FOLIA 384

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 13(2) 2023

ISSN 2657-8549

DOI 10.24917/26578549.13.2.11

ARTYKUŁY

Natalia Borodziuk
Prywatne Akademickie Centrum Kształcenia w Krakowie
ORCID 0009-0007-8278-9875

Walka informacyjna – wpływ agentury i przykłady metod przeciwdziałań jako strategia budowania odporności społecznej

Information warfare – the influence of agencies and examples of countermeasures as a strategy for building social resilience

Abstrakt

Sposób prowadzenia wojen, wraz z rozwojem technologii oraz środowiska bezpieczeństwa, będzie poddawany nieuchronnym zmianom. W przyszłych konfliktach militarnych i niemilitarnych istotnego znaczenia nabierać będzie powszechna informacja, która obecnie wykorzystywana jest zarówno jako rodzaj broni, jak i narzędzie do wymierzania ataków. Informacja staje się głównym elementem działań w zakresie walki informacyjnej, która prowadzona jest przez jednostki służb specjalnych. W ciągu ostatnich lat obserwuje się nie tylko szeroki rozwój sposobów walki informacyjnej, ale także rozwiązania mające na celu zapewnienie bezpieczeństwa własnego państwa przed takim rodzajem broni. W pracy ujęta została istotność informacji, a także problem eskalacji walki informacyjnej. Publikacja przedstawia także działania agencji w walce informacyjnej.

Słowa kluczowe: służby specjalne, dominacja informacyjna, walka informacyjna, agentura, agentura wpływu

Abstract

Developments in technology and the security environment are changing warfare. In the present and in the future, information will become increasingly important. Information is used as a weapon, but also as the purpose for attack. Information is one of the most important elements of the information warfare that the secret services conduct. The purpose of this article is to present the role of information in the modern world, but also to present and characterise information warfare and solutions to this phenomenon, which become a defence against this type of conflict. The article covers the relevance of the information and the problem of the escalation

of the information battle. The publication also presents the participation of agent activities in the course of the ongoing information struggle.

Keywords: Secret Service, information dominance, information warfare, agent, security

Poznanie innych i poznanie siebie to zwycięstwo bez ryzyka.
Poznanie otoczenia i poznanie sytuacji to zwycięstwo całkowite.
Sun Tzu, *Sztuka Wojny*

Wstęp

W wyniku postępującej globalizacji oraz rozwoju technologicznego zwiększa się znaczenie posiadania i ochrony informacji. Posiadanie szerokiej gamy wiadomości staje się kluczowym czynnikiem wpływającym na przewagę konkurencyjną. Jednocześnie rośnie również istotność szeroko zakrojonych działań dezinformacyjnych, manipulacyjnych oraz operacji mających na celu kradzież danych. Te działania są przede wszystkim prowadzone przez służby specjalne i stanowią formę obrony zasobów informacyjnych państwa oraz utrzymania ogólnego bezpieczeństwa. Niemniej jednak zauważalne jest, że walka informacyjna staje się nie tylko środkiem obronnym, lecz także współczesną bronią, której narzędzia mogą prowadzić do wewnętrznego destabilizowania państwa. W tym kontekście informacja staje się strategicznym narzędziem, będąc celem ataków oraz kluczowym czynnikiem wpływającym na przebieg procesu decyzyjnego. Uzyskanie dominacji informacyjnej wymaga podejmowania zarówno działań ofensywnych, jak i defensywnych, przy wykorzystaniu nowoczesnych możliwości technologicznych, które umożliwiają prowadzenie walki informacyjnej w szerokim spektrum działań[1]. Wojna informacyjna wykorzystuje przede wszystkim propagandę, manipulację, dezinformację, zakłócanie informacyjne, działania psychologiczne. Prowadzenie takiego rodzaju działań należy do zadań służb specjalnych (jak już zostało wspomniane), a przede wszystkim realizowane jest to przez agentów i agenturę wpływu. Działania te są szczególną działalnością, która pozwalają także na rozpoznanie przeciwnika, jak również jego strategii i interesów.

W pracy zostały podjęte istotne zagadnienia dotyczące roli informacji we współczesnym świecie, gdzie omówione zostało znaczenie informacji oraz zjawisko walki informacyjnej, wsparte przykładami ilustrującymi różnorodne aspekty tego zjawiska. Ponadto, szczególną uwagę poświęcono problemowi prowadzenia agentury wpływu, dokonując analizy i porównania różnych źródeł, co pozwoliło na przedstawienie propozycji najlepszych rozwiązań w zakresie zwalczania walki informacyjnej.

W publikacji podjęto próby odpowiedzi na szczegółowe pytania badawcze: Czym jest wojna informacyjna? Czym charakteryzuje się wojna informacyjna? Jaką rolę nabiera informacja? Co staje się źródłem walki informacyjnej? Jakie są przewidywane

[1] D. Kaźmierczak (2017). *Walka informacyjna we współczesnym świecie i jej społecznych konsekwencje*. „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili", 7, 112.

rozwiązania mające na celu przeciwdziałanie wojnie informacyjnej? Został postawiony również problem główny, mianowicie: Jaki jest wpływ agentury na walkę informacyjną i jakie są konsekwencje tych działań?

Celem niniejszego artykułu jest przedstawienie roli informacji we współczesnym świecie, ale także przedstawienie obrazu prowadzenia walki informacyjnej i rozwiązań wobec tego zjawiska, które stają się obroną przed takim rodzajem konfliktu. Metoda wykorzystana w pracy to analiza i porównanie wykorzystanych źródeł co pozwoliło przedstawić wpływ agentury wpływu na zjawisko walki informacyjnej oraz sposoby reagowania na ten problem w celu budowania poprawnej i bezpiecznej odporności społecznej.

1. Znaczenie informacji we współczesnym świecie

Początek rozwoju informacji można wyznaczyć na czas odnalezienia alfabetu greckiego w 700 roku p.n.e. To ważne odkrycie pozwoliło na połączenie mowy z językiem. Wynalazek ten stał się istotny także ze względu na wcześniejsze sposoby przekazywania komunikatów, które odbywały się za pomocą prostych odruchów, czyli za pomocą środków właściwych istocie ludzkiej[2]. Ważny był także ze względu na zasięg przekazywania informacji. Istotnym instrumentem służącym do przechowania i utrwalenia istotnych wiadomości była pamięć ludzka[3]. Do upowszechnienia dostępu do informacji przyczyniły się wynalezienie i rozwój druku. Zaś poprzez rozbudowę dróg łatwiej było przekazywać nowiny (choćby za pomocą poczty lub poczty kupieckiej). W późniejszym czasie pojawiły się inne środki przekazywania informacji, takie jak prasa czy kolej, telegraf, radio etc. Dzięki temu przekaz przekroczył bariery odległościowe i powstała możliwość przekazywania danych na wysoką skalę[4]. Kolejnym ważnym krokiem w upowszechnieniu przekazywania informacji jest wynalezienie Internetu oraz współczesne przemiany techniczne i technologiczne. Zmiany te pozwoliły na rozwój interaktywnej sieci[5].

Kolejnym ważnym elementem w postrzeganiu znaczenia informacji są istniejące uwarunkowania bezpieczeństwa informacyjnego. Bezpieczeństwo informacyjne staje się jednym z najważniejszych przedmiotów bezpieczeństwa w ostatnich latach. Należy je zdefiniować jako przede wszystkim: „wszelkiego rodzaju wysiłki, służące ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnienie przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub

[2] W. Krztoń (2017). W*alka informacyjna w cyberprzestrzeni w XXI wieku.* Rambler Press. Warszawa, s.14.

[3] *Ibidem*, s. 14.

[4] *Ibidem*, s.15.

[5] *Ibidem*.

innych podmiotów)"[6]. Bezpieczeństwo to obejmuje nie tylko zakres pojęcia informacji, ale również dotyczy systemów bezpieczeństwa. Dotyczy ono także wszelkiego rodzaju sposobów przechowywania, przetwarzania, analizowania zasobów informacji, co należy rozumieć jako zasadę poufności, integralności oraz dostępności informacji[7]. W otaczającym i ciągle rozwijającym się technologicznie środowisku bezpieczeństwa należy wyróżnić zagrożenia wobec bezpieczeństwa informacyjnego. Mianowicie są to kryteria takie jak:

- zagrożenia losowe (np. pożary obiektów przechowujących informacje),
- tradycyjne zagrożenia (np. szpiegostwo),
- zagrożenia technologiczne (np. cyberterroryzm),
- zagrożenia dotyczące praw społecznych i obywatelskich (np. sprzedaż informacji podmiotom nieuprawnionym)[8].

