V. BEZPIECZEŃSTWO INFORMACYJNE

POLITYKA INFORMACYJNA A BEZPIECZEŃSTWO INFORMACYJNE

Krzysztof Liderman

Wojskowa Akademia Techniczna

Andrzej Malik

Sztab Generalny WP

Streszczenie. W artykule została przedstawiona problematyka polityki informacyjnej, przede wszystkim w odniesieniu do polityki informacyjnej resortu Obrony Narodowej, ograniczonej specyficznie do treści zamieszczanych w Internecie. Wskazano na możliwości osiągania różnych celów propagandowych poprzez umiejętne manipulowanie atrybutami informacji (rozdz. 2 i 3) oraz na możliwości wykorzystania Internetu w zakresie kształtowania świadomości jego użytkowników (rozdz. 4).

Wstęp

Wspomniana w motcie artykułu „Sieć" to Internet, pod którą to nazwą kryje się zarówno infrastruktura sprzętowa, programowa i obsługujący ją ludzie, jak i olbrzymie, zmienne zasoby informacyjne zgromadzone w urządzeniach pamięciowych wchodzących w skład infrastruktury. Socjolog ten obraz prawdopodobnie dopełniłby ludźmi korzystającymi w różny sposób z tych zasobów, czyli tzw. użytkownikami Internetu.

Niniejszy artykuł jest próbą pokazania możliwych związków pomiędzy działaniami określanymi mianem „polityki informacyjnej" a atrybutami jakości informacji przetwarzanej w Internecie. Przykładową polityką informacyjną, na której te związki będą pokazane, jest polityka informacyjna resortu obrony narodowej ([5], patrz rozdz. 4). Jednak ze względu duże znaczenie (nie tylko zdaniem autorów, patrz np. [7], [8], [12]) dostępu do treści cyfrowych o odpowiedniej jakości, podstawowy opisywany w tym artykule problem zostanie poprzedzony informacjami na temat kryteriów jakości informacji (rozdz. 2), w tym kryterium takim jak „bezpieczeństwo" informacji (rozdz. 3).

Rozwój elektroniki spowodował, że pojawiła się „elektroniczna postać informacji", która może być łatwo i szybko przetwarzana, przesyłana i przechowywana. Do przesyłania takiej informacji służą sieci teleinformacyjne ewoluujące obecnie w kierunku jednej homogenicznej sieci obejmującej cały glob – Internetu; do przetwarzania i przechowywania – węzły sieci z ulokowanymi w nich zasobami przechowującymi

i przetwarzającymi informację (od pojedynczych „domowych" komputerów po centra danych). Z powodu wymienionego w poprzednim zdaniu, ilość dostępnej informacji gwałtownie rośnie i niezbędna staje się jej selekcja i ocena pod względem szeroko rozumianej jakości. Dostęp do dobrej jakościowo informacji we właściwym czasie daje przewagę w wyścigu po dobra materialne, władzę i pieniądze.

Wymienione trzy czynniki, w połączeniu z rozpowszechnieniem urządzeń dostępowych (takich jak telefony komórkowe różnej klasy i typów oraz przenośne komputery typu tablet czy notebook), powstaniem tzw. sieci społecznościowych (Facebook, Twitter itp.) oraz coraz częstszym wykorzystywaniem sieci publicznych jako medium do przesyłania informacji dla systemów przemysłowych spowodowały, że informacja stała się istotnym czynnikiem decydującym nie tylko o wiedzy, władzy czy bogactwie, lecz także o bezpieczeństwie pojedynczych ludzi, organizacji i państw[1]. Dlatego czynione są wysiłki zarówno w skali ponadpaństwowej, jak Unia Europejska, jak i w skali pojedynczych państw, w tym także państwa polskiego [11], opanowania tej swoistej eksplozji informacyjnej tak, aby informację można było skutecznie kontrolować oraz aby zapewnić jej odpowiednią jakość. Osiągnięcie tych celów wymaga skoordynowanych działań legislacyjnych, organizacyjnych i technicznych.

