DOI: 10.34752/qjs8-1r89

Aneta KOŁODZIEJ [1]

FAKE NEWS JAKO BROŃ PRZECIW TERRORYZMOWI

Słowa kluczowe: *terroryzm, wojna informacyjna, propaganda, fake news*

STRESZCZENIE

Walka z terroryzmem wymaga ciągłego reagowania na posunięcia przeciwnika. Masowy rozwój technologiczny daje ekstremistom nowe narzędzia, nie tylko do rozprzestrzeniania ideologii, ale również zdobywania nowych członków, zwolenników i sponsorów. Główną platformą systematycznego propagowania idei ekstremistycznych jest Internet. Metodycznym rozpowszechnianiem swoich idei, terroryści próbują zmieniać świadomość odbiorców przez przejmowanie kontroli nad ich umysłami, a co za tym idzie – modyfikować ich zachowania. Oczywistym jest, że odpowiedź koalicji antyterrorystycznej musi być równie zdecydowana. Także ona wykorzystuje nowoczesne formy walki psychologicznej, propagandowej, informacyjnej i dezinformacyjnej. Koalicja wspierana jest przez hakerów, którzy już dokonali kilku spektakularnych operacji dezinformacyjnych, burząc porządek w szeregach organizacji terrorystycznych. Tworzone przez nich fakty, zwane faktoidami lub fake newsami, przyczyniają się do spadku morale zwolenników ruchów ekstremistycznych, poddają pod wątpliwość system ich wartości, szkodzą ich interesom i zamierzeniom. Koniecznie jest jak najszybsze zbadanie znaczenia poziomu cywilnego walki informacyjnej jako zjawiska wspierającego działania komponentu militarnego.

Wprowadzenie

Terroryzm jest zjawiskiem, które nawet mimo braku bezpośredniego zagrożenia, wpływa na nasze poczucie bezpieczeństwa, w każdej sferze życia społecznego. Dlatego też budzi tyle emocji, strachu a jednocześnie woli walki z ekstremistami. Wciąż jednak wybrzmiewa pytanie, w jaki sposób walczyć z nieuchwytnymi, na co dzień niewidocznymi, ale w swoim działaniu bezwzględnymi, organizacjami terrorystycznymi? Jak wygrać z ideą? Konwencjonalne sposoby walki są dalece niewystarczające, stąd próba atakowania ekstremistów ich własną bronią. Chodzi

[1] Wydział Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

o wykorzystanie fałszywych informacji jako narzędzi osłabiania morale i wpływania na sposób myślenia ekstremistów i ich zwolenników.

Pojęcie terroryzmu w literaturze przedmiotu

Wielu badaczy na polu bezpieczeństwa, między innymi Paul D. Williams – profesor w dziedzinie bezpieczeństwa międzynarodowego na Uniwersytecie Warwick w Wielkiej Brytanii – wskazuje, że dla bezpieczeństwa większym problemem od terroryzmu są takie zjawiska jak: nędzą, szkody wywoływane klęskami żywiołowymi, wojną, przestępczością, a nawet wypadkami drogowymi. Mimo to właśnie zjawisko terroryzmu wciąż wzbudza powszechne emocje. Zainteresowanie to wzrosło po atakach przeprowadzonych przez członków organizacji Al-Kaida, 11 września 2001 roku. Dzięki przekazom telewizyjnym niemal wszyscy ludzie na świecie, w czasie rzeczywistym, mogli śledzić samoloty porwane przez terrorystów wbijające się w wieże World Trade Center czy Pentagon. Jak zwraca uwagę Paul D. Williams, *zamachy z 11 września przyniosły w ciągu jednego tylko dnia śmierć blisko trzech tysięcy ludzi, jednakże codziennie co najmniej tyle samo dzieci umiera w państwach Południa wskutek uleczalnych chorób układu pokarmowego, takich jak biegunka czy dyzenteria – najczęściej za sprawą skażenia zasobów wodnych*[2]. Tego decydenci i globalna opinia publiczna zdają się nie zauważać. Nie toczy się na ten temat ogólnoświatowa dyskusja. Zupełnie inaczej sprawa ma się z terroryzmem. Co ważne, strach nie jest tu jedynym czynnikiem. Warto przypomnieć, że ataki z 11 września 2001 roku, za sprawą decyzji administracji prezydenta George'a W. Busha, uznano za początek wojny z terroryzmem. Dało to możliwość wprowadzenia twardych koncepcji przywództwa Stanów Zjednoczonych Ameryki na arenie międzynarodowej, a walkę z terroryzmem uznano za najważniejszy sposób utrzymania bezpieczeństwa na świecie.

Współczesny terroryzm jest tak skomplikowanym i trudnym do zidentyfikowania zjawiskiem, że społeczność międzynarodowa do tej pory nie ustaliła jednej definicji, która kompleksowo opisałaby ten fenomen. Jedną z głównych przyczyn trudności z precyzyjnym określeniem tego, czym jest terroryzm, jest globalizacja. *Stanowić ma ona efekt gwałtownych zmian naruszających równowagę społeczną oraz kryzysu tożsamości. W wyniku procesów globalizacji następuje fragmentacja społeczna, detradycjonalizacja, relatywizacja, kryzys tożsamości, oraz związany z nim deficyt i konflikt tożsamości*[3]. Dodatkowo gwałtowny rozwój technologii, rozwój społeczeństwa

[2] P.D. Williams, *Studia bezpieczeństwa*, Uniwersytet Jagielloński, Kraków 2012, s. 168.

[3] B. Bolechów, *Terroryzm – aktorzy, statyści, widownie*, PWN, Warszawa 2010, s. 150.

informacyjnego, w którym każdy może być odbiorcą ale i nadawcą treści – często tworząc szum medialny – powoduje, że prawie niemożliwe jest precyzyjne odczytywanie zamierzeń terrorystów i zahamowanie rozprzestrzeniania się ich ideologii. Jak zauważa Dominik Duda, *zaskoczenie leży po ich stronie, to oni wybierają sposób i miejsce uderzenia*[4]. Czym jest więc terroryzm?

Nazwa tego zjawiska pochodzi od łacińskiego słowa *terror*, który oznacza strach, grozę. Rozumiany jest także jako: *stosowanie przemocy, gwałtu, ucisku, okrucieństwa w celu zastraszenia, zniszczenia przeciwnika*[5]. Pojęcie terroru zaczęło funkcjonować w kręgu kultury zachodniej w latach Wielkiej Rewolucji Francuskiej. Wtedy powstało pojęcie Wielkiego Terroru, które opisywało twarde rządy Maksymiliana Robespierre'a. Oznaczało ono *bezkompromisową walkę i zastraszanie przez jakobinów wrogów rewolucji przez zmasowane zbrodnie i represje*[6]. Za rządów jakobinów, w latach 1793–1794 ścięto około siedemnastu tysięcy Francuzów. Mówiąc o terroryzmie, za jego umowny początek badacze uznają zdarzenie z 13 lipca 1793 roku, kiedy to żyrondystka, Karilina Corday, zasztyletowała jakobińskiego trybuna Jana Pawła Marata.

Mimo wspólnego źródłosłowu, należy odróżnić terror – jako gwałt i przemoc „silniejszych" organów państwa wobec „słabszych obywateli – od terroryzmu[7], który jest gwałtem i przemocą „słabszych" wobec „silniejszych". W odniesieniu do zjawiska terroryzmu to rozgraniczenie, co do zasady funkcjonowania, nie budzi wątpliwości. Gorzej ze zdefiniowaniem samego terroryzmu. Obecnie istnieje ponad 200 definicji tego zjawiska.

Według najbardziej dostępnej definicji, w Encyklopedii PWN, terroryzm [łac.] to: *różnie umotywowane, najczęściej ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, podejmowane z naruszeniem istniejącego prawa w celu wymuszenia od władz państwowych i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych; działania te są realizowane z całą bezwzględnością, za pomocą różnych środków (nacisk psychiczny, przemoc fizyczna, użycie broni i ładunków wybuchowych), w warunkach specjalnie nadanego im rozgłosu i celowo wytworzonego w społeczeństwie lęku*[8].