Należy również wymienić źródła pochodzenia zagrożeń i są to:

- wewnętrzne,
- zewnętrzne,
- fizyczne (dotyczące wypadku, awarii, katastrofy i w związku z tym utracenia informacji)[9].

Ważnym czynnikiem stanowiącym zagrożenie wobec bezpieczeństwa informacji jest działalność człowieka. Celem takich działań jest włamanie do systemu informacyjnego oraz dostęp do dysku komputerowego czy też sieci. Osoby tego dokonujące posługują się takimi sposobami działania jak na przykład:

- celowe inicjowanie awarii,
- podsłuch,
- szantaż,
- złamanie hasła dostępu,
- wirusy,
- bomby logiczne,
- groźne aplikacje systemowe[10].

Bardzo ważnym i potrzebnym działaniem w celu zachowania bezpieczeństwa informacji jest monitorowanie, identyfikacja realnych oraz potencjalnych zagrożeń. W szczególności dotyczy to sytuacji, w której zasoby danych mogą zostać wykorzystane w celu zachwiania bezpieczeństwa informacyjnego[11].

Poruszając kwestie informacji oraz znaczenia jej we współczesnym świecie, należy podać jej definicję. Pojęcie informacji jest trudne do zdefiniowania. Według słownika języka polskiego PWN „informacja to wyjaśnienie, zawiadomienie. Posiada elementarny

---

[6] A. Polończyk (2017). *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa*. W H. Batorowska E.Musiał (red.), *Bezpieczeństwo informacyjne w dyskursie naukowym*. Wydawnictwo Uniwersytetu Pedagogicznego. Kraków, s. 79–80.

[7] *Ibidem*, s. 81.

[8] *Ibidem*, s. 82.

[9] *Ibidem*.

[10] *Ibidem*, s. 83.

[11] *Ibidem*.

charakter i rozpatrywana jest w trzech aspektach, tj. syntaktycznym (dotyczy ilości informacji, jaka może być potencjalnie zawarta w danej wiadomości), semantycznym (znaczenia i zawartości treściowej wiadomości) i pragmatycznym (przydatności informacji, tj. wartości informacji zawartej w wiadomości ze względu na realizowany przez odbiorcę cel). W sensie syntaktycznym definiuje się informację albo poprzez ilość (miarę) informacji I (informacji teoria), albo jako synonim pojęcia dana (dane)"[12]. Warto także zaznaczyć, że użyteczna informacja posiada pewne cechy i są nimi: dokładność, aktualność, kompletność, odpowiedniość[13].

Potrzeba informacji pozwala na spełnienie funkcji wewnętrznych oraz zewnętrznych państwa. Posiadanie, pozyskiwanie odpowiednich danych umożliwia także wrogie działania nakierowane na przeciwnika[14]. To właśnie informacja staję się przedmiotem toczących się walk pomiędzy decydentami dysponującymi sprawnym aparatem informacyjno-zasilającym. W związku z tym prowadzi się działania ofensywne i defensywne, którymi są m.in.: propaganda, zdrada[15]. Ważne jest również to, że podczas trwającego konfliktu zbrojnego i niezbrojonego informacja nabiera szczególnego i priorytetowego znaczenia. To posiadanie szerokiej informacji oraz sprawne nią zarządzanie decyduje o przebiegu poruszania się uczestników w dynamicznym środowisku bezpieczeństwa. Wykorzystanie takich zasobów decyduje również o dostosowaniu się do sytuacji i działań (także tych przyszłych), czego pokłosiem jest osiągnięcie sukcesu w stosunku do zagrożeń, ale także wypracowanie szansy na rozwój skutecznych działań[16].

Informacja to również najważniejszy czynnik składający się na pożądaną egzystencję i gwarancję spokoju człowieka. Dotyczy to choćby dostępu do informacji o miejscu uzyskania pożywienia. Aby uniknąć niebezpieczeństw, ważne jest, aby dostarczyć odpowiednim decydentom informację o istniejącym zagrożeniu (potencjalnym czy też realnym). Ta kwestia nie byłaby możliwa bez powszechnej wymiany danych[17].

2. Walka informacyjna – wybrane aspekty

Walka informacyjna – definicja, istota zjawiska

Zjawisko globalizacji oraz rozwój i postęp technologiczny przyniósł nie tylko pozytywne efekty, takie jak na przykład szerokie zaspokajanie potrzeb, dostarczanie usług czy wsparcie działań ludzkich poprzez Internet, ale również niebezpieczeństwa. Takimi zagrożeniami za pomocą techniki informacyjnej są: cyberterroryzm, cyberwojna,

---

[12] PWN (b.d.w.). *Informacja.* https://encyklopedia.pwn.pl/haslo/informacja;3914686.html [dostęp 01.03.2022].

[13] Encyklopedia Zarządzania (b.d.w.). *Informacja*. https://mfiles.pl/pl/index.php/Informacja [dostęp 01.03.2022].

[14] A. Żebrowski (2016). *Służby wywiadowcze uczestnikami zakłócenia informacyjnego (wybrane problemy)*. W A. Żebrowski, A. Woźny (red.), *Siły Zbrojne. Działania wywiadu w XX i XXI w. Wybrane zagadnienia*. Uniwersytet Pedagogiczny w Krakowie. Kraków, s. 26.

[15] *Ibidem*, s. 26.

[16] *Ibidem*, s. 26–27.

[17] W. Krztoń (2017), *Walka…. Op. cit.*, s. 13.

cyberagresja, cyberszpiegostwo[18]. W związku z tym we współczesnym świecie pojawia się potrzeba rywalizacji o informację i dominacji w tej sferze. Dlatego też rodzi się coraz większa potrzeba pozyskania informacji, a wraz z tym pojawia się właśnie walka o informację. Przedmiotem tej walki staje się informacja oraz wszystkie możliwe środki i narzędzia do zdobycia i ochrony pozyskanych i przechowywanych danych[19]. Należy zauważyć, że wiele organizacji (także tych o charakterze terrorystycznym) oraz krajów prowadzi działania z elementami walki informacyjnej, przy czym nie podmioty te nie rezygnują z tradycyjnych form działań, ataków. Ataki cyberterrorystyczne lub operacje psychologiczne są uzupełnieniem konwencjonalnej działalności podmiotów[20]. Zaznaczyć trzeba, że to informacja będzie głównym czynnikiem decydującym o postępie konfliktu zbrojnego, ale w obszarze informacji[21].

Omawiając w niniejszej pracy zjawisko walki informacyjnej czy też walki o informację, należy przedstawić definicję tejże walki. W pracy Waldemara Krztonia odnaleźć możemy wyjaśnienie walki informacyjnej, według niego są to „działania prowadzone przez pododdziały i oddziały wojskowe w celu uzyskania przewagi informacyjnej nad przeciwnikiem lub uszkodzenia jego zasobów informacyjnych oraz wojskowych systemów i sieci teleinformatycznych. Przedmiotem walki informacyjnej nie jest informacja a system informacyjno-sterujący"[22]. Istnieje wiele ujęć dotyczących walki informacyjnej, warto tutaj podać definicję zjawiska według Piotra Sienkiewicza: „jest to całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięciem zamierzonych celów militarnych (politycznych). W rozumieniu infowojny ważne jest: po pierwsze – zniszczenie lub degradacja wartości zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych, po drugie – zapewnienie bezpieczeństwa własnym zasobom i wykorzystywanym systemom informacyjnym"[23]. Należy także określić, co wchodzi w obręb wojny informacyjnej. Przede wszystkim jest to wieloaspektowy i wielokierunkowy proces, który składa się z elementów takich jak: akcja psychologiczna, wojna psychologiczna, budowanie relacji publicznych i interpersonalnych, dyplomacji publicznej[24].

W pracy należy również wyjaśnić, na czym polega i czym charakteryzuje się walka informacyjna. Andrzej Żebrowski wyjaśnia, iż jest to „zorganizowana forma przemocy polegająca na aktywności wewnętrznej państwa, która prowadzona jest w celu uzyskania celów (politycznych). Skierowana jest wobec zniszczenia lub modyfikacji systemów informacyjnych albo zasobów danych przeciwnika. Jest to również działalność nakierowana na ochronę własnych zasobów informacji oraz systemów informacyjnych przed takim

[18] *Ibidem*, s. 148.

[19] *Ibidem*.

[20] *Ibidem*, s. 149.

[21] A. Żebrowski (2017). *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa*. Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie. Kraków.