Ważnym dokumentem dotyczącym postępu technologicznego jako takiego, jednak skupiającym się na uzyskaniu trwałych korzyści ekonomicznych i społecznych z jednolitego rynku cyfrowego w oparciu o bardzo szybki Internet, jest *Europejska Agenda Cyfrowa* [7]. Jest to jeden z siedmiu flagowych programów w ramach strategii reform gospodarczych „Europa 2020". Celem Agendy jest wyznaczenie kierunków rozwoju i wskazanie działań w obszarze społeczeństwa informacyjnego, pozwalających na maksymalne wykorzystanie potencjału nowoczesnych technologii informacyjnych i komunikacyjnych, w szczególności Internetu. Agenda wskazuje na ponad sto działań, które prowadzić będą zarówno Komisja Europejska, jak i państwa członkowskie.

Wszystkie te działania z zakresu legislacyjno-organizacyjnego, rozwój technologii oraz zmiany w świadomości społeczeństwa sprawiają, że pojawiło się w obiegu (również tym oficjalnym [12]) określenie „społeczeństwo informacyjne" mające podkreślać rolę informacji w życiu współczesnego człowieka. Dobitnym przykładem realnej siły „społeczeństwa informacyjnego" są wydarzenia z początku 2012 roku mające związek z podpisaniem przez Polskę ACTA (*Anti-Counterfeiting Trade Agreement*), których rozdział 2, sekcja 5: *Dochodzenie i egzekwowanie praw własności intelektualnej w środowisku cyfrowym* dotyczy bezpośrednio działalności szerokiej rzeszy internautów w tzw. środowisku cyfrowym. Warto zauważyć, że „społeczeństwo

[1] Należy jednak pamiętać, że według danych Międzynarodowej Unii Telekomunikacyjnej (ITU) obecnie dostęp do Internetu ma około 30% mieszkańców Ziemi, zatem przytaczane tutaj przyczyny „eksplozji informacyjnej" nie dotyczą przeważającej części ludzkości – ich problemy informacyjne są na innym poziomie.

informacyjne" użyło Internetu (czyli ww. „środowiska cyfrowego") zarówno do organizacji protestów, jak i bezpośrednich ataków na środowisko cyfrowe wybranych agencji rządowych i członków rządu.

1. Kryteria jakości informacji

W dokumentach unijnych podkreśla się znaczenie dostępu do treści cyfrowych (pierwszy obszar strategiczny *Jednolity rynek cyfrowy*, patrz [7]). Jednak w tych dokumentach brakuje odniesienia/zaleceń dotyczących jakości treści udostępnianych w Internecie. A przecież dla spełnienia przez informację roli kluczowego czynnika szeroko rozumianego „sukcesu" we współczesnym świeci podstawowe znaczenie ma jej dobra jakość. Ogólnie uznanymi kryteriami jakości informacji są:

1. *Relewantność* – co oznacza, czy informacja jest istotna dla odbiorcy, związana z tym, czego odbiorca poszukuje.
2. *Dokładność* – oznacza precyzję oraz sposób prezentacji odpowiedni do poziomu wiedzy jej użytkownika.
3. *Aktualność* – oznacza, że informacja jest zmieniana bez opóźnień odpowiednio do zmian przedmiotu opisu.
4. *Kompletność* – oznacza, że jest dostępna w ilości i stopniu szczegółowości zgodnym z wymaganiami jej użytkownika.
5. *Spójność* – oznacza, że poszczególne fragmenty informacji są niesprzeczne, dotyczą zadanego tematu i są prezentowane i przekazywane w jednolitej formie.
6. *Odpowiedniość formy* – oznacza taki sposób prezentacji informacji, który minimalizuje jej błędną interpretację.
7. *Wiarygodność* – oznacza, że zawarte są w niej elementy upewniające co do rzetelności niesionego przez nią przekazu.