---

[4] D. Duda, *Nowa wojna z terroryzmem*, [w:] A. Parzymies (red.) *Islam a terroryzm*, DIALOG, Warszawa 2003, s. 263.

[5] https://encyklopedia.pwn.pl/szukaj/terror.html [dostęp: 23.03.2019].

[6] Por. J. Tomasiewicz, *Terroryzm*, APIS, Katowice 2000, s. 11.

[7] Termin terroryzm wywodzi się z języka greckiego: greckie treo – znaczy „drżeć, bać się", „stchórzyć, uciec", za: E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2011, s. 137.

[8] https://encyklopedia.pwn.pl/szukaj/terroryzm.html [dostęp: 23.03.2019].

Marek Madej podaje zbliżoną definicję, w której terroryzm definiuje jako: *służącą realizacji jakiegoś programu politycznego przemoc lub groźbę jej użycia ze strony podmiotów niepaństwowych (sub- lub transnarodowych), która ma wzbudzić strach w grupie szerszej niż bezpośrednio atakowana i przez taką presję skłonić poddane jej rządy do ustępstw lub też doprowadzić do zniszczenia dotychczasowego porządku politycznego*[9]. W kolejnej grupie definicji, oprócz politycznej natury terroryzmu, podkreśla się jego psychologiczny charakter. Według Alexa Schmida i Jannego de Graafa *bezpośrednia ofiara jest jedynie instrumentem, skórą na bębnie, w który uderza się, chcąc osiągnąć wykalkulowany wpływ na szersze audytorium, Jako taki, akt terroryzmu jest w rzeczywistości aktem komunikacji*[10].

Stanisław Koziej zwraca uwagę na międzynarodowy charakter terroryzmu, czyli jego globalny zasięg. Uważa, że istotą terroryzmu jest *ostentacyjne i maksymalistyczne (masowe, totalne, nieograniczone), celowe (tj. świadomie zamierzone) atakowanie niewinnych, postronnych (cywilnych) osób i dóbr publicznych (otoczenia) dla pośredniego (asymetrycznego, poprzez opinię publiczną) oddziaływania na rzeczywistego przeciwnika politycznego lub ideologicznego*[11].

W związku z globalnym charakterem terroryzmu, w przestrzeni międzynarodowej również powstało wiele definicji dotyczących terroryzmu. NATO definiuje terroryzm, jako *bezprawne użycie lub zagrożenie użyciem siły lub przemocy przeciwko jednostce lub własności w zamiarze wymuszenia lub zastraszenia rządów lub społeczeństw dla osiągnięcia celów politycznych, religijnych lub ideologicznych*[12].

Dla Federalnego Biura Śledczego FBI: *Terroryzm to bezprawne użycie siły lub przemocy wobec osób lub mienia, aby zastraszyć lub wymusić na rządzie lub społeczeństwie zapewnienie realizacji określonych politycznych bądź społecznych celów*[13]. Jednak już według CIA, oprócz bezprawnego użycia siły i próby wymuszenia na rządzie bądź społeczeństwie realizacji żądań terrorystów, akcje te musza być zaplanowane i motywowane politycznie. *Skierowane przeciwko celom niemilitarnym przez*

---

[9] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa 2007, s. 134.

[10] W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm, globalne wyzwanie*, PWN, Warszawa 2009, s. 29.

[11] S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, wyd. Adam Marszałek, Toruń 2008, s. 31.

[12] https://www.nato.int/cps/en/natohq/topics_69482.htm?selectedLocale=en [dostęp: 28.03.2019].

[13] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 20.

subpaństwowe grupy lub tajnych agentów zwykle mającą na celu zwrócenie uwagi społeczności na ich żądania[14].

Własną definicję terroryzmu zaproponowała też Komisja Europejska. Według niej, przestępstwa terrorystyczne, to przestępstwa popełniane z premedytacją przez pojedyncze osoby lub grupy przeciwko jednemu lub większej liczbie krajów, ich instytucjom lub obywatelom, w celu zastraszania ich i poważnej zmiany lub zniszczenia politycznych, gospodarczych lub społecznych struktur krajów. Unia Europejska rozszerza katalog osób odpowiedzialnych. Są to nie tylko zamachowcy, ale również wszyscy ci, którzy umożliwiają im ten proceder. Należy wymienić tu ich zleceniodawców, osoby zajmujące się zdobywanie środków finansowych na działalność terrorystyczną. Do prawodawstwa Unii Europejskiej wprowadzono m.in. trzy nowe przestępstwa:

- publiczne nawoływanie do popełniania przestępstw terrorystycznych,
- rekrutacja na potrzeby terroryzmu,
- szkolenie terrorystyczne[15].

Tomasz Bolechów proponuje zawężenie definicji organizacji terrorystycznej i proponuje, aby określać tym mianem te, dla których działalność terrorystyczna stanowi podstawową metodę działania. Podkreśla jednocześnie znaczenie aktu terrorystycznego jako komunikatu. *Terroryzm, to wywołująca lęk metoda powtarzalnych aktów przemocy, motywowana politycznie, stosowana przeciwko celom niewalczącym, gdzie, w odróżnieniu od innych form przemocy politycznej, bezpośredni cel ataku nie jest celem głównym. Cele bezpośrednie wybierane są losowo bądź selektywnie i służą jako generatory komunikatów*[16].

Bez względu na to, czy mamy do czynienia z terroryzmem etnonacjonalistycznym, separatystycznym, religijnym czy sponsorowanym przez państwo, dla wszystkich charakterystyczne są zjawiska usystematyzowane przez Bruce'a Hoffmana i Alexa Schmida czyli:

– stosowanie przemocy, siły lub groźby ich użycia,
– polityczną motywację sprawców,
– działanie w celu wywołania strachu,
– chęć wywołania psychologicznych skutków i reakcji,
– rozróżnienie celu zamachu i bezpośredniej ofiary,
– celowość i planowanie działań,
– metoda walki,

---

[14] Tamże, s. 20.

[15] Decyzja ramowa Komisji Europejskiej zmieniająca decyzję ramową 2002/475 w sprawie zwalczania terroryzmu (*15139/08* i *8807/08*).

[16] B. Bolechów, op.cit., s. 9.

– konflikt z obowiązującymi regułami zachowań społecznych,
– wymuszenia,
– wykorzystywanie mediów w celu poszukiwania rozgłosu,
– zbrodnia ślepa (przypadkowy dobór ofiar),
– wykorzystywanie symboliki,
– nieobliczalność działań sprawców,
– ukryty charakter organizacji stosującej metody terrorystyczne[17].

Wszystkie przytoczone definicje wskazują też, że podstawowy cel terrorystów pozostaje bez zmian i jest to wywołanie określonego efektu politycznego wyrażonego w określonym działaniu. T.R. Aleksandrowicz podkreśla, że terroryzm jest teatrem dla efektu, a nie dla wyniku i zwraca uwagę na rozwojowy charakter terroryzmu. *Jak wszystkie zjawiska polityczne i społeczne, tak i terroryzm jest kategorią historyczną, a więc zmienną w czasie*[18]. Oznacza to, że organizacje te ewoluują dostosowując się do nowych okoliczności i jednocześnie wykorzystując możliwości jakie daje np. globalizacja czy nowe technologie, za pomocą których mogą dotrzeć do szerokiej międzynarodowej opinii publicznej. Mass media stały się łatwym do wykorzystania i bardzo efektywnym narzędziem do prowadzenia m.in. wojny psychologicznej przez przekazywanie fałszywych albo sprzecznych informacji. To bardzo łatwe narzędzie do siania lęku wśród odbiorców, przez publikowanie drastycznych zdjęć, filmów i oświadczeń. Warto podkreślić, że narzędzie to wykorzystują obie strony wojny z terroryzmem.