[22] W. Krztoń (2017). *Walka…. Op. cit.*, s. 150.

[23] *Ibidem*, s. 152.

[24] *Ibidem*, s. 153.

rodzajem działalności przeciwnika"[25]. Należy zauważyć, że informacja w walce informacyjnej staje się zasobem, celem ataku, a także broni[26]. Jest to także działalność destrukcyjna infrastruktury wykorzystywana przez przeciwnika do działań operacyjnych. Żebrowski przedstawia również wpływ walki informacyjnej oraz samej informacji:

WALKA INFORMACYJNA + INFROMACJA = DECYZJA → DZIAŁANIE
lub
WALKA INFORMACYJNA + INFORMACJA = DECYZJA → DZIAŁANIE = DESTRUKCJA[27]

Dominacja informacyjna skutkować może wygraną z wrogiem przy braku użycia uzbrojenia, zastosowania walki zbrojnej. Należy również zaznaczyć, że celem ataku coraz częściej stają się systemy informacyjne. Realnym i znaczącym w pracy przykładem są systemy informacyjne służb specjalnych[28]. Podkreślić również trzeba, że walka informacyjna polega na dojściu i zdobycia poufnych danych, informacji, a także strategii (wszelkiego rodzaju). Istotna staje się także wartość informacji, a także przewaga informacyjna, która daje możliwość osiągnięcia celów politycznych, militarnych, ekonomicznych czy informacyjnych[29]. Walka informacyjna dotyczy również sfery militarnej (wojskowej). Ma ona wpływ na obszar informatyczny na szczeblach dowodzenia. W omawianiu problemu walki informacyjnej ważna jest także sieciocentryczność, która prowadzi do tworzenia złożonego systemu, zastosowania techniki informatycznej. Szczególna zasada sieciocentryczności to wykorzystywanie dostępnych zasobów informacji w taki sposób, aby zwiększyć potencjał bojowy[30].

Danuta Kaźmierczak w swojej pracy *Walka informacyjna we współczesnym świecie i jej społeczne konsekwencje*[31] podkreśla, że „według myśli strategicznej USA wojna informacyjna staje się elementem wykorzystywanym coraz częściej w konfliktach zbrojnych co pozwala na ograniczenie użycia uzbrojenia, przemocy, a także strat w ludziach"[32]. Operacje informacyjne, a także psychologiczne prowadzone są właśnie w otoczeniu informacyjnym. Operacja informacyjna prowadzona jest na płaszczyźnie poznawczej (gdzie celem staje się człowiek), informacyjnej (dane stają się celem), fizycznej (cel to system informacyjny)[33]. Zjawisko wojny informacyjnej nie jest nowym i nieznanym problemem. Nawiązuje do niego już Sun Tzu w swoich poglądach: „Największym osiągnięciem jest pokonanie wroga bez walki"[34].

---

[25] A. Żebrowski (2016). *Op. cit.*, s. 29.
[26] *Ibidem*, s. 30.
[27] *Ibidem*.
[28] *Ibidem*, s. 31.
[29] *Ibidem*, s. 149.
[30] *Ibidem*, s. 158–159.
[31] D. Kaźmierczak (2017). *Walka informacyjna…. Op. cit.*, s. 120.
[32] *Ibidem.*
[33] *Ibidem*.
[34] A. Żebrowski (2017). *Op. cit.*, s. 99.

Należy tutaj również wymienić źródła walki informacyjnej, które w całym tym aspekcie są bardzo istotne. Podstawą skutecznej wojny informacyjnej są przede wszystkim czynniki wojskowo-technicznej:

- informatyzacja sił zbrojnych i rozwój możliwości łączności w dowodzeniu,
- unowocześnienie, modernizacja armii (w tym także elektrooptyczne urządzenia rozpoznania obrazu);
- oraz pozawojskowe:
- powstanie i rozwój ogólnopaństwowej bazy informatycznej (też pozapaństwowej),
- komputeryzacja gospodarki,
- rozwój systemów łączności elektronicznej,
- różnorodne bazy danych,
- masowe wykorzystywanie komputerów[35].

Ważny jest również zakres prowadzonej walki konwencjonalnej i niekonwencjonalnej, co oznacza wyznaczenie obszaru walki oraz jego wnętrza. Jest to istotne ze względu na to, że otoczenie obszaru jest odpowiedzialne za stymulację procesu informacyjnego (układ sterująco-decyzyjny oraz obiekt oddziaływania). Natomiast wnętrze walki odpowiada za opis procesu informacyjnego, który steruje walką, a także za opis procesu informacyjnego wewnętrznego w układach sterujących[36]. Walka informacyjna nie jest prowadzona tylko w obszarze dowodzenia. Ze względu na sposób prowadzenia wojny informacyjnej daje ona możliwości m.in.: zdobywania informacji, maskowania operacyjnego i taktycznego, działań psychologicznych, ochrony informacji niejawnych. W sferze militarnej walka ta prowadzona jest przez wszystkie rodzaje sił zbrojnych, ale także przez wywiad i kontrwywiad, i inne podmioty, które posiadają odpowiednie uprawnienia do takich działań. Prowadzona jest również przez podmioty takie jak: NATO, UE, organizacje przestępcze, organizacje terrorystyczne, korporacje gospodarcze, organizacje narodowowyzwoleńcze[37].

Metody walki informacyjnej

Najważniejszymi metodami walki informacyjnej jest: operacja psychologiczna, propaganda, dezinformacja, cyberatak (różnego rodzaju), manipulacja informacją.

1. *Operacja psychologiczna*. Celem prowadzenia takiego rodzaju operacji jest przede wszystkim osłabienie aktywności i działań przeciwnika, zaangażowanie i wzmocnienie przyjaznych obiektów oddziaływania, zdobycie poparcia ze strony środowisk niezaangażowanych[38]. Operacje te prowadzone są przez organy propagandowo-agitacyjne. W wojnie psychologicznej wykorzystuje się konflikty takie jak np.: religijne, narodowościowe, społeczne oraz inicjuje się m.in.: chaos, panikę, sabotaż, dywersję. Powszechne jest także fałszywe zapewnienie polepszenia statusu życia czy swobód i praw obywatelskich. W operacji psychologicznej

[35] *Ibidem*, s. 100.

[36] *Ibidem*, s. 104.

[37] *Ibidem*, s. 107.

[38] T. Grabowski (2016). *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014–2016)*. „Horyzont Polityki", 20(7), 34.

wspiera się również organizacje terrorystyczne, nieprzyjazne czy też wrogie grupy przestępcze, wrogie partie polityczne[39]. Doktryna NATO wyróżnia dwa rodzaje operacji psychologicznych: zaczepne (celem jest osłabienie walki przeciwnika) oraz obronne (celem jest zdobycie wsparcia podmiotów dotąd niezaangażowanych oraz poprawienie i wzmocnienie nastrojów własnego narodu)[40].

2. *Propaganda.* Celem działań propagandowych jest przekazanie fałszywych, nieprawdziwych komunikatów czy informacji. Istotne w szerzeniu propagandy jest to, że używa się przemyślanych i składnych sformułowań czy też przekonujących fotografii, nagrań, pieśni, manifestacji i innych środków przekazu. Wykorzystuje się również wiedzę naukową w zakresie poprawnego czy efektywnego wpływania na emocje i zachowania ludzkie. Propaganda posiada w sobie funkcje informacyjne (wyjaśnienie), ale również perswazyjne (wpływ na zachowanie, wzmacnianie postaw i wyczekiwanych zachowań)[41]. Należy również wymienić źródła propagandy. Wyróżnia się propagandę: białą (nadawca jest znany), szarą (nadawca jest lub nie jest zidentyfikowany, a przekazywane informacje nie są precyzyjne), czarną (nadawca jest niezidentyfikowany, a przekaz jest nieprawdziwy, fałszywy). Kierunki propagandy mogą być wewnętrzne lub zewnętrzne. Można ją określić ze względu na czas: poprzedzająca, towarzysząca, następcza[42].
3. *Dezinformacja.* Jest to działanie mające na celu wprowadzenie w błąd poprzez podanie fałszywych informacji. Charakterystyczne dla dezinformacji jest to, że przekazywane przez nią informację są mylące (poprzez ich fałszywość)[43]. Według definicji używanej przez NATO, dezinformacja obejmuje także prowokacyjne działania mające na celu naruszenie interesów przeciwnika. Ważne jest podkreślenie, że działania dezinformacyjne dążą do wprowadzenia przeciwnika w błąd i są to działania celowe. Sposoby dezinformacji obejmują wykorzystanie agentury, manipulację otoczeniem, propagandę radiową i elektroniczną, a także działania za pośrednictwem mediów masowego przekazu[44].
4. *Manipulacja informacją.* Stanowi nieodłączny element dezinformacji i propagandy. Obejmuje ona celowe manipulowanie prawdziwymi informacjami w taki sposób, aby wywołać określony efekt u odbiorców. Przykładowo, może to oznaczać celowe pomijanie istotnych informacji, aby przekaz wywołał określone reakcje wśród odbiorców[45]. Sposoby manipulacji informacją obejmują przekazywanie danych o dużym znaczeniu jako marginalnych, przesyłanie danych wieloznacznych, które

[39] *Ibidem*, s. 34–35.