Jak widać, ocena jakości informacji bazuje na trzech składowych: treści, formie i użytkowniku informacji. Waga branych pod uwagę kryteriów może się różnić w zależności od dziedziny wykorzystywania informacji: obronność, zarządzanie kryzysowe, finanse, statystyka, prawo, ekonomia itp.

Żeby móc poprawnie ocenić jakość informacji, potrzebna jest dodatkowa informacja ją opisująca[2]. Przykładem takiej „informacji opisującej", która staje się standardem dla informacji umieszczanej w Internecie, są:

Informacje o interesariuszach (ang. *transparency and honesty*) – dane identyfikacyjne dostawców treści, administratorów strony, sponsorów, reklamodawców

[2] Oczywiście, ta informacja też powinna być dobrej jakości – pojawia się tutaj problem „kto kontroluje kontrolera". Przykładem takich „kontrolerów" dla danych są kody detekcyjno-korekcyjne oraz podpis cyfrowy.

itd., a także określenie celów i zamiarów właściciela strony internetowej oraz grupy docelowej, do której skierowana jest zamieszczona na niej informacja.

Informacje uwierzytelniające prezentowane treści (ang. *authority*) – obejmują status wykorzystanych źródeł informacji, dane i rekomendacje o podmiotach opracowujących treści, daty ich dostarczania.

Informacje o stosowanej polityce zachowania prywatności i ochronie danych (ang. *privacy and data protection*) – obejmują wskazanie polityki zabezpieczania własności intelektualnej i prywatności oraz zgodności z obowiązującymi przepisami prawa.

Informacje o aktualności treści (ang. *updating of information*) – dotyczą daty wprowadzenia zmian, w tym uaktualniania linków.

Informacje umożliwiające rozliczalność (ang. *accountability*) – są to dane identyfikacyjne i kontaktowe osób przygotowujących merytoryczną treść strony WWW oraz zasady edytowania stron i doboru materiału.

2. Problem ochrony informacji

Poza wymienionymi w poprzednim rozdziale atrybutami jakości informacji, mając na względzie techniczną stronę jej przesyłania, przechowywania i przetwarzania, wyróżnia się szereg atrybutów związanych z ochroną informacji[3], takich jak:

1. *Tajność* – informuje o wymaganej sile ochrony informacji przed nieuprawnionym dostępem. Wielkość tej siły jest uzgadniana przez osoby lub organizacje dostarczające i otrzymujące informację.
2. *Integralność* – informuje, czy dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji.
3. *Dostępność* – informuje, czy dane, procesy i aplikacje są dostępne zgodnie z wymaganiami użytkownika (lub wymaganiami na system).
4. *Rozliczalność* – informuje o możliwości identyfikacji użytkowników informacji i systemu teleinformatycznego oraz wykorzystywanych przez nich usług. Atrybut ten decyduje także o możliwości prowadzenia skutecznej analizy powłamaniowej.
5. *Niezaprzeczalność* – informuje o możliwości wyparcia się uczestnictwa przez podmiot uczestniczący w wymianie informacji.
6. *Autentyczność* – oznacza możliwość jednoznacznego stwierdzenia, jaki podmiot przesłał dane.

Atrybuty wymienione na tej liście nie zależą wyłącznie od informacji jako takiej, ale również od przyjętych rozwiązań organizacyjnych i technicznych systemu, w jakim są przetwarzane, przechowywane lub przesyłane.

[3] W tym kontekście wymienione atrybuty też można traktować jako atrybuty jakości informacji.

Ze względu na wagę informacji dla współczesnego społeczeństwa, istotnego znaczenia nabiera tzw. *bezpieczeństwo informacyjne*, obejmujące wszystkie formy (także werbalne) wymiany, przechowywania i przetwarzania informacji. Według ogólnie uznanych poglądów (por. np. [1]) bezpieczeństwo informacyjne dotyczy podmiotu (człowieka lub organizacji), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. Zatem bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji.

Z kolei *bezpieczeństwo informacji* oznacza uzasadnione (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufanie, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego): ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie obiegu informacji.