Informacja jako siła i zagrożenie

Informacja jest dziś najcenniejszym towarem. XXI wiek nazywany jest erą informacji, a globalne społeczeństwo poprzedza przymiotnik informacyjne. *Informacja jest zatem traktowana jako zasób strategiczny – posiada ona swoją wartość, jej zdobycie i wykorzystanie pociąga za sobą określone koszty, zaś jej brak oznacza brak skuteczności w działaniu*[19].

Norbert Wiener, ojciec cybernetyki, informację definiuje jako *nazwę treści zaczerpniętej ze świata zewnętrznego, w miarę jak przystosowujemy do niego swoje*

[17] W. Dietl, K. Hirschmann, R. Tophoven, op.cit., s. 12.

[18] *Zarządzanie informacją i energią w systemie bezpieczeństwa Unii Europejskiej*, Wyższa Szkoła Gospodarki Euroregionalnej, Józefów 2010; Aleksandrowicz T.R., *Terroryzm jako walka informacyjna*, s. 343.

[19] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Difin, Warszawa 2013, s. 9.

zmysły, przy założeniu, że *proces otrzymywania i wykorzystywania informacji jest procesem naszego dostosowywania się do różnych ewentualności środowiska zewnętrznego oraz naszego czynnego życia w tym środowisku*[20]. Z badań IDC Degital Universe „Extracting Value from Chaos" wykonanych na zlecenie EMC Corporation wynika, że co dwa lata liczba informacji powiększa się dwukrotnie. Autorzy raportu prognozowali na 2011 roku utworzenie i zreplikowanie 1,8 zettabajtów, a w 2020 przedsiębiorstwa będą zarządzać 50-krotnie większą ilością danych[21]. Liczba danych w Internecie rośnie bardzo szybko, do 2020 roku będzie ich 45 zettabajtów – wskazuje w rozmowie z agencją informacyjną Newseria Biznes Maciej Sawa, ekspert Cloud Technologies. – To są przede wszystkim dane o tym, co użytkownicy robią w Internecie, o ich intencjach zakupowych i zainteresowaniach[22].

Aby spróbować zobrazować, jaką potęgę stanowi 45 zettabajtów, wyobraźmy sobie: 500 000 000 000 dwugodzinnych filmów HD, na obejrzenie których potrzebnych jest 1 175 000 000 lat, bądź taka ilość informacji zapełniłaby 1 437 500 000 000 urządzeń Apple iPad z pamięcią 32 GB[23].

Ilość informacji przyrasta w lawinowym tempie. Już teraz obywatel rozwiniętego kraju dostaje taką dawkę informacji, jaką poprzedzające go dwa pokolenia przez całe życie[24]. *O tempie rozwoju Sieci świadczy m.in. to, iż osiągnięcie 50 milionów użytkowników przez tylko jeden Internetowy serwis Facebook trwało zaledwie dwa lata. Popularność tę radio uzyskało po 38 latach, telewizja po 13, a Internet po 4 latach. Z badań wynika, że 40% ludzi na ziemi ma dostęp do Internetu. To ponad 3 mld*[25]. Warto też zauważyć, że według szacunków z Internetu korzysta ok. 157 milionów Arabów, czyli 45% ogólnej populacji[26].

---

[20] Za: R. Kwećka, *Bezpieczeństwo informacyjne*, s. 399, [w:] *Podstawy bezpieczeństwa narodowego (państwa)*, J. Pawłowski (red.), Akademia Sztuki Wojennej, Warszawa 2017.

[21] Za: https://www.microsofttranslator.com/bv.aspx?dl=pl&mkt=pl-PL&ref=SERP&refd=www.bing.com&r=true&a=https%3A%2F%2Fwww.slideshare.net%2Fllevine%2Fidc-report-extractingvaluefromchaos [dostęp: 21.05.2018].

[22] https://biznes.newseria.pl/news/na-swiecie-w-2020-roku,p1905167266 [dostęp: 21.05.2018].

[23] Opracowanie własne za: https://poland.emc.com/about/news/press/2011/20110628-01.htm [dostęp: 21.05.2018].

[24] Za T.R. Aleksandrowicz, *Analityk informacji w administracji rządowej*, s. 13, [w:] *Analiza Informacji w zarządzaniu bezpieczeństwem*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Difin, Warszawa 2013.

[25] http://antyweb.pl/40-ludzi-na-swiecie-korzysta-z-internetu-duzo-malo/ [dostęp: 21.05.2018].

[26] Z. Sawicka, *Wpływ nowych mediów na przemiany polityczne wybranych państw Bliskiego Wschodu na przykładzie Arabskiej Wiosny*, Wyższa Szkoła Informatyki i Zarządzania

Jak dowodzi Włodzimierz Gogołek, jednym z największych problemów rozwoju Internetu i lawinowego przyrostu informacji jest możliwość manipulacji nimi. Jak zauważa – wiadomości rozprzestrzeniają się zbyt szybko, by móc na nie skutecznie reagować[27]. Na co dzień, wielu z nas nie zdaje sobie sprawę, że decyzje które podejmujemy są efektem przetworzonej przez nas, określonej porcji informacji. W zależności od tego, w jakim stopniu wiadomości te są kompletne, podejmujemy bardziej lub mniej prawidłową decyzję. Również na bazie informacji, wyrabiamy opinie i sondy. Jedne postawy oceniamy pozytywnie, inne odrzucamy, uznając za niedopuszczalne. *Decyzja zostaje podjęta intuicyjnie w oparciu o funkcjonujące w podświadomości mechanizmy wypracowane w wyniku uprzednich doświadczeń lub zdobytej wiedzy teoretycznej*[28]. Widać więc, że informacja spełnia wiele funkcji. Najczęściej informacja opisywana jest przez cztery funkcje: informacyjną, decyzyjną, sterowalnością i konsumpcyjną.

Funkcja informacyjna opisywana jest jako odwzorowywanie rzeczywistości, a także daje możliwość poszerzania naszego zasobu wiedzy. Decyzyjna z kolei polega na dostarczaniu informacji, na podstawie których podejmowane są decyzje. Funkcja sterująca to między innymi wywoływanie u odbiorcy określonego zachowania. Olesiński dowodzi, iż *nadawca wiadomości określa odbiorców i kanał informacyjny*. (…) *Dla nadawcy wiadomość jest instrumentem sterowania odbiorcą, dla odbiorcy wiadomość może być postrzegana w różny sposób; jako narzędzie sterowania, jako poszerzenie zasobów wiedzy, jako informacja wspomagająca podjęcie decyzji*[29]. Ostatnią omawianą przez Olesińskiego funkcją jest funkcja konsumpcyjna. Oznacza to, że informacja jest towarem.

Jak łatwo zniekształcić odbiór rzeczywistość za pomocą narracji, dowodzi przykład słuchowiska radiowego Orsona Wellesa z 1938 roku, pod tytułem „Wojna światów", nadanego w CBS. Była to opowieść science fiction o inwazji Marsjan na Ziemię. Na potrzeby audycji radiowej, miejsce ataku zmieniono z Wielkiej Brytanii na New Jersey. Słuchowisko rozpoczęło się o 20.00, ale w tym czasie większość odbiorców słuchała radia NBC, gdzie do 20.12 trwał popularny skecz brzuchomówcy. Kiedy więc odbiorcy przełączyli się na CBS, słuchowisko trwało już kilkanaście minut. Usłyszeli wtedy m.in. o meteorycie, który uderza w ziemię i lądujących Marsjanach. Wielu słuchaczy uznało tę historię za prawdziwe informacje. Wywołało to

---

z siedzibą w Rzeszowie, s. 55–56.

[27] W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, wyd. Oficyna Wydawnicza ASPRA-JR, Warszawa 2010, s. 233.

[28] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011, s. 13.

[29] K. Liedel, T. Serafin, op.cit., s. 37–39.

panikę wśród mieszkańców New Jersey. Gdy informacja o panującej histerii dotarła do CBS, prowadzący przypomniał, że to tylko słuchowisko. Niektóre źródła mówiły o setkach tysięcy, a nawet milionie osób, które wpadły w panikę. *Niezależnie od rzeczywistej skali słynne już słuchowisko pokazało, że za pomocą odpowiedniej narracji można istotnie zniekształcić rzeczywistość i sprawić, że ludzie uwierzą w fikcję*[30].