[40] *Ibidem*, s. 35.

[41] *Ibidem*, s. 37.

[42] *Ibidem*, s. 38.

[43] Z. Modrzejewski (2018). *Dezinformacja w służbie walki informacyjnej*. W T.W. Grabowski, M. Lakomy, K. Oświecimski (red.), *Bezpieczeństwo informacyjne w dobie postprawdy*. Wydawnictwo Naukowe Akademii Ignatianum w Krakowie. Kraków, s. 93.

[44] *Ibidem*, s. 96.

[45] T. Grabowski (2016). *Metody walki…. Op. cit.*, s. 45.

utrudniają zrozumienie, oraz generowanie nadmiaru informacji w celu spowodowania tzw. chaosu informacyjnego[46].

5. *Cyberatak.* Działania mające na celu wykorzystanie sieci czy systemów komputerowych i użycia szkodliwego oprogramowania do zniszczenia lub kradzieży danych często bardzo istotnych dla bezpieczeństwa podmiotu. Jest to narzędzie wykorzystywane do oszustw czy kradzieży[47]. Do rodzajów cyberataków zalicza się na przykład: *phishing* (podszywanie się pod różne zaufane instytucje w celu kradzieży istotnych danych takich jak hasła za pomocą spreparowanych wiadomości), *sniffing* (wyłudzanie danych, haseł dostępowych za pomocą przechwycenia informacji przez niezaszyfrowane przepływające w sieci dane), *skimming* (przekopiowanie danych z kart magnetycznych za pomocą specjalnych urządzeń ulokowanych w czytnikach kart), atak DDoS (atak hackerski przeprowadzany z wielu źródeł)[48].

Przykłady metod walki informacyjnej

Sposobów walki informacyjnej obecnie jest wiele. Ze względu na dynamiczny i ciągły rozwój technologii, ale także różnych obszarów Internetu coraz trudniej jest zapanować nad tym zjawiskiem i walka informacyjna staje się dostępna dla każdego podmiotu (przedsiębiorstwa, organizacji, państw itd.). Dobrym przykładem takiego działania są fake newsy rozpowszechniane w mediach, Internecie, a nawet prasie. Problem ten kształtuje zjawisko postprawdy, czyli nieobiektywnego przekazywania prawdziwych informacji, które są przepełnione emocjami czy osobistymi przekonaniami[49]. Jako przykład można wymienić sprawę zestrzelonego Boeinga 777 nad Donbasem oraz przekaz przebiegu prowadzonego oficjalnego śledztwa przez rosyjskiego eksperta wojskowego Aleksandra Chramczychina, który stwierdził, iż: „nie jest prowadzone w celu ustalenia prawdy, ale właśnie w celu stworzenia odpowiedniego tła emocjonalnego w społeczeństwie. To bardzo symboliczne, że najbardziej niezadowolona z takiego przebiegu śledztwa jest Malezja, a więc kraj niedemokratyczny z zachodniego punktu widzenia"[50]. Innym bardzo ciekawym przykładem postprawdy, ale również szerzenia propagandy są przedstawiane tezy Chramczychina dotyczące otrucia byłego rosyjskiego agenta – Siergieja Skripala. Mianowicie podaje on naprawdę mało wiarygodne i mało prawdopodobne rozwiązania tejże sytuacji: „a) Skripalowie zostali otruci przez rosyjskich agentów jako zemsta za ich zdradę, b) Skripalowie zostali otruci przez Brytyjczyków (lub Amerykanów), aby każdy mógł pomyśleć, że Skripalowie zostali otruci przez rosyjskich agentów jako zemsta za zdradę, c) Skripalowie zostali otruci przez rosyjskich agentów, aby wszyscy myśleli, że

[46] *Ibidem*, s. 45–46.

[47] IBM (b.d.w.). *Czym są cyberataki i jak się przed nimi bronić?* https://www.ibm.com/pl-pl/services/business-continuity/cyber-attack [dostęp 08.03.2022].

[48] Chmuraprawna (2020). *Rodzaje cyberataków*. https://chmuraprawna.pl/2020/09/03/rodzaje-cyberatakow/ [dostęp 08.03.2022].

[49] M. Dura (2020). *Polska celem wojny informacyjnej*. https://cyberdefence24.pl/bezpieczenstwo-informacyjne/rosja-polska-celem-wojny-informacyjnej-opinia [dostęp 08.03.2022].

[50] *Ibidem*.

Brytyjczycy (lub Amerykanie) otruli Skripalów, tak aby sądzono, że Skripalowie zostali otruci przez rosyjskich agentów jako zemstę za zdradę, d) nikt w ogóle nie otruł Skripalów, a Brytyjczycy całkowicie wymyślili całą historię, aby wszyscy myśleli, że Skripalowie zostali otruci przez rosyjskich agentów jako zemsta za zdradę[51]".

Jednym z najbardziej znanych, ale także najpoważniejszych ataków o charakterze walki informacyjnej było unieruchomienie witryn rządowych Estonii w 2007 roku poprzez metodę DDoS. Celem tego ataku stały się także serwisy internetowe oraz bankowe. Spowodowało to także zablokowanie możliwości płatności kartą i wykonywania połączeń telefonicznych[52]. Również na szczególną uwagę zasługuje przykład udostępnienia ściśle strzeżonych danych. W 2010 roku ujawniono depesze przesyłane między Departamentem Stanu USA a ambasadami. Ujawnione dokumenty posiadały nawet najwyższe klauzule tajności i zostały opublikowane przez m.in. WikiLeaks (WikiLeaks specjalizuje się w analizie i publikacji dużych zbiorów danych cenzurowanych lub w inny sposób ograniczonych oficjalnych materiałów dotyczących wojny, szpiegostwa i korupcji. Do tej pory opublikowała ponad 10 milionów dokumentów i powiązanych analiz[53]) oraz inne mass media. Opublikowane dokumenty przedstawiały np. tajne informacje, nazwiska informatorów. Kradzież była możliwa dzięki atakowi DDoS[54].

Bardzo dobrym, znanym i szerokim działaniem wojny informacyjnej jest również jej wymiar społeczny. Przykładem tego jest nasilenie migracji w 2014 roku i wraz z tym przedostawanie się nieprawdziwych i trudnych do zwalczenia informacji[55]. Innym przykładem kłamstwa przekazywanego za pomocą portali internetowych i Internetu jest trolling internetowy. W obecnym czasie jest to powszechny problem, który z biegiem czasu będzie się rozwijał, a to narzędzie walki informacyjnej będzie wykorzystywane jeszcze częściej. Trolling internetowy polega na publikacji kłamliwych informacji czy przekazów. Jest to również szerzenie zjawisk takich jak np. nacjonalizm, przy pomocy mediów społecznościowych, ale również tworzenie złej, gorszącej i bolesnej opinii na temat grupy społecznej czy jednostki, nazywane również hejtem[56]. W środowisku cybernetycznych pojawiają się także trolle polityczne, których działaniem jest rozpowszechnianie fałszywych i kłamliwych informacji na temat przeciwnika politycznego. Przykładem tego jest prowadzone wrogie i obraźliwe działanie wobec Hillary Clinton w 2016 roku w kampanii wyborczej kandydatki. Powszechnie wiadomo, że za opisanym atakiem stał przeciwnik Clinton, a późniejszy prezydent USA Donald Trump, który operację tą przeprowadził przy pomocy rosyjskich trolli politycznych[57].

---

[51] *Ibidem*.

[52] B. Jagusiak, S. Olczak (2016). *Wpływ wojny informacyjnej na bezpieczeństwo europejskie – wybrane problem*. „Studia Administracji i Bezpieczeństwa", 1, 154.

[53] WikiLeaks (2015). *O nas*. https://wikileaks.org/What-is-WikiLeaks.html [dostęp 08.03.2022].

[54] B. Jagusiak, S. Olczak (2016). *Op. cit.*, 156.

[55] *Ibidem*, s. 159.