Z przytoczonych definicji wynika, że bezpieczeństwo informacji jest składową bezpieczeństwa informacyjnego – informację trzeba najpierw pozyskać, a potem, w trakcie jej wykorzystywania przez podmiot (przechowywania, przetwarzania, przesyłania), odpowiednio chronić. Można także zauważyć, że „bezpieczeństwo" nie jest ani obiektem, ani zdarzeniem, ani procesem – to imponderabilia z dziedziny psychologii.

Do dalszych rozważań przyjmuje się, że system informacyjny to system przesyłania, przetwarzania i przechowywania informacji (bez względu na jej formę i nośnik). Natomiast system informatyczny[4] to ta część systemu informacyjnego, w której do przesyłania, przetwarzania i przechowywania informacji wykorzystywane są środki techniki komputerowej. Ta definicja obejmuje wszystkie warianty praktycznej realizacji takiego systemu, według różnych klasyfikacji, takich jak sieć komputerowa, system rozproszony, a także przemysłowy system sterowania (ang. ICS – *Industrial Control System*).

Bezpieczeństwo informacyjne jest podstawą szeroko rozumianego bezpieczeństwa, obejmującego bezpieczeństwo militarne, finansowe, energetyczne, socjalne itd., w skali globalnej i pojedynczych państw. Bez zapewnienia bezpieczeństwa informacyjnego osiągnięcie bezpieczeństwa „innoprzymiotnikowego" jest skazane na niepowodzenie. Niestety (patrz np. Wstęp w [2]), bezpieczeństwo informacyjne przez specjalistów z dziedzin bezpieczeństwa „innoprzymiotnikowego", przynajmniej w Polsce, wydaje się być niedostrzegane, a w najlepszym przypadku marginalizowane.

Samo bezpieczeństwo informacyjne, ze względu na coraz większy udział w transmisji, przechowywaniu i przetwarzaniu informacji środków technicznych, jest podatne na różne formy tzw. cyberzagrożeń, w tym tych związanych z działaniami terrorystycznymi[5].

[4] W dalszej części artykułu termin „informatyczny" będzie używany zamiennie z terminem „teleinformatyczny" dla podkreślenia faktu, że obecnie systemy informatyczne są łączone za pomocą sieci telekomunikacyjnych w bardziej złożone struktury.

[5] Zainteresowany Czytelnik więcej informacji na ten temat może znaleźć w [2] i [3].

3. Polityka informacyjna a bezpieczeństwo (nie tylko) informacyjne

Wojskowi działania przeciwnika prowadzone w Internecie i przeciwko Internetowi lokują w grupie tzw. asymetrycznych zagrożeń bezpieczeństwa państwa. Ta kategoria zagrożeń jest zwykle definiowana jako zagrożenia, których celem jest neutralizacja lub likwidacja przewagi militarnej przeciwnika poprzez zastosowanie taktyki i dostępnej broni w niekonwencjonalny sposób, pozwalający na wykorzystanie zarówno słabych punktów przeciwnika, jak i własnej przewagi w jakimś elemencie prowadzonych operacji.

Do takich zagrożeń asymetrycznych należy wojna informacyjna, obejmująca operacje informacyjne INFOPS[6] oraz oddziaływanie psychologiczne PSYOPS[7] (w przypisach dolnych za [15] wyjaśnienie tych skrótów). W dalszej części artykułu możliwości osiągania różnych celów propagandowych poprzez umiejętne manipulowanie atrybutami informacji oraz możliwości wykorzystania Internetu w zakresie kształtowania świadomości jego użytkowników zostaną przedstawione w kontekście polityki informacyjnej resortu obrony narodowej RP.

