzi troll otrzyma, tym więcej „kliknięć" dostanie w przyszłości (efekt śnieżnej kuli). Nawet negatywne reakcje mogą służyć zamysłom trolla, • każda reakcja może służyć prowokacji w przyszłości.

Źródło: NATO StratCom Centre of Excellence, 2016, s. 77.

KONKLUZJA

Podjęty w artykule problem badawczy dotyczył odpowiedzi na pytanie o rolę, jaką we współczesnych konfliktach politycznych odgrywają zmagania w sferze informacyjnej. Deskrypcja najczęściej spotykanych współcześnie metod walki informacyjnej pozwala stwierdzić, że rola ta wzrasta i może mieć decydujące znaczenie w czasie kryzysu, konfliktu czy wojny. Wytworzone metody i posiadane środki techniczne pozwalają na wywieranie szerokiego wpływu społecznego za pomocą różnorodnych kanałów komunikacji. Jednocześnie metody walki informacyjnej ulegają stałej ewolucji i udoskonaleniom, co wynika głównie z rozwoju technologicznego. Podmioty realizujące zadania w tej sferze tworzą też nowe rozwiązania, aby unikać szablonowości i powtarzania wcześniej zastosowanych działań. Przykładami nowych form oddziaływania informacyjnego są: propaganda 2.0 oraz cyberataki społecznościowe.

Powyższe wnioski potwierdza analiza konfliktu rosyjsko-ukraińskiego z lat 2014-2016. Operacje informacyjne miały kluczowe znaczenie dla jego przebiegu i dotychczasowych wyników. Były istotnym komponentem tzw. wojny hybrydowej i pozwoliły stronie atakującej osiągnąć określone cele bez widocznego przekraczania tzw. progu agresji.

Doświadczenia te wskazują, iż wrogie działania informacyjne stanowią coraz większe zagrożenie i wymagają szczególnej uwagi podmiotów odpowiedzialnych za bezpieczeństwo narodowe. Konieczne jest opracowanie nowych dokumentów doktrynalnych zawierających nowy katalog zagrożeń i terminologię adekwatną do współczesnych uwarunkowań bezpieczeństwa, a także refleksja nad skutecznymi metodami przeciwdziałania atakom informacyjnym. Czynnikiem niezwykle istotnym jest rozpowszechnienie w szerokich kręgach społecznych wiedzy na ten temat. Poruszona problematyka powinna też zainteresować środowisko akademickie i eksperckie. Być może podjęta w niniejszym artykule prezentacja zagrożeń informacyjnych będzie mogła zostać wykorzystana w działaniach szkoleniowych i edukacyjnych oraz wskaże kierunki dalszych dociekań, co stanowiłoby walor aplikacyjny prezentowanego tekstu.

Bibliografia

Balcerowicz, B. (2013). *O Pokoju. O Wojnie. Między esejem a traktatem*. Warszawa: Wydawnictwo Rambler.

Biuro Bezpieczeństwa Narodowego. (2015a). *(Mini)słownik BBN: propozycje nowych terminów z dziedziny bezpieczeństwa*. Pozyskano z: https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html

Biuro Bezpieczeństwa Narodowego. (2015b). *Doktryna bezpieczeństwa informacyjnego (projekt)*. Pozyskano z: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf

Brzeski, R. (2014). *Wojna informacyjna – wojna nowej generacji*, Komorów: Wydawnictwo Antyk Marcin Dybowski.

Carr, N. (2013). *Płytki umysł. Jak Internet wpływa na nasz mózg.* Gliwice: Wydawnictwo Helion.

Dutsyk, D. (2015). Ukraine's Information Policy During War: Critical Comments. W: *Counteraction to Russian Information Aggression: Joint Action to Protect Democracy*. Kyiv: NGO Telekritika, 6-12.

Fryc, M. (2009). *Wojna – współczesne oblicze.* Toruń: Wydawnictwo MADO.

Hypki, T. i Szulc T. (2014). *Przewrót na Ukrainie*. Pozyskano z: http://www.altair.com.pl/magazines/article?article_id=5149

Kacała, T. (2015). Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa. *Przegląd Prawa Konstytucyjnego*, *2*(24), 49-65. DOI 10.15804/ppk.2015.02.03

Lakomy, M. (2013). *Demokracja 2.0., Interakcja polityczna w nowych mediach*. Kraków: Wydawnictwo WAM.

Lange-Ionotamishvili, E. i Svetoka, S. (2015). Strategic Communications and Social Media in the Russia-Ukraine Conflict. W: K. Geers (red.), *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 103-111.

Lepa, A. (1997), Świat manipulacji. Częstochowa: Tygodnik Katolicki Niedziela.

Liedel, K. (2015). Zagrożenie hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP? *Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne – Wojna hybrydowa*, 51-58.

Liedel, K., Piasecka, P. i Aleksandrowicz, T.R. (2012). *Analiza informacji. Teoria i praktyka*. Warszawa: Wydawnictwo Difin.

Mattson, P.A. (2015). *Modern Russian Psychological Operations (PSYOPS)*. Pozyskano z: https://www.doria.fi/bitstream/handle/10024/117652/MATTSSON%20Peter_WG10_Abstract_Modern%20Russian%20Psychological%20Operations%20(PSYOPS).pdf?sequence=2

Ministerstvo Oborony Rossijskoj Federacii. (2012). *Konceptual'nye vzglâdy na deâtel'nost' Vooružennyh Sil Rossijskoj Federacii v informacionnom prostranstve*. Pozyskano z: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

Modrzejewski, Z. (2014). *Operacje informacyjne*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Munkler, H. (2004). *Wojny naszych czasów.* Kraków: Wydawnictwo WAM.

NATO StratCom Centre of Excellence. (2016). *Internet trolling as a tool of hybrid warfare: the case of Latvia.* Riga: StratCom.

Nissen, T.E. (2015). *The Weaponization Of Social Media. Characteristics of Contemporary Conflicts*. Copenhagen: Royal Danish Defence College.

Rieger, D., Frischlish, L. i Bente, G. (2013). *Propaganda 2.0 – Psychological Effects of Right-Wing and Islamistic Extremist Internet Videos*. Köln: Wolters Kluwer.

Szurmiński, Ł. (2016). *Pojęcie propagandy*. Pozyskano z: http://www.id.uw.edu.pl/~lukasz.szurm/Anatomia%20propagandy/2.%20Poj%C4%99cie%20propagandy.pdf

The National Institute for Strategic Studies. (2014). *Regarding the information-psychological component of aggression of Russian Federation against Ukraine (according to the results of events during 1-2 March 2014)*. Pozyskano z: http://en.niss.gov.ua/public/File/englishpublic/Russia_aggression.pdf

Volkoff, V. (1991). *Dezinformacja – oręż wojny*. Warszawa: Wydawnictwo Delikon.

Wikipedia. (2016). *Trollowanie*. Pozyskano z: https://pl.wikipedia.org/wiki/Trollowanie

Zwoliński, A. (2003). *Słowo w relacjach społecznych*. Pozyskano z: http://www.opoka.org.pl/biblioteka/I/IK/zwolinski-slowo-00.html

Żebrowski, A. (2016). *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*. Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.