[56] Newprojcet (2021). *Trolling internetowy*. https://www.newproject.biz.pl/2021/12/11/trolling-internetowy/ [dostęp 08.03.2022].

[57] *Ibidem*.

Kolejnym ciekawym i wysoce rozwiniętym przykładem walki informacyjnej jest prowadzenie wojny informacyjnej przez Federację Rosyjską. Wydarzeniem takim był chociażby atak na gruzińskie strony rządowe podczas konfliktu gruzińskiego w 2008 roku. Atak ten polegał na wyświetlaniu na stronie parlamentu gruzińskiego podobizny prezydenta do Adolfa Hitlera. Strona gruzińska jest przekonana (na podstawie wielu dowodów, połączeń i źródeł internetowych), że za opisanym atakiem stały rosyjskie służby specjalne[58]. Celem ataku Federacji Rosyjskiej stała się (i z pewnością w przyszłości stanie się również) Polska. Przykładem tego są działania w przestrzeni informacyjnej nie tylko polskiej, ale również międzynarodowej, które mają na celu tworzenie przekazu destabilizującego stronę polską, a nawet izolację międzynarodową, m.in. poprzez: kreację negatywnego obrazu polski, budowanie niepokoju i realnego zagrożenia[59]. Aktualnym problemem związanym z działaniami rosyjskimi jest prowadzenie rozbudowanej dezinformacji podczas trwającej wojny na Ukrainie. Strona rosyjska za pomocą dezinformacji separuje przede wszystkim własnych obywateli od prawdy, jaką jest atak sił zbrojnych Rosji na Ukrainę. Przekazywane są fałszywe i nieprawdziwe informacje o tym, że prowadzone działania militarne nie nazywają się wojną, a tylko „operacją specjalną", która ma zapewnić bezpieczeństwo państwa. Co ciekawe, wiele gazet na terenie Rosji publikuje treści przekonujące, że Rosja nie chce wojny i eskalacji siły w Ukrainie, a prowadzenie jej byłoby błędem[60].

3. Agentura – wpływ na walkę informacyjną oraz sposoby przeciwdziałania wojny informacyjnej i agentury

Agentura – wyjaśnienie pojęcia i rodzaje

Służby specjalne każdego państwa posługują się wieloma tajnymi i jawnymi środkami oraz narzędziami, które na celu mają nie tylko pozyskanie istotnych informacji, ale także strategii przeciwnika czy prowadzenia zakłóceń. Jednym z najważniejszych istniejących zasobów służb wywiadowczych jest osobowe źródło informacji, czyli agentura. Agentura skupia się na zdobyciu informacji istotnych i będących w zainteresowaniu służb specjalnych, ale również na penetracji środowiska przestępczego[61]. Trudno jest odnaleźć w literaturze i dostępnych źródłach definicji agentury. Z pewnością problem ten związany jest z charakterem agentury, działalności agenta. Prowadzenie agentury wiąże się oczywiście z niejawnymi i tajnymi działaniami. Jedno z najwłaściwszych wyjaśnień tego pojęcia znaleźć można na witrynie internetowej Instytutu Pamięci Narodowej: „sieć

[58] B. Jagusiak, S. Olczak (2016). *Op. cit.*, s. 161.

[59] Raport Bezpieczeństwa i Obronności (2017). *Rosyjska wojna informacyjna wobec Polski*. https://pulaski.pl/wp-content/uploads/2015/02/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf [dostęp 08.03.2022].

[60] M. Potocki (2022). *Rosyjska propaganda obrzuca Ukraińców błotem i szuka zdrajców*. https://serwisy.gazetaprawna.pl/media/artykuly/8370196,rosyjska-propaganda-wojna-w-ukrainie-media-dezinformacja.html [dostęp 08.03.2022].

[61] A. Żebrowski (2018). *Agentura wpływu uczestnikiem walki informacyjnej*. „Studia nad Autorytaryzmem i Totalitaryzmem", 1, 62.

agenturalna, wszystkie dostępne osobowe źródła informacji"[62]. Służby specjalne wykorzystują agenturę głównie w celach prowadzenia zakłóceń przestrzeni informacyjnej (osobowej oraz technicznej). Należy także zaznaczyć, że agentura to pośredni sposób zdobycia informacji, które znajdują się w kręgu zainteresowań służb wywiadowczych[63]. Dodatkowo agent ma także wpływ na poglądy polityków czy mass mediów w taki sposób, aby było to korzystne dla obcego państwa. Zauważyć trzeba także, że istnieje agentura wpływu polegająca na działalności agenta, który przekazuje informacje dezinformacyjne, propagandowe. Działa on w obszarze jednostek decyzyjnych[64].

Typami agentów, którzy mają wpływ na przebieg walki informacyjnej, są: *agent główny* (pełni rolę prowadzącego, steruje innymi agentami i ich zadaniami), *agent nieświadomy* (nie jest poinformowany, że przekazywane informację posłużą służbom wywiadowczym), *agent zamieszania* (jego celem jest zakłócanie pracy obcych służb specjalnych czasem i własnych), *agent podwójnie przewerbowany* (agent działający dla obcych służb i odkryty przez ojczyste służby specjalne, zostaje zmuszony lub też nie do współpracy przeciwko służbom wywiadowczych, dla których zdobywał informację), *agent podwójny* (działający dla dwóch konkretnych służb specjalnych i przekazując im informacje dotyczące konkurenta. Zwykle zwerbowany pod przymusem), *agent prowokator* (celem jego działań jest przedstawienie w złym świetle, upokorzenie wybranej osoby lub grupy, nakłania również do czynów karanych prawnie), *agent urojony* (agent fikcyjny, wymyślone źródło domniemanych informacji), *agent uśpiony* (agent rozpoczynający działalność po odpowiednim znaku, sygnale), *agent czysty* (niedziałający w obszarze pracy operacyjnej, nieznany przeciwnikowi), *agent odpad* (osoba wystawiona w celu ochrony innego ważnego agenta)[65].

Agentura wpływu

Bezapelacyjnie działalność agentury ma istotny wpływ na przebieg walki informacyjnej. Z treści niniejszej publikacji wiadomo już, że wojna informacyjna prowadzona jest za pomocą informacji i na celu ma niszczenie przeciwnika. W tym punkcie należy także zaznaczyć, że jednym z najważniejszych narzędzi walki informacyjnej jest służba wywiadu i kontrwywiadu państwa. Głównym zadaniem tych służb wobec tego rodzaju wojny jest pozyskiwanie informacji dotyczących wroga lub przedmiotów będących w zainteresowaniu państwa oraz prowadzenie walki informacyjnej. Oczywiście służby wywiadu i kontrwywiadu charakteryzują się odpowiednią organizacją i przygotowaniem[66]. Jednym z bardzo ważnych sposobów działań służb specjalnych w zakresie walki informacyjnej jest prowadzenie propagandy, ale także manipulacji. Poprzez dywersję

[62] Biuletyn Informacji Publicznej IPN (b.d.w.). *Agentura*. https://katalog.bip.ipn.gov.pl/slownik/ [dostęp 09.03.2022].

[63] A. Żebrowski (2018). *Op. cit.*, 66.

[64] J. Rokitowska (2019). *Uczestnicy walki informacyjnej*. W O. Wasiuta, R. Klepka (red.), *Vademecum Bezpieczeństwa Informacyjnego*. Instytut Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego im. KEN w Krakowie, Kraków, s. 483.

[65] Żebrowski A. (2018). *Op. cit.*, 65–66.

[66] J. Kossecki (b.d.w.). *Elementy wojny informacyjnej*. http://autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf [dostęp 10.03.2022].

wywiadowczą można wpływać na podjęcie decyzji przez przeciwnika, a konsekwencje tego czynu mogą zostać odpowiednio wykorzystane. Istotną metodą prac wywiadu i kontrwywiadu jest manipulacja, której celem jest ukryte sterowanie przeciwnikiem tak, aby sam dokonał szkód na obszarze własnego pola działania[67].