Roman Kwećka również zauważa, że niekontrolowany przepływ informacji może prowadzić do potęgowania chaosu informacyjnego czy manipulowania informacją. *Oznacza to, że procesy informacyjne lub pochodne ich funkcji są czynnikami decydującymi o wszelkich stanach, zjawiskach i procesach w globalnej przestrzeni bezpieczeństwa*[31]. Już teraz nie ma urządzenia, ani instytucji, która potrafiłaby przeanalizować wszystkie pojawiające się informacje. Sprawdzić, które są prawdziwe i wartościowe, a które nie. To jest przyczyną kolejnego groźnego zjawiska, zwanego szumem informacyjnym. Jak zauważa Aleksandrowicz, zasoby informacyjne przypominają śmietnik, w którym można znaleźć użyteczne informacje, ale wyłuskanie ich wymaga pewnych umiejętności. *Taka sytuacja otwiera pole manipulowania informacją, stosowania dezinformacji czy innych technik socjotechnicznych*[32].

Wśród technik manipulacyjnych, które wpływają na zachowania społeczeństw bądź wybranych grup, wymienić należy propagandę, dezinformację, postprawdę, fake news. Przez propagandę należy rozumieć taki sposób wpływania na zachowania ludzi, w którym osoba lub grupa poddawana wpływowi, nie zdaje sobie sprawy z istnienia takiego mechanizmu[33]. Ważne jest, że manipulacja taka, jest zawsze procesem świadomym, z precyzyjnie określonymi celami. Kolejnym narzędziem wpływania na inżynierię społeczną jest dezinformacja. Według jednej z definicji dezinformacja to *sfabrykowane świadectwa, taktyka oczerniania*[34]. Celem jej jest dyskredytacja przeciwnika. Natomiast definicja znajdująca się w Wielkiej Encyklopedii Radzieckiej określa dezinformacje jako rozpowszechnianie, za pomocą mediów, fałszywych wiadomości w celu wprowadzenia w błąd opinii publicznej[35].

---

[30] I. Urych, M. Gmurek, *Społeczne uwarunkowania bezpieczeństwa. Wybrane zagadnienia psychologii i socjologii, cz. 2*, Akademia Sztuki Wojennej, Warszawa 2016, s. 62.

[31] R. Kwećka, *Bezpieczeństwo informacyjne*, s. 394, [w:] J. Pawłowski (red.), *Podstawy bezpieczeństwa narodowego (państwa)*, Akademia Sztuki Wojennej, Warszawa 2017.

[32] Zarządzanie informacją i energią w systemie bezpieczeństwa Unii Europejskiej; T.R. Aleksandrowicz, *Terroryzm jako walka informacyjna*, s. 344.

[33] Więcej: *Popularna encyklopedia mass mediów*, red. J. Skrzypczak, Wydawnictwo Kurpisz, Poznań 1999, s. 302, 315–317.

[34] R. Deacon, *Spyclopaedia*, London, Futura, 1987, s. 400.

[35] Zobacz: R. Brzeski, *Wojna informacyjna – wojna nowej generacji*, Antyk, Komorów 2014, s. 104.

Kolejnym terminem opisującym techniki manipulacyjne jest pojęcie postprawda, który w 2016 roku został wybrany najpopularniejszym słowem roku. Oxford Dictionary wskazuje, że termin ten odnosi się do okoliczności, w których fakty mają mniejsze znaczenie niż emocje i osobiste przekonania[36]. Według Mirosława Lakomego postprawda to *konstrukt rzeczywistości fabrykowany dla osiągnięcia zakamuflowanych celów*[37]. Celów, które stawia sobie decydent. Oczywiście jednostki, grupy bądź całe społeczeństwa nie zdają sobie sprawy ani z wywieranego wpływu ani z celów, które mają być osiągnięte. Nie znają też decydenta. Kolejnym terminem związanym z technikami manipulacyjnymi jest fake news. Hunt Allcott i Matthew Gentzkow opisują go jako intencjonalne i weryfikowalnie fałszywe artykuły informacyjne[38]. Twórcy raportu Fake news, czyli jak kłamstwo rządzi światem przyjmują, że fake news to *informacja opublikowana przez media, sprawiająca wrażenie zweryfikowanej oraz opisującej fakty, która w rzeczywistości wprowadza opinię publiczną w błąd, uwiarygadniając zawarte w niej niepotwierdzone informacje, dane oraz niezweryfikowane źródła*[39]. Alexander Sängerlaub natomiast stawia na równi fake newsy z dezinformacją i zwraca uwagę, że mogą one dotyczyć najbardziej wrażliwych obszarów, także tożsamościowych.

Głównym nośnikiem fake newsów w Internecie są media społecznościowe. W sierpniu 2017 roku naukowcy z Indiana University w Bloomington, którzy przeprowadzili pierwsze systematyczne badanie rozpowszechniania fałszywych informacji na Twitterze dowiedli, że boty – zautomatyzowane konta zaprogramowane na rozpowszechnianie fałszywych informacji, pełnią ważną rolę w rozsiewaniu nieprawdziwych informacji.

Naukowcy przeanalizowali strony niezależnych organizacji, które zajmują się wyszukiwaniem fałszywych informacji w Internecie. Na stronach snopes.com,

---

[36] https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016, …*Word of the Year 2016 is post-truth – an adjective defined as 'relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief*' [dostęp: 7.11.2018].

[37] M. Lakomy, *Postprawda w dyskursie publicznym. Wprowadzenie*, [w:] *Postprawda jako zagrożenie dla dyskursu publicznego*, red. W. Grabowski, M. Lakomy, K. Oświecimski, Kraków 2018, s. 9.

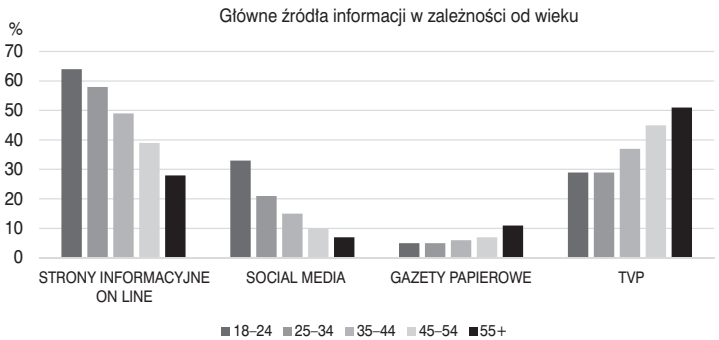
[38] „We define fake news to be stories that were circulated during the election which have been determined to be unambiguously false", za: M. Gentzkow, *The fake news problem isn't nearly as bad as you might* think, wywiad dotyczył badania H. Allcott, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, https://www.vox.com/conversations/2017/1/27/14266228/donald-trump-hillary-clinton-fake-news-media-2016-election [dostęp: 8.11.2018].

[39] https://biznes.newseria.pl/files/raport-fake-news-newseria.pdf [dostęp: 22.05. 2018].

polirifact.com i factcheck.org wyselekcjonowali 122 witryny, które podają fałszywe informacje. Należą do nich infowars.com, breitbart.com, poliricususa.com, theonion.com. Uwagę należy zwracać również na portale określające się mianem satyrycznych, ponieważ duży procent fałszywych informacji w sieci ma właśnie tam swoje źródło.

Po wyselekcjonowaniu odpowiednich witryn uczeni monitorowali 400 000 zgłoszeń i analizowali w jaki sposób się rozprzestrzeniają. W ciągu tego procesu zebrali około 14 milionów postów na Twitterze, które wspomniały o obserwowanych zgłoszeniach. Uzyskane wyniki badacze porównali z kontami na Twitterze, które rozpowszechniały obserwowane informacje. Okazało się, że boty są dużo wydajniejsze w rozprzestrzenianiu fałszywych wiadomości. Dzieje się tak dlatego, że kierują je do najbardziej wpływowych użytkowników, którzy z kolei, często nieświadomie, rozprzestrzeniają je dalej[40].