3.1. Polityka informacyjna i możliwości jej kształtowania w Internecie

Zasady realizacji polityki informacyjnej w resorcie obrony narodowej reguluje decyzja Nr 108 /MON z dnia 7 kwietnia 2009 r. *w sprawie zasad realizacji polityki informacyjnej w resorcie obrony narodowej*[8]. Dokument ten definiuje i reguluje politykę informacyjną resortu, wymienia osoby uprawnione do informowania mediów oraz precyzuje zasady udzielania informacji. Zgodnie z decyzją, **polityka informacyjna to całokształt działań i decyzji resortu, związanych z informowaniem opinii publicznej o sprawach Sił Zbrojnych Rzeczpospolitej Polskiej i obronności oraz kształtowaniem pozytywnego wizerunku Sił Zbrojnych**. Najważniejszym celem polityki informacyjnej jest zaspokojenie potrzeb informacyjnych społeczeństwa oraz pozyskanie zrozumienia i akceptacji społecznej dla celów i działań podejmowanych przez resort. Kierunki polityki informacyjnej określa Minister Obrony Narodowej, a za jej realizację odpowiada Dyrektor Departamentu Prasowo-Informacyjnego[9].

[6] InfoOps: NATO military advice and co-ordination of military information activities in order to create desired effects on the will, understanding, and capabilities of adversaries and other NA-approved parties in support of Alliance operations, missions and objectives.

[7] PsyOps: Planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.

[8] Dz.Urz. MON Nr 7, poz. 82 oraz z 2011 r. Nr 2, poz. 25.

[9] Za materiałami zamieszczonymi na stronie www.mon.gov.pl.

Z punktu widzenia tematyki tego artykułu, istotne są paragrafy 31-33 ww. Decyzji:

„31. Najważniejsze informacje dotyczące resortu publikowane są w informacyjnym portalu internetowym resortu www.mon.gov.pl, za którego strukturę, zawartość oraz właściwe funkcjonowanie odpowiada dyrektor DPI.

32. Każda jednostka (komórka) organizacyjna może posiadać własny serwis WWW, po uzyskaniu zezwolenia dyrektora DPI.

33. Serwisy WWW powinny być tworzone w sieci INTER-MON, a w przypadku braku takiej możliwości – w ogólnodostępnej sieci internetowej.

Abstrahując na razie od „polityki informacyjnej" w rozumieniu Decyzji (patrz „Podsumowanie"), to biorąc pod uwagę prowadzenie polityki informacyjnej w Internecie, można w nim:

1. Prezentować swoje informacje.
2. Powodować lepszy/łatwiejszy dostęp do swoich informacji (np. przez tzw. pozycjonowanie). Konstruując odpowiednio stronę WWW i wykorzystując pewne narzędzia programowe, można spowodować, że „nasza" strona będzie się w różnych wyszukiwarkach pokazywała na pierwszych miejscach[10]. Niestety, przeciwnik może także korzystać z tych samych metod.
3. Kształtować pozytywną opinię użytkowników Internetu nt. informacji własnych, generując dużą liczbę pozytywnych o nich opinii, co przy posługiwaniu się odpowiednimi narzędziami programowymi jest łatwe do realizacji[11].
4. Polemizować z informacjami przeciwnika. Wymaga to dobrego dopracowania materiałów polemicznych, o ile takie są prezentowane statycznie, lub doboru dobrych dyskutantów-ekspertów, jeżeli polemika odbywa się dynamicznie (np. na czacie).
5. Uniemożliwiać prezentację informacji przez przeciwnika. Można to osiągnąć poprzez: blokowanie stron WWW z określonymi treściami jako efekt ataku DoS (ang. *Denial of Services*) lub (częściej) rozproszony atak DoS (ang. *Distributed Denial of Services*), usuwanie (całości lub części) treści ze stron WWW. Można to osiągnąć:
   - drogą współpracy z administratorem strony lub serwera, na którym taka strona jest przechowywana. Oprócz dobrej woli konkretnego

[10] Warto także w tym miejscu zwrócić uwagę, że już obecnie, poszukując informacji w Internecie, nie otrzymujemy tego, co chcemy, tylko to, co twórcy algorytmów wyszukiwania zaimplementowanych w wyszukiwarkach (Google, Yahoo, Bing itd.) uważali, że chcemy znaleźć lub uznali, że warto znaleźć (patrz też raport [6]).