W niniejszej pracy istotnym elementem w procesie walki informacyjnej jest kanał sterowniczy, nazywany agenturalnym. Ten kanał ma na celu realizację wszystkich zadań wydawanych przez centralne ośrodki kierujące. Obowiązki te są wykonywane w zamian za wynagrodzenie lub korzyści, lub też motywowane wyznawanymi ideami oraz zasadami etycznymi. Przykładem takiego działania może być agent wywiadu lub tajny współpracownik służb, który wykonuje polecenia oficera prowadzącego[68]. Ważne jest również, aby podać dwa istotne kanały sterownicze, których zadaniem jest oddziaływanie na przeciwnika. Są nimi:

- kanały informacyjne (zbieranie i przekazywanie zdobytych informacji o przeciwniku),
- kanały sterowniczo-dywersyjne (celem jest tworzenie wpływów przeciwko przeciwnikowi, w szczególności w celu zakłócenia jego systemów)

Walka informacyjna ma na celu niszczenie przeciwnika i jego systemów, ale także ochronę własnego systemu przed wymienionymi działaniami. Wykonywane zadania mogą być jawne lub nie, agent wywiadu jest rozwiązaniem niejawnym, natomiast attaché wojskowy jest jawny[69].

Bardzo ważnym narzędziem do pozyskania informacji, ale przede wszystkim w celu dezinformacji przeciwnika jest agent wpływu. Faktem jest, że osoba pełniąca rolę agenta wpływu może współpracować jako typowy agent, ale także w pozbawionej dystansu i relacji formie: oficer prowadzący–agent[70]. Narzędzie, jakim staje się agentura wpływu, jest najskuteczniejszym sposobem prowadzenia dezinformacji czy propagandy, a dodatkowo metoda ta jest trudna do ujawnienia, odkrycia. Największe efekty mogą zostać uzyskane w społeczeństwie, które jest niestabilne, pozbawione etyki i pełne chaosu. Operacja przy wykorzystaniu wpływu agentury zwykle nie sprawdza się w państwie ułożonym, posiadającym normy prawne[71]. Należy też zaznaczyć, że agentura wpływu nie pozyskuje jedynie danych (co pozostaje w obszarze kompetencji służb specjalnych), nie panuje jedynie nad przepływem informacji. Przede wszystkim realizuje zadania z zakresu: wykradania danych, wzmocnienia i użycia dezinformacji[72]. Agent wpływu bez problemu potrafi utożsamić się z obserwowanym środowiskiem, dzięki czemu może mieć bardzo istotny wpływ na decyzje, które są podejmowane. Przykładem tego mogą być chociażby te dotyczące poczynań politycznych. Bardzo ważne jest, aby dany agent posiadał szeroką wiedzę dotyczącą państwa pobytu, ale także o najważniejszych

[67] *Ibidem*.

[68] *Ibidem*.

[69] *Ibidem*.

[70] B. Piasecki (2021). *Kontrwywiad atak i obrona*. Wydawnictwo LTW. Łomianki, s. 231.

[71] Strona Józefa Darskiego Jerzy Targalski (1952–2021) (2010). *Agentura Wpływu*. https://jozefdarski.pl/6330-agentura-wplywu [dostęp 11.03.2022].

[72] *Ibidem*.

politykach, osobach w tym kraju. Praca agenta wpływu polega przede wszystkim na *zakłócaniu informacyjnym* (celem jest obniżenie potencjału systemów odpowiedzialnych nie tylko za kierowanie, ale też dowodzenie; dotyczy to również służb wywiadowczych i kontrwywiadowczych). Ten sposób oddziaływania agenta wpływu jest bardzo istotny, bo dzięki temu nie tylko posiada on możliwość wpływu na decyzje odpowiednich decydentów, ale również na otoczenia takiej osoby. Do działań agenta należy także przedstawienie jak najbardziej fałszywego obrazu rzeczywistości[73]. Metoda polegająca na zakłócaniu informacyjnym prowadzona jest w formie zbrojnej i niezbrojnej i posiada kilka podstawowych funkcji. Mianowicie wyróżnia się:

- pozorowanie, czyli wprowadzenie w błąd osoby decyzyjnej oraz odwracanie uwagi od swojej osoby (od podejrzeń);
- dezorganizację pracy (wpływ na decyzje decydenta).

Ważne jest, aby agent w swojej pracy dbał o swoje bezpieczeństwo i wykonywał swoje zadania w sposób proporcjonalny[74].

Należy także podkreślić istotność prowadzenia dezinformacji osobowej, której celem jest prowadzenie zakłóceń informacyjnych, podawanie fałszywych informacji, tak, aby wpłynąć na jego morale w celu podejmowania przez tę osobę niekorzystnych dla niej decyzji. Wykorzystywanie spreparowanych informacji zostaje wprowadzane do wybranego środowiska przez służby specjalne, w tym poprzez agenturę[75]. Służby wywiadowcze i kontrwywiadowcze w swojej pracy przewidują posługiwanie się środkami psychologicznymi, socjologicznymi i technicznymi. Jednym z mechanizmów psychologicznych jest manipulacja, której celem jest wpływ na świadomość i podświadomość, a także na sterowaniu postępowaniem. Działania takie nieść mogą różne konsekwencje, jak występowanie agresji, brutalności, uprzedzeń, wrogości wobec innych narodowości czy państw[76]. Andrzej Żebrowski w swojej pracy wyróżnia następujące formy oddziaływania manipulacji na stany osobowe:

1. „w zachowaniu osób (lub grupy) zawarte są wyraźne wskazówki świadczące o tym, że osoba ta wywiera wpływ na inną osobę lub grupę w celu zmiany modyfikacji postawy i zachowania;
2. wskazówki świadczące o wywieranym wpływie są zazwyczaj ukrywane, lecz dostępne poznaniu osoby (grupy) będącej przedmiotem wpływu po dokonaniu przez nią odpowiedniej analizy zachowania lub intencji osoby wywierającej wpływ;
3. osoba (grupa) będąca przedmiotem wpływu nie powinna zdawać sobie sprawy z wywieranego wpływu;
4. percepcja danych, jawnych bądź ukrytych, świadczy o tym, czy mamy do czynienia z całkowicie lub częściowo jawnymi metodami wpływu społecznego, czy też manipulacją;

---

[73] Żebrowski A. (2018). *Op. cit.*, 65–66.

[74] *Ibidem*, 67–68.

[75] *Ibidem*, 68.

[76] *Ibidem*, 69.

5. manipulacja odnosi się do trzeciego rodzaju percypowania wpływu — może być wykorzystywana jako technika wpływania na behawioralny komponent zachowań i postaw;
6. epistemologiczną istotą oddziaływania manipulacyjnego jest proces sterowania, który prowadzi do realizacji celów podmiotu działań — zgodnie z celem i obiektywnym interesem własnych sił prowadzących działania zbrojne i/lub niezbrojne. Innymi słowy manipulację można prowadzić tam, gdzie odpowiedni przekaz informacyjny (sterowanie) będzie modyfikował postawy i zachowania przeciwnika, a także, gdy sterowana osoba (osoby) nie wykona zadania, zaniecha lub zaniedba działania ważne dla własnej pomyślności, własnych interesów bądź celów tego, kto formalnie nią kieruje i dowodzi"[77].

Dodatkowo podczas użycia manipulacji wywoływane są emocje oraz wpływa się na odczucia. Dla uzyskania ustalonych postaw czy zachowań jednostki manipulowanej stosuje się m.in.:

- informacje istotne, ważne przekazywane jako marginalne,
- przekazywanie sygnałów, informacji niezrozumiałych,
- tworzenie chaosu informacyjnego,
- przekaz fałszywych informacji[78].

Działania takie jak dezinformacja, manipulacja, zakłócanie informacyjne stosuje się nie tylko wobec jednostki, ale także grup społecznych, które atakuje się za pomocą mediów (przekazów medialnych) czy gier komputerowych. Do tego celu wykorzystywana jest agentura, agentura wpływu, dyplomacja, operacje specjalne, organy państwowe, ale także media. Warto także podkreślić, że agenci wykonujący czynności związane z agenturą wpływu często zajmują stanowiska urzędnicze, mogą być oni dziennikarzami, dyplomatami, cywilnymi pracownikami służb specjalnych. Zajmują tak wysokie stanowiska, aby wpływać na życie polityczne danego państwa[79].

Sposoby przeciwdziałania metodom wojny informacyjnej oraz agenturze

Jak już wspomniano wcześniej, działania służb specjalnych, a w szczególności agentury i agentury wpływu skupiają się głównie na pozyskiwaniu istotnych, tajnych informacji, ale jest to także dezorganizacja sił przeciwnika czy akcje propagandowe, działania w celu osłabienia gospodarki wroga (także potencjału wojskowego, spraw politycznych) i potencjału obronnego. Wszystkie wymienione kwestie należą do działań dywersyjnych[80]. Warto też nadmienić, że celem ataków stają się zasoby informacyjne czy też kancelarie tajne państwa i systemy informatyczne. Przed zaplanowanym atakiem służb specjalnych na dany podmiot przeprowadza się rozpoznanie danego obiektu w celu ustalenia używanych środków (w tym środków ochrony fizycznej

[77] *Ibidem*, 69–70.