Według Reuters Digital News Report 2017 Internet, obok telewizji, jest podstawowym źródłem pozyskiwania informacji (rys. 1). Najwięcej użytkowników sieci to ludzie młodzi, do 44 roku życia. W tego samego raportu wynika, że szczególnie młodzi odbiorcy – 33% osób między 18–24 rokiem życia, 21% między 25–34 rokiem życia informacje czerpie z portali społecznościowych.

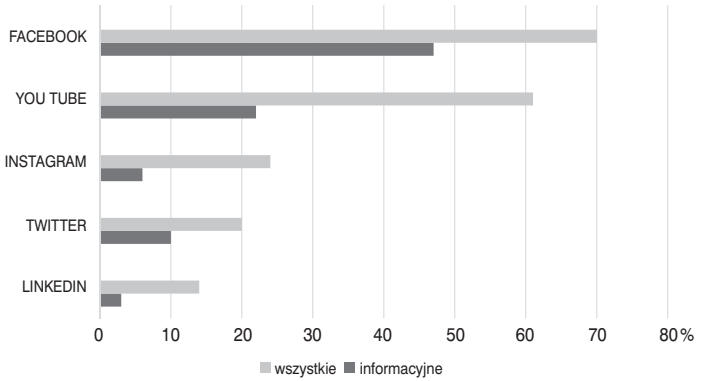


Rysunek 1. Główne źródła pozyskiwania informacji przez odbiorców

Źródło: opracowanie własne za Reuters Digital News Report 2017; http://www.digitalnewsreport.org/survey/2017/overview-key-findings-2017/ [dostęp: 22.05.2018].

[40] https://www.technologyreview.com/s/608561/first-evidence-that-social-bots-play-a-major-role-in-spreading-fake-news/ [dostęp: 22.05.2018].

Z badań wynika również, że najpopularniejszym portalem na świecie jest Facebook (rys. 2). Zarówno jeżeli chodzi o platformę jako źródło informacji (wybiera go 47% użytkowników portali społecznościowych) oraz jako miejsce funkcjonowania w Internecie (wybiera go 70% użytkowników portali społecznościowych). Na drugim miejscu uplasował się YouTube, odpowiednio z 22% i 61%. Trzecie miejsce zajmuje Instagram z 6% i 24%. Na czwartym miejscu uplasował się Twitter z 10% i 20%, a na piątym LinkedIn z zaledwie 3% i 14%.



Rysunek 2. Najpopularniejsze portale społecznościowe

Źródło: opracowanie własne za Reuters Digital News Report 2017; http://www.digitalnewsreport.org/survey/2017/overview-key-findings-2017/ [dostęp: 22.05.2018].

Jak wynika z raportu „Fake news, czyli jak kłamstwo rządzi światem" w mediach społecznościowych nie istnieją żadne mechanizmy kontroli, które chroniłyby te przestrzenie przed szerzeniem się fałszywych informacji. Temu zjawisku sprzyja również postawa użytkowników serwisów. Bombardowani tysiącami informacji nie przywiązują wagi do nich, które pobieżnie przeglądają. *W przypadku Fecebooka problemem jest także działanie algorytmów, których zadaniem jest dobieranie treści atrakcyjnych dla użytkowników. A dla czytelnika najbardziej atrakcyjne są te materiały, które są zgodne z jego poglądami*[41]. Na Twitterze, który w pierwszym kwartale 2017 roku miał 328 milionów aktywnych użytkowników, szerzenie fałszywych informacji odbywa się często za pomocą fałszywych kont prowadzonych przez ludzi lub boty. W sieci działają też serwisy, które wykonują fałszywe zrzuty ekranowe, posty

[41] https://biznes.newseria.pl/files/raport-fake-news-newseria.pdf [dostęp: 22.05. 2018].

i tweety. Fake news szerzy się również przez łańcuchy powołujących się na siebie serwisów. Niektóry z nich przypominają serwisy poważanych instytucji. Można poznać je po tym, że mają bardzo podobne adresy. Różnią się jedną czasem kilkoma literami. Algorytmy decydują jaką informacje i gdzie zobaczymy. Wśród narzędzi wzmacniających siłę przekazu należy wymienić również tzw. roje informacyjne – *sieć powiązanych ze sobą serwisów informacyjnych, blogów agencji informacyjnych, stron think-tanków i (często fałszywych) kont w mediach społecznościowych*. (…) *badacz tematu Christopher Lawrence odkrył na Twitterze sieć* ***17 tysięcy*** *powiązań*[42].

Nowe technologie a grupy terrorystyczne

W 2008 roku Narodowa Rada Wywiadu USA, która przygotowywała raport „Global Trends 2025: A Transformed World" zauważyła, że najniebezpieczniejszą bronią organizacji terrorystycznych około 2025 roku będzie rozpowszechnianie się wiedzy technologicznej i naukowej[43]. Rosnące znaczenie technologii informacyjnej, jako warunku rozwoju nowoczesnych systemów broni, uczyni samą informację podstawowym celem w czasie przyszłych konfliktów[44].

Już teraz jednym z głównych środowisk aktywności organizacji terrorystycznych i samotnych wilków jest Internet. To, dla fundamentalistów, doskonała platforma do prowadzenia działalności. Po pierwsze – kiedy jest taka potrzeba – można być w sieci anonimowym, po drugie – w zasięgu nadawców informacji są miliony odbiorców. *Właściwie to Internet stał się tym najważniejszym narzędziem do komunikacji zwrotnej, które dawało odbiorcy możliwości kontaktowania się z nadawcą, a także tworzenia swojego własnego źródła informacji*[45]. Grupy terrorystyczne regularnie korzystają z nowych technologii. Oprócz Internetu należy wymienić: pocztę elektroniczną, telewizję satelitarną, telefonię komórkową z obrazem i dźwiękiem. Za pomocą nowych środków przekazu promują swoją działalność, ideologię, zdobywają sponsorów, kolejnych zwolenników, a nawet członków. Marek Madej za najważniejszą cechę tego typu działalności uznaje możliwość całkowitej kontroli publikowanych treści i ich formy. Istotna jest również aterytorialność Internetu i możliwość dotarcia z przekazem do każdego zakątka na ziemi. Nawet, mimo ogra-

[42] https://biznes.newseria.pl/files/raport-fake-news-newseria.pdf [dostęp: 22.05.2018].

[43] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf, s. IX [dostęp: 22.05.2018].

[44] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf, s. 71 [dostęp: 22.05.2018].

[45] K. Liedel, T. Serafin, op.cit., s. 14.

niczeń jurysdykcyjnych. Wystarczy umieścić stronę organizacji, uznawanej w danym kraju za nielegalną, na serwerze, który zabroniony nie jest. Nie spowoduje to reakcji organów ścigania[46]. *Najbardziej przełomowe zmiany w technikach komunikacyjnych przypadły mniej więcej na połowę lat 90., lecz już relacje telewizyjne z porwań samolotów z końcem lat 60. i na początku 70. Podobnie przyczyniły się do zwrócenia uwagi świata na palestyńskich terrorystów, zwielokrotniając doniosłość przeprowadzanych przez nich działań*[47].

Rozwój i nieograniczony dostęp do Internetu spowodował, że każdy, anonimowo bądź nie, może być twórcą informacji. Może też rozpowszechnić ją pośród nieograniczonej liczby użytkowników sieci. Jeżeli taka jest wola nadawcy informacji, może ona trafić tylko do określonej grupy odbiorców, do wydzielonych środowisk zbudowanych wokół określonych problemów czy obejmujących określone regiony (m.in. portale społecznościowe czy blogi). Należy zauważyć, że rozwój technologiczny ciągle postępuje. Wciąż będzie również rosła liczba dostarczanych nam informacji. *O tyle będą one miały znaczenie, o ile ich posiadanie będzie wiązało się z zaspakajaniem ludzkich potrzeb, tak tych pozytywnych, jak i negatywnych*[48].