[78] *Ibidem*, 70.

[79] *Ibidem*, 71.

[80] J. Depo (2013). *Teoretyczne i prawne aspekty przeciwdziałania i zwalczania destrukcyjnej działalności obcych służb specjalnych*. „Kultura Bezpieczeństwa. Nauka–Praktyka–Refleksje", 14, 88.

informacji niejawnych), narzędzi. Rozpoznanie polega także na poznaniu możliwości ataku na słabe punkty danego systemu czy wykorzystywanych systemów alarmowych oraz możliwości ich wyłączenia. Skupia się ono również na osobach, które mogą pomóc wywiadowi w osiągnięciu celu poprzez pozyskanie cennej informacji[81]. Znane są dwa źródła ujawnienia informacji istotnych dla bezpieczeństwa państwa. Jedno z nich to system, maszyna, takie jak np. faks, telefon, komputer, radio, sieci łączności. Wszystkie te narzędzia z łatwością poddawane są podsłuchom (teleinformatycznym, radiowym, telefonicznym). Jeśli chodzi o ten rodzaj źródła wypływu informacji, to łatwo jest zapobiegać działaniom związanym z wojną informacyjną. Ze względu na rozwój technologii z łatwością można narzędzia te poddać zabezpieczeniom poprzez kodowanie dwustronne czy w przypadku komputerów – zastosowanie szczelnych kabin ekranujących[82]. Mogą być to również programy ochronne, antywirusowe. Sytuacja jest inna, bardziej skomplikowana, kiedy źródłem ujawnienia informacji staje się człowiek. Szczególnym przypadkiem jest kierownictwo jednostki organizacyjnej. Wypływ informacji od takich osób wiąże się najczęściej z tym, że są oni: podatni na wykorzystywanie ich działań niezgodnych z prawem, brak jasno określonych zasad wewnętrznych dotyczących ochrony informacji niejawnych, brak nawyków personelu o ochronie informacji niejawnych, brak kontroli kierownictwa w zakresie poprawnej ochrony informacji niejawnych. Rozwiązaniem w tej sytuacji jest dokładne przestrzeganie zasad weryfikacji osób, które mają mieć dostęp do zasobów informacji niejawnych, co jasno jest określone w odpowiednich ustawach[83]. Ważne w tej kwestii jest także przestrzeganie przepisów dotyczących OIN oraz stałe szkolenia z zasad przestrzegania OIN, które dotyczą także procedur udzielenia dostępu[84].

Innym bardzo ważnym sposobem zapobiegania działaniom z zakresu walki informacyjnej jest rola rządu oraz edukacji. Trudno jest w środowisku cyfrowym o skuteczną samoobronę osoby atakowanej. Trudności też pojawiają się w momencie działań dywersyjnych na psychikę ofiary. Dlatego też tak ważna jest edukacja na temat obronności i samoobrony[85]. W tym zakresie najważniejsze jest nabywanie wiedzy w taki sposób, aby w późniejszym czasie móc ocenić procesy we współczesnym świecie, zdobywać informacje na temat realnych i aktualnych zagrożeń oraz zapobiegać im w odpowiedni sposób (na skalę globalną i regionalną). Danuta Kaźmierczak w swojej pracy *Walka informacyjna we współczesnym świecie* przeciwdziałania te określa mianem *cognitive skills*, polegają one na: spostrzegawczości, wyciąganiu wniosków, przetwarzaniu informacji, orientacji przestrzennej, koncentracji oraz pamięci[86]. Istotnym procesem w zapobieganiu jednemu z rodzajów narzędzi walki informacyjnej staje się rozpoznanie dezinformacji. Nie jest to łatwe ze względu na potrzebę szerokiej oceny danych zasobów

[81] *Ibidem*, 89.

[82] *Ibidem*, 90.

[83] *Ibidem*, 91.

[84] *Ibidem*, 94.

[85] D. Kaźmierczak (2017). *Walka informacyjna we współczesnym świecie i jej społecznych konsekwencje*. „Studia de Securitate et Educatione Civili". 7, 112.

[86] *Ibidem*, 124.

informacyjnych. Kolejnym ważnym sposobem staje się poprawna, efektowna analiza zdobywanych informacji. Daje to możliwość poprawnego prognozowania, określania przyszłych konsekwencji[87]. Warto także nadmienić zalecenia w formie zadań operacyjnych zamieszczonych w projekcie (z 2015 roku) *Doktryny Bezpieczeństwa Informacyjnego*. W dokumencie wymienia się m.in.:

- ,,zadania sektora publicznego (wymiar krajowy), np.: wykorzystywanie dyplomacji publicznej, monitorowanie i dystrybucja informacji w kwestii cywilnej i wojskowej, edukacja i uświadamianie obywateli, rozpoznanie i neutralizacja dezinformacji;
- zadania sektora publicznego (wymiar międzynarodowy), np.: monitorowanie tworzenia propagandy wobec Polski i wszelkich materiałów dyskredytujących Polskę, analiza źródeł przekazu, kooperacja w zakresie nadawania treści w mediach na Białorusi;
- zadania sektora obywatelskiego, np.: identyfikacja treści, co pozwala na zapobieganie dezinformacji czy propagandzie;
- zadania transsektorowe, np.: współpraca administracji ze służbami państwowymi takimi jak wojsko w celu ochrony interesów państwa w zakresie informacji, kreowania morale społeczeństwa wobec bezpieczeństwa narodowego"[88].

Bardzo ważną rolę w zakresie przeciwdziałania wojnie informacyjnej pełni społeczeństwo obywatelskie. To środowisko badawcze, medialne czy dydaktyczne ma za zadanie rozpoznać dezinformację, doradzać w zakresie tego problemu, ale także kształcić pracowników służb publicznych i edukować osoby wykonujące zadania w środowisku informacyjnym. Dodatkowo prowadzi się (w krajach o wysokiej świadomości problemu) inicjatywy eksperckie. Jedne z najważniejszych i najbardziej znanych ośrodków pochodzą z Wielkiej Brytanii oraz kontynentu amerykańskiego (np. amerykański Atlantic Council)[89]. Przewiduje się także jeszcze rozwiązania technologiczne w celu zabezpieczenia informacji. Dotyczą one zarządzania danymi, zabezpieczeń systemu komputerowego oraz ochrony przed wirusami komputerowymi. Metody te zapobiegają głównie szerzeniu dezinformacji, ale również atakom hackerskim[90].

Wnioski

W niniejszej pracy przedstawiony został problem zjawiska walki informacyjnej, która z biegiem lat nie będzie robiła „kroku w tył", lecz w dynamiczny sposób będzie się rozwijać i przesuwać do przodu. We współczesnym, zglobalizowanym świecie informacja, w szerokim tego słowa znaczeniu, staje się coraz bardziej istotna. To również

[87] *Ibidem*, 125.

[88] *Ibidem*, 126–127.

[89] T. Chłoń (2021). *Przeciwdziałanie dezinformacji – inicjatywy i instrumenty obywatelskie, rządowe i międzynarodowe w wybranych państwach, instytucjach i organizacjach*. Elipsa. Warszawa, s. 72.

[90] J. Janecki (2020). *Problem dezinformacji w procesie decyzyjnym*. W A. Sopińska A. Modliński (red.), *Współczesne zarządzanie – koncepcje i wyzwania*. Oficyna Wydawnicza SGH. Warszawa, s. 242.

dzisiejszy model prowadzenia wojny (wojny hybrydowej) ukazuje, co jest najczęstszym przedmiotem ataku, ale również bronią – oczywiście są to szerokie zasoby informacyjne, w tym także oprogramowanie czy system informacyjny przeciwnika. Tekst ten odpowiada również na pytanie, dlaczego to informacja jest tak ważna. Ta kwestia staje się istotna ze względu na to, że na podstawie zasobów informacyjnych podejmowane są kluczowe decyzje z zakresu bezpieczeństwa państwa czy też w zakresie polityki. Dlatego też zapobieganie, prewencja wobec walki informacyjnej jest tak ważna dla budowania odporności społecznej. Odporność społeczna rozumiana jest jako zabezpieczenie społeczności, państwa przed zagrożeniami, ale jest to także utrzymanie takiego stanu. Sprawność ta utrzymana jest poprzez rozwój, umiejętność przeciwdziałania, ale również wykorzystywanie doświadczenia i umiejętności w radzeniu sobie w walce z zagrożeniem[91]. Realnym i jednym z najbardziej współczesnych przykładów wojny informacyjnej są wydarzenia z 2014 roku związane z tzw. „zielonymi ludzikami" na Krymie. Było to połączenie ukrytych operacji wojskowych, dezinformacji oraz cyberataków, czyli wszystkich elementów składających się na wojnę hybrydową, w tym na walkę informacyjną[92]. Jest to kolejny przykład potrzeby przeciwdziałania walce informacyjnej, która prowadzona jest już nie tylko przez podmioty polityczne, ale również inne organizacje i jednostki. Bardzo niebezpiecznym uczestnikiem (który również prowadzi taką walkę) stają się służby specjalne, które posługują się właśnie agenturą wpływu. Jest to także argument dla opracowania ochrony systemów informacji, jak i samych zasobów informacyjnych w taki sposób, aby mogły one płynnie funkcjonować i spełniać wymogi ochronne oraz kontrolne.

Wobec tego, istotnym elementem obrony przed walką informacyjną jest sprawnie działający kontrwywiad, zwłaszcza kontrwywiad ofensywny. Służby specjalne państwa prowadzą działania mające na celu rozpoznanie działań obcych i wrogich wywiadów, często poprzez wprowadzanie własnych agentów do środowisk wywiadowczych przeciwnika lub obserwację podejmowanych decyzji, a nawet uczestnictwo w procesach decyzyjnych. Ochrona informacji niejawnych odgrywa również kluczową rolę w walce informacyjnej, co zostało omówione w niniejszej pracy. Te informacje są chronione poprzez stosowanie odpowiednich systemów, procedur oraz nadzoru przez upoważnione podmioty przetwarzające tajne dane.

Przedstawione przykłady udowadniają, jak ważna jest przewaga informacyjna. Istotne jest również efektywne i dynamiczne przeciwdziałanie dezinformacji, manipulacji, propagandzie czy agenturze wpływu. Działania te zapewnić mogą stabilną i bezpieczną odporność społeczną. Powinno to zostać zrealizowane przez odpowiednie służby państwowe, rząd, ale również aktywność społeczną.

---

[91] K. Górska-Rożej (2018). *Kształtowanie odporności na zagrożenia w społecznościach lokalnych*. „Przegląd Policyjny", 129(1), 58.

[92] A. Pędziwioł (2018). *Były planista NATO: Atak zielonych ludzików bardziej prawdopodobne niż dywizji czołgów*. https://www.dw.com/pl/by%C5%82y-planista-nato-atak-zielonych-ludzik%C3%B3w-bardziej-prawdopodobny-ni%C5%BC-dywizji-czo%C5%82g%C3%B3w/a-46319143 [dostęp 14.03.2022].

Bibliografia

Biuletyn Informacji Publicznej IPN (b.d.w.). *Agentura*. https://katalog.bip.ipn.gov.pl/slownik/ [dostęp 09.03.2022].

Chłoń T. (2021). *Przeciwdziałanie dezinformacji – inicjatywy i instrumenty obywatelskie, rządowe i międzynarodowe w wybranych państwach, instytucjach i organizacjach*. Elipsa. Warszawa.

Chmuraprawna (2020). *Rodzaje cyberataków*. https://chmuraprawna.pl/2020/09/03/rodzaje-cyberatakow/ [dostęp 08.03.2022].

Depo J. (2013). *Teoretyczne i prawne aspekty przeciwdziałania i zwalczania destrukcyjnej działalności obcych służb specjalnych*. „Kultura Bezpieczeństwa. Nauka–Praktyka–Refleksje", s. 88–94.

Dura M. (2020). *Polska celem wojny informacyjnej*. https://cyberdefence24.pl/bezpieczenstwo-informacyjne/rosja-polska-celem-wojny-informacyjnej-opinia [dostęp 08.03.2022].

Encyklopedia Zarządzania (b.d.w.), *Informacja*. https://mfiles.pl/pl/index.php/Informacja [dostęp 01.03.2022].

Górska-Rożej K. (2018). *Kształtowanie odporności na zagrożenia w społecznościach lokalnych*. „Przegląd Policyjny", 129(1), 58.

Grabowski T. (2016). *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014–2016)*. „Horyzont Polityki", 20, 34, 35, 37, 38, 45.

IBM (b.d.w.). *Czym są cyberataki i jak się przed nimi bronić?* https://www.ibm.com/pl-pl/services/business-continuity/cyber-attack [dostęp 08.03.2022].

Jagusiak B., Olczak S. (2016). *Wpływ wojny informacyjnej na bezpieczeństwo europejskie – wybrane problem*. „Studia Administracji i Bezpieczeństwa", 1, 154, 156, 161.

Janecki J. (2020). *Problem dezinformacji w procesie decyzyjnym*. W A. Sopińska, A. Modliński (red.), *Współczesne zarządzanie – koncepcje i wyzwania* (s. 235–246). Oficyna Wydawnicza SGH. Warszawa.

Kaźmierczak D. (2017). *Walka informacyjna we współczesnym świecie i jej społecznych konsekwencje*. „Annales Universitatis Paedagogicae Cracoviensis. 250 Studia de Securitate et Educatione Civili", 7, 12, 112, 120, 124, 125, 126, 127.

Kossecki J. (b.d.w.). *Elementy wojny informacyjnej*. http://autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf [dostęp 10.03.2022].

Krztoń W. (2017). *Walka informacyjna w cyberprzestrzeni w XXI wieku*. Rambler Press. Warszawa.

Modrzejewski Z. (2018). *Dezinformacja w służbie walki informacyjnej*. W T.W. Grabowski, M. Lakomy, K. Oświecimski (red.), *Bezpieczeństwo informacyjne w dobie postprawdy* (s. 91–118). Wydawnictwo Naukowe Akademii Ignatianum w Krakowie. Kraków.

Newprojcet (2021). *Trolling internetowy*. https://www.newproject.biz.pl/2021/12/11/trolling-internetowy/ [dostęp 08.03.2022].

Pędziwioł A. (2018). *Były planista NATO: Atak zielonych ludzików bardziej prawdopodobne niż dywizji czołgów*. https://www.dw.com/pl/by%C5%82y-planista-nato-atak-zielonych-ludzik%C3%B3w-bardziej-prawdopodobny-ni%C5%BC-dywizji-czo%C5%82g%C3%B3w/a-46319143 [dostęp 14.03.2022].

Piasecki B. (2021). *Kontrwywiad atak i obrona*. Wydawnictwo LTW. Łomianki.

Polończyk A. (2017). *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa*. W H. Batorowska, E. Musiał (red.), *Bezpieczeństwo*

informacyjne w dyskursie naukowym (s. 79–94). Wydawnictwo Uniwersytetu Pedagogicznego.Kraków.

Potocki M. (2022). *Rosyjska propaganda obrzuca Ukraińców błotem i szuka zdrajców*, https://serwisy.gazetaprawna.pl/media/artykuly/8370196,rosyjska-propaganda-wojna-w-ukrainie-media-dezinformacja.html

PWN (b.d.w.). *Informacja.* https://encyklopedia.pwn.pl/haslo/informacja;3914686.html [dostęp 01.03.2022].

Raport Bezpieczeństwa i Obronności (2017). *Rosyjska wojna informacyjna wobec Polski*. https://pulaski.pl/wp-content/uploads/2015/02/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf [dostęp 08.03.2022].

Rokitowska J. (2019). *Uczestnicy walki informacyjnej*. W O. Wasiuta, R. Klepka (red.), *Vademecum bezpieczeństwa informacyjnego* (s. 483–485). Instytut Nauki Bezpieczeństwie Uniwersytetu Pedagogicznego im. KEN w Krakowie. Kraków.

Strona Józefa Darskiego Jerzy Targalski (1952–2021) (2010). *Agentura Wpływu*. https://jozefdarski.pl/6330-agentura-wplywu [dostęp 11.03.2022].

WikiLeaks (2015). *O nas*. https://wikileaks.org/What-is-WikiLeaks.html [dostęp 08.03.2022].

Żebrowski A. (2016). *Służby wywiadowcze uczestnikami zakłócenia informacyjnego (wybrane problemy)*. W A. Żebrowski, A. Woźny (red.), *Siły Zbrojne. Działania wywiadu w XX i XXI w. Wybrane zagadnienia* (s. 15–63). Uniwersytet Pedagogiczny, Kraków.

Żebrowski A. (2017). *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa,* Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie. Kraków.

Żebrowski A. (2018). *Agentura wpływu uczestnikiem walki informacyjnej*. „Studia nad Autorytaryzmem i Totalitaryzmem", 40, 1.