Sposoby walki z organizacjami terrorystycznymi

Głównym komponentem walki informacyjnej jest oczywiście informacja. Nigdy dotąd dostęp do niej nie był tak łatwy jak obecnie. Każdy może być jej odbiorcą i twórcą. Jak już zauważono, Internet, który w założeniach miał być sferą wolności, stał się globalnym śmietniskiem. Można w nim znaleźć więcej informacji o wątpliwej jakości niż tych prawdziwych, rzetelnie opisujących stany, zjawiska, wydarzenia, świat.

Już sześć tysięcy lat temu, wybitny strateg Sun Tzu, opisując strategie prowadzenia wojen, ogromną wagę przywiązywał do zdobywania informacji i używania podstępu, w stosunku do przeciwnika. Wielki mistrz pouczał: *Wojna jest to Tao wprowadzania w błąd*[49]. W traktacie Sun Tzu przekonuje, że należy zdezorientować, zmanipulować przeciwnika przez dostarczanie mu błędnych informacji, stwarzanie pozorów, stosowanie sztuczek i forteli.

Obecnie nie istnieje jedna definicja walki informacyjnej. Marek Madej proponuje rozpatrywanie jej w dwóch ujęciach: szerokim (inkluzywnym) i wąskim

[46] M. Madej, op.cit., s. 336–337.

[47] P.D. Williams, op.cit., s. 177.

[48] K. Liedel, T. Serafin, op.cit., s. 36.

[49] Sun Tzu, Sun Pin, *Sztuka wojny*, wyd. HELION, Gliwice 2008, s. 45.

(ekskluzywnym). W ujęciu inkluzywnym proponuje zdefiniować walkę informacyjną jako całość poczynań rozmaitych uczestników danego konfliktu zmierzających do uzyskania kontroli nad treścią, przepływem i dostępnością istotnych informacji. Jak tłumaczy: chodzi o różnego typu działania, mające na celu zniszczenie, modyfikację (zafałszowanie, uszkodzenie) lub dobycie i wykorzystanie posiadanych przez przeciwnika zasobów informacji oraz systemów ich przechowywania, przetwarzania i przesyłania, jak również ochronę własnych zasobów informacyjnych[50]. W ujęciu wąskim walka informacyjna ograniczona jest do działań przy użyciu technologii informatycznych i powstałych w wyniku rozwoju tych technologii – powiązań o charakterze wirtualnym. Warto zauważyć, że w ujęciu inkluzywnym, walka informacyjna – choć wywodzi się ze sfery militarnej – ma bardzo szeroko zarysowane ramy obejmujące wiele dziedzin życia społecznego. Od kultury po politykę. Od propagandy po wykradanie danych wrażliwych i fizyczne niszczenie urządzeń. Poza tym, termin walka informacyjna uznawany jest za synonim wojny (walki) cybernetycznej. Jak zastrzega jednak Bolesław Balcerowicz – to pojęcia nietożsame, choć komplementarne[51], bo nie wszystkie przejawy walki informacyjnej muszą mieć odzwierciedlenie w cyberprzestrzeni. Winn Schwartau zdefiniował wojnę informacyjną jako działania 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[52]. Nawet jeśli zniekształcone dane lub zmanipulowana informacja powodują awarie urządzeń i obiektów technicznych, to po to, aby w konsekwencji wpłynąć na psychikę człowieka, także poprzez bodźce fizyczne. Ważną cechą działań w cyberprzestrzeni jest możliwość zachowania anonimowości. Nie mniej ważnymi są: aterytorialność, niskie koszty i możliwość działania w skali globalnej.

Krzysztof Liedel dzieli źródła zagrożeń, występujące w ramach pozamilitarnej walki informacyjnej na:

- systemowe (ustrukturyzowane), czyli państwa, ugrupowania terrorystyczne, zorganizowane grupy przestępcze;
- pospolite (nieustrukturyzowane), czyli pojedynczy hakerzy, przestępcy, wandale, frustracji czy aktywiści[53].

---

[50] M. Madej, op.cit., s. 324.

[51] B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu i wojny*, Scholar, Warszawa 2010, s. 179–180.

[52] Za: K. Liedel, P. Piasecka, T.R. Aleksandrowicz, op.cit., s. 15.

[53] Tamże, s. 22.

Kolejnymi zagadnieniami wiązanymi z wojną informacyjna są operacje psychologiczne i informacyjne. Operacje psychologiczne polegają na wykorzystaniu informacji przeciw ludzkiemu umysłowi. M. Libicki podzielił je na cztery kategorie[54]:

- przeciwko woli narodowej;
- przeciwko dowództwu przeciwnika;
- przeciwko żołnierzom;
- konflikt kulturowy.

Operacje informacyjne *są to działania podjęte w celu wywarcia wpływu na informacje i systemy informacyjne przeciwnika przy jednoczesnej obronie własnych informacji i systemów informacyjnych*[55]. Operacje te dzielą się na ofensywne, których celem jest wpływanie na decydentów przeciwnika i defensywne, których zadaniem jest integrowanie i koordynowanie polityki, procedur, personelu, słowem wszystkich elementów, których mobilizacja jest potrzebna do obrony własnych informacji i systemów informacyjnych.

W literaturze przedmiotu coraz wyraźniej wybrzmiewa stanowisko, że wojna informacyjna, oprócz proponowanych przez W. Schwartaua poziomów: osobistego, korporacyjnego i globalnego, powinna być rozpatrywana na dwóch dodatkowych poziomach: cywilnym i militarnym. *Płaszczyzna cywilna związana jest z faktem, iż oddziaływania w obszarze informacyjnym mają kontekst społeczny*[56].

Jak zauważają Liedel i Serafin, za francuskim pisarzem Vladimirem Volkoffem, każda kampania dezinformacyjna musi mieć chwytliwy temat przewodni. Kolejnymi ważnym elementem są tzw. pudła rezonansowe, czyli ośrodki za pomocą których nieprawdziwe treści będą rozpowszechniane (portale społecznościowe, tweety, blogi, videoblogi, wikisłowniki). Vladimir Volkoff, w swoich rozważaniach, wskazuje również grupę docelową. Jednak jak już wspominano, w przypadku propagandy – nie występuje konkretna grupa docelowa[57]. Ważne, by nieprawdziwa informacja, która ma wzmacniać albo osłabić określoną ideologię, trafiła do jak największej liczby osób.

Do tej pory międzynarodowe środowiska akademickie, analityczne i wojskowe ograniczały się do analiz dotyczących fałszywych kampanii informacyjnych prowa-

---

[54] M. Libicki, *What is Information Warfare?*, National Defense University, Washington D.C. 1995, s. 35.

[55] The Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, https://www.hsdl.org/?view&did=3759, s. I-9 [dostęp: 30.03.2019].

[56] A. Lelonek, *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowania*, Fundacja „Centrum Badań Polska-Ukraina", https://capd.pl/images/dokumenty/05PL_Lelonek.pdf [dostęp: 30.03.2019].

[57] Za: K. Liedel, T. Serafin, op.cit., s. 88.

dzonych przez Rosję. Tymczasem, dezinformacja, a uszczegóławiając – fake news – może stać się skuteczną bronią przeciw terroryzmowi. Obecnie, szczególnie po kilku udanych akcjach uderzenia w samozwańcze Państwo Islamskie fake news'em, kręgi międzynarodowe coraz częściej rozpatrują możliwość wykorzystania kampanii dezinformacyjnych, jako skutecznego narzędzia walki w cyberprzestrzeni.

Informacja jest narzędziem, za pomocą którego mogą być zaspokajane różnego rodzaju potrzeby, w zależności od woli wytwórcy bądź nadawcy informacji. Otwiera to niegraniczoną przestrzeń manipulacji i wpływania na decyzje, a nawet światopogląd użytkowników m.in. Internetu. Proces wpływania na odbiorcę przez publikowanie fake newsów jest analogiczny jak w działaniu dezinformacyjnych na wirtualnym polu walki, którego wynik przekłada się na zyski i straty w rzeczywistości realnej. Jednak o ile *dezinformacja wymaga zidentyfikowania przeciwnika, którego mechanizm analityczny zamierza się wypaczyć*[58] o tyle propaganda kierowana jest często do przypadkowego odbiorcy. Tu chodzi o konsekwencję i aktywność rozumianą jako długotrwałe działanie.

Hakerzy kontra ekstremiści

Należy zauważyć, że w sieci aktywne są wszystkie największe organizacje terrorystyczne, od ISIS przez organizację Al-Kaida po Boko Haram. Walka z nimi, w realnym świecie, wymaga wielu nakładów osobowych, finansowych i nie daje gwarancji sukcesu. Walka w przestrzeni wirtualnej, wymaga zaangażowania nieporównywalnie mniejsze liczby osób i co najważniejsze – nieporównywalnie mniej kosztuje. Poza tym, należy zauważyć, że dobrze przygotowana i przeprowadzona kampania również może przynieść, zaatakowanej stronie, ogromne straty m.in. wizerunkowe. Należy podkreślić jednocześnie, że np. utrata zaufania jest szkodą, którą skompromitowanemu podmiotowi najtrudniej odrobić.

Organizacje terrorystyczne od lat wykorzystują środki technologiczne jako tuby propagandowe. Social media i fora dyskusyjne są dla nich otwartym, nieograniczonym polem dostępu do szerokich mas użytkowników sieci, spośród których pozyskują kolejnych sympatyków, fundatorów, a nawet rekrutów. Ogólnodostępną sieć wykorzystują także do inspirowania osób będących pod wpływem fundamentalistycznej ideologii, zachęcając ich do samobójczych ataków. Powszechnie wiadomo, że w Internecie można znaleźć dokładne instrukcje jak przygotować bombę czy zaplanować i przeprowadzić zamach.

[58] Tamże, s. 85.

Wykorzystując Internet, jako ważną przestrzeń działalności grup terrorystycznych i ich zwolenników, należy szukać nowych rozwiązań, które pozwolą z nimi walczyć również w cyberprzestrzeni. Jak się okazuje, skuteczną bronią przeciwko grupom ekstremistycznym może okazać się fake news.

Do tej pory międzynarodowe środowiska akademickie, analityczne i wojskowe ograniczały się do analiz dotyczących fałszywych kampanii informacyjnych prowadzonych przez Rosję. Obecnie, szczególnie po kilku udanych akcjach uderzenia w samozwańcze Państwo Islamskie za pomocą fake news'ów, kręgi międzynarodowe coraz częściej rozpatrują możliwość wykorzystania kampanii dezinformacyjnych, jako skutecznego narzędzia walki w sieci. To uzupełnienie katalogu metod zwalczania terroryzmu subpaństwowego, oprócz metod tradycyjnych, które polegają na zapewnianiu bezpieczeństwa przez działania policyjne i wywiadowcze czy bezpośrednie działania wojskowe przeprowadzane przeciwko terrorystom. Operacje dezinformacyjne mają na celu uderzenie w najczulszy punkt, członków i zwolenników grup terrorystycznych, jakim jest motywacja. Od niej bowiem zależy między innymi determinacja i wiara w idee przedstawiane przez fundamentalistów. Proces wpływania na odbiorcę przez publikowanie fake news'ów jest analogiczny jak w działaniu dezinformacyjnych na wirtualnym polu walki, którego wynik przekłada się na zyski i straty w rzeczywistości realnej. Jednak o ile *dezinformacja wymaga zidentyfikowania przeciwnika, którego mechanizm analityczny zamierza się wypaczyć*[59] o tyle propaganda kierowana jest często do przypadkowego odbiorcy. Tu chodzi o konsekwencję i aktywność rozumianą jako długotrwałe działanie.

Grupy terrorystyczne od dawna wykorzystują działania dezinformacyjne. Ekstremiści wykorzystują fake newsy do wzmacniania wizerunku oraz zwiększania siły przyciągania nowych zwolenników. Jedną z metod jest branie odpowiedzialności niemal za wszystkie najbardziej spektakularne zamachy, które przyciągają uwagę widzów na całym świecie. Jednym z takich przypadków jest atak w Las Vegas z 1 października 2017 roku. 64-letni emerytowany księgowy otworzył ogień z pokoju na 32 piętrze hotelu Mandalay Bay. Zabił 59 osób, a 546 ranił. Stephen Paddock popełnił samobójstwo. Do zamachu przyznała się ISIS. Dzień po zamachu na stronie agencji informacyjnej współpracującej z ekstremistami z ISIS – Amaq – pojawiło się oświadczenie, w którym fundamentaliści twierdzili, że emerytowany księgowy przeszedł na islam. Śledztwo prowadzone przez amerykańskie służby, nie potwierdziło tych twierdzeń. Okazało się, że sprawca masakry miał problemy psychiczne.

[59] K. Liedel, T. Serafin, op.cit., s. 85.

Działania dezinformacyjne stały się nie tylko dodatkowym narzędziem organizacji terrorystycznych, ale również orężem w walce z nimi. Wykorzystują je między innymi sunnickie grupy hakerów. Głównym celem ich działań jest osłabianie morale i manipulowanie społecznym odbiorem członków organizacji fundamentalistycznych. Tak, aby ich wizerunek zniechęcał do popierania fundamentalistów. Charakterystyczny dla nich hasztag to: #SilenceTheSwords.

13 października 2017 roku jedna z grup sunnickich, o nazwie „Di5s3nSi0N" rozpropagowała w sieci informacje uderzające w ISIS. 25 października 2017 roku organizacja na Twitterze umieściła dwukrotnie ostrzeżenie przed możliwymi atakami na strony ISIS. Doprowadziło to do dezaktywacji strony Amaq. Tymczasem Amaq to agencja informacyjna, która powstała w 2013 roku i od początku istnienia współpracuje z ISIS. Zwykle jako pierwsza zamieszcza oświadczenia organizacji, w których bierze ona na siebie odpowiedzialność za akty terrorystyczne. Po raz kolejny strona Amaq została zhakowana 30 października 2017 roku. 11 listopada na stronie dedykowanej nowym technologiom i wiadomościom dotyczącym włamywania się na strony informowano, że udało się włamać na stronę Amaq i zdobyć szczegółowe informacje dotyczące 1784 użytkowników strony.

17 listopada 2017 roku Di5s3nSi0N umieścił kilka oświadczeń, w których informował, że chce „uciszyć" Amaq. Jesteśmy jak wirus w waszym systemie którego nie można usunąć. Nasza podróż do uciszenia Daesh będzie trwała[60] – w jednym z nich napisali członkowie grupy.

Kolejną grupą walczącą w sieci z ekstremistami jest Daeshgram. Utworzyli ją młodzi hakerzy z Iraku, którzy wykorzystując możliwości jakie daje Internet obracają propagandę ISIS przeciw organizacji. Infiltrują jej kanały informacyjne i rozpowszechniają w nich fałszywe informacje. Głównie na komunikatorze o nazwie Telegram. To kanał preferowany przez członków samozwańczego Państwa Islamskiego, bo bardzo łatwo, poza kontrolą, można na nim założyć konto. Daje to także hakerom większe możliwości tworzenia dużej liczby fałszywych kont i nakierowywanie na nie członków ISIS[61].

Na początku działalności grupa uderzyła w agencję informacyjną Amaq, zalewając ją tak dużą ilością informacji, że strona nie była w stanie ich przerobić. Spowodowało to konieczność przejścia strony na tryb pracy w „trybie offlinie" – atak DDoS. W tym czasie hakerzy podwiązywali linki do fałszywych wersji Amaq. Na

[60] https://www.independent.co.uk/news/world/middle-east/isis-hacked-propaganda-amaq-mailing-list-emails-subscribers-published-islamic-state-online-caliphate-a8049771.html [dostęp: 2.04.2019].

[61] https://news.sky.com/story/meet-daeshgram-the-iraqi-hackers-using-islamic-states-propaganda-against-them-11136026 [dostęp: 22.05.2018].

stronach fałszywej agencji hakerzy informowali między innymi o śmierci bojownika i wyśmiewali ideologię terrorystów.

Jedną z najbardziej spektakularnych akcji przeprowadzonych przez młodych hakerów z Iraku było umieszczenie zdjęć pornograficznych na oficjalnej stronie ISIS. Wywołały one zamieszanie w szeregach terrorystów i ich zwolenników. Ekstremiści nie wiedzieli, w które informacje wierzyć, a w które nie. Czuli się oszukani, manipulowani i podważone zostało ich morale. Według autora artykułu, który ukazał się w stacji sky news, jeden ze zwolenników IS napisał: *Im więcej kanałów i grup utrzymujemy, tym więcej mamy problemów*. Natomiast jeden z członków Daeshgram tak opisywał sposób przygotowania się do akcji dezinformacyjnej przeciw terrorystom: *budowaliśmy wiarygodność w grupach ISIS na Telegramie, rozumiejąc w jaki sposób publikują, czego nie chcą słyszeć, jakie sprawy jak chcą widzieć i jakiego rodzaju treści publikują w swoich grupach*. Głównym celem członków Daeshgram jest unicestwienie ISIS. Organizacji, która dopuszcza się najstraszniejszych okrucieństw, jakie można sobie tylko wyobrazić. Członkami Daeshgram są w większości studenci, dlatego ich aktywność jest determinowana przez kalendarz uniwersytecki. Działalność Daeshgram jest przerywana np. na czas sesji egzaminacyjnych. Wielu bliskich i znajomych młodych hakerów z Iraku zostało zabitych przez członków ISIS, ale aktywiści nie poddają się.

Wśród grup, które za pomocą fake newsów w sieci chce walczyć z ISIS, jest również grupa Anonymous. Jej nadrzędnym celem ich jest zamknięcie kont powiązanych z ISIS. Walka w sieci trwa.

Podsumowanie

Zaprezentowane rozważania pozwalają stwierdzić, że operacje dezinformacyjne są skutecznym narzędziem walki z grupami terrorystycznymi. Jest to możliwe dzięki lawinowemu rozwojowi technologicznemu, który każdemu daje możliwość bezpłatnego i niemal nieograniczonego dostępu do informacji. Każdy użytkownik Internetu może być nie tylko obiorcą publikowanych tam treści, ale również ich nadawcą. Daje to możliwość błyskawicznego rozpowszechniania dowolnych treści w wymiarze globalnym. Do niedawna, z tej możliwości korzystały organizacje terrorystyczne, które używały technik manipulacyjnych, takich jak propaganda czy fake news, w celu wzmacniania siły głoszonej ideologii, zdobywania nowych zwolenników, rekrutacji nowych członków czy zdobywania funduszy. Operacje informacyjne i psychologiczne wykorzystuje też międzynarodowa koalicja walcząca z organizacjami terrorystycznymi. Nowym zjawiskiem jest wykorzystywanie możliwości

wpływania na umysły czytelników przez dystrybuowanie odpowiednich treści przez hakerów-cywilów, próbujących osłabić wpływy terrorystów. Działania te przynoszą wymierne efekty w postaci zamętu wprowadzanego w szeregi nie tylko członków organizacji ekstremistycznych, ale również wśród ich zwolenników. Zjawisko to znalazło się w spektrum zainteresowania badaczy. Należy odpowiedzieć na wiele pytań, m.in. – jakie znaczenie w wojnie informacyjnej odgrywa komponent cywilny? i jakie warunki muszą być spełnione, aby działania prowadzone przez cywilów skuteczniej wspierały działania koalicji?

Bibliografia

Aleksandrowicz T., *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

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

Bolechów B., *Terroryzm – aktorzy, statyści, widownie*, PWN, Warszawa 2010.

Brzeski R., *Wojna informacyjna – wojna nowej generacji*, Antyk, Komorów 2014.

Deacon R., *Spyclopaedia*, London, Futura, 1987.

Dietl W., Hirschmann K., Tophoven R., *Terroryzm, globalne wyzwanie*, PWN, Warszawa 2009.

Duda D., *Nowa wojna z terroryzmem*, [w:] A. Parzymies (red.), „Islam a terroryzm", DIALOG, Warszawa 2003.

Gogołek W., *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, wyd. Oficyna Wydawnicza ASPRA-JR, Warszawa 2010.

Koziej S., *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, wyd. Adam Marszałek, Toruń 2008.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza Informacji w zarządzaniu bezpieczeństwem*, Difin, Warszawa 2013.

Liedel K., Piasecka P., Aleksandrowicz T.R., Analiza informacji. Teoria i praktyka, Difin, Warszawa 2013.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.

Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa 2007.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2011.

Pawłowski J. (red.), *Podstawy bezpieczeństwa narodowego (państwa)*, Akademia Sztuki Wojennej, Warszawa 2017.

Popularna encyklopedia mass mediów, red. J. Skrzypczak, Wydawnictwo Kurpisz, Poznań 1999.

Postprawda jako zagrożenie dla dyskursu publicznego, red. W. Grabowski, M. Lakomy, K. Oświecimski, Kraków 2018.

Sawicka Z., *Wpływ nowych mediów na przemiany polityczne wybranych państw Bliskiego Wschodu na przykładzie Arabskiej Wiosny*, Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie.
Sun Tzu, Sun Pin, *Sztuka wojny*, wyd. HELION, Gliwice 2008.
Tomasiewicz J., *Terroryzm*, APIS, Katowice 2000.
Urych I., Gmurek M., *Społeczne uwarunkowania bezpieczeństwa. Wybrane zagadnienia psychologii i socjologii, cz.2*, Akademia Sztuki Wojennej, Warszawa 2016.
Williams Paul D., Studia bezpieczeństwa, Uniwersytet Jagielloński, Kraków 2012.
Zarządzanie informacją i energią w systemie bezpieczeństwa Unii Europejskiej, Wyższa Szkoła Gospodarki Euroregionalnej, Józefów 2010.

Strony internetowe

http://antyweb.pl/40-ludzi-na-swiecie-korzysta-z-internetu-duzo-malo/
https://biznes.newseria.pl/news/na-swiecie-w-2020-roku,p1905167266
https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016
https://encyklopedia.pwn.pl/szukaj/terror.html
https://encyklopedia.pwn.pl/szukaj/terroryzm.html
https://news.sky.com/story/meet-daeshgram-the-iraqi-hackers-using-islamic-states-propaganda-against-them-11136026
https://poland.emc.com/about/news/press/2011/20110628-01.htm
https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf
https://www.microsofttranslator.com/bv.aspx?dl=pl&mkt=pl-PL&ref=SERP&refd=www.bing.com&r=true&a=https%3A%2F%2Fwww.slideshare.net%2Fllevine%2Fidc-report-extractingvaluefromchaos
https://www.nato.int/cps/en/natohq/topics_69482.htm?selectedLocale=en
https://www.technologyreview.com/s/608561/first-evidence-that-social-bots-play-a-major-role-in-spreading-fake-news/
https://www.vox.com/conversations/2017/1/27/14266228/donald-trump-hillary-clinton-fake-news-media-2016-election

FAKE NEWS AS A WEAPON AGAINST TERRORISM

Keywords: terrorism, Information War, propaganda, fake news

SUMMARY

Counter-terrorism requires continuous responding to enemy's actions. Widespread technological advancement gives extremists new tools that can be used not only to propagate their ideology but also to win new organization members, followers, and sponsors. The Internet has become the main platform to spread out various extremist ideas. Thanks to methodical proliferation

of controlled messages terrorists attempt to change the recipients' awareness, take control over their minds, and, what follows, affect their behaviour. The response of counter-terrorist coalition must be adequate. It involves modern forms of psychological warfare, propaganda, information and disinformation. The coalition is supported by civilian hackers who carried out a number of disinformation operations, which brought about chaos within terrorist organizations. The factoids and fake news provided by them decrease the morale amongst followers of extremist movements, and questioned their values, as well as damaging their interest and intentions. It is therefore worthwhile analysing the meaning of the civil content of Information War, as the phenomenon involving the military component support.