[11] Patrz np. praca magisterska obroniona w 2013 roku w Instytucie Teleinformatyki i Automatyki Wydziału Cybernetyki WAT: Wiktor Patkowski: *Badanie możliwości kształtowania opinii forów internetowych za pomocą wielu kont/tożsamości.*

człowieka wymaga to najczęściej istnienia odpowiednich przepisów prawa umożliwiających takie działanie;
- poprzez włamanie na konkretną stronę lub serwer i usunięcie wskazanych treści. Są to oczywiście najczęściej działania bezprawne w świetle prawa miejscowego;
- poprzez fizyczne zniszczenie serwera udostępniającego określone treści. Jest to działanie bezprawne w świetle prawa miejscowego, wymaga użycia grup dywersyjnych lub sabotażowych. Nie oznacza pełnego sukcesu (strona/treści zwykle mogą być łatwo odtworzone z kopii zapasowych w nowej lokalizacji), ale samo działanie destrukcyjne może mieć działanie odstraszające dla podmiotów hostujących takie treści. Obecnie, ze względu na wykorzystywanie zasobów wirtualnych oraz tzw. „przetwarzania w chmurze" (ang. *cloud computing*), wspomniane działania wymagają precyzyjnego wyboru miejsca akcji.

6. Zmieniać informację przeciwnika (naruszanie integralności informacji) poprzez włamanie na konkretną stronę lub serwer i podmianę wskazanych treści. Są to oczywiście najczęściej działania bezprawne w świetle prawa miejscowego.
7. Podszywać się pod przeciwnika, prezentując fałszywe treści.
8. Kształtować negatywną opinię użytkowników Internetu nt. informacji zamieszczonych przez przeciwnika. Można to osiągnąć:
   - wprowadzając np. na określone fora dyskusyjne trolla[12], co prawdopodobnie skłoni część uczestników do wycofania się z dyskusji i wyrobienia sobie negatywnego zdania o ludziach zajmujących się daną tematyką i przez pryzmat tego również negatywnej opinii o prezentowanej tematyce („to temat dla durniów i nawiedzonych, nie warto się tym zajmować");
   - generując dużą liczbę negatywnych opinii o prezentowanej tematyce, co przy posługiwaniu się odpowiednimi narzędziami programowymi jest łatwe do realizacji;
   - dezorientując uczestników dyskusji przez wskazanie na odpowiednio spreparowane treści (patrz punkt 7).

Są to jedynie przykłady działań (ich lista na pewno nie została tutaj wyczerpana), którymi można się posłużyć, prowadząc politykę informacyjną z wykorzystaniem Internetu. Działania opisane w punktach 1-4 są działaniami z zakresu „białego"

[12] Trollowanie (trolling) – antyspołeczne zachowanie charakterystyczne dla forów dyskusyjnych i innych miejsc w Internecie, w których prowadzi się dyskusje. Trollowanie polega na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia (czego następstwem jest wywołanie kłótni) poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych informacji czy też stosowanie różnego typu zabiegów erystycznych.

public relations, natomiast te z punktów 5-8 można zakwalifikować do PR „czarnego". Mając na uwadze paragraf 33 przytoczonej wcześniej Decyzji, warto zauważyć, że:

- potencjalny przeciwnik może także stosować metody wymienione w punktach 1-8;
- oficjalnie, jeżeli nie ma stanu wojny, dopuszczalne są jedynie działania z punktów 1-4;
- „wystawione" w sieci INTER-MON informacje są (a przynajmniej powinny być) lepiej chronione przed destrukcyjnymi działaniami przeciwnika niż w przypadku wystawienia ich bezpośrednio „w Internecie".

Osobnego rozważenia z perspektywy działań w Internecie, ze względu na wagę tego zagadnienia dla ogólnoświatowego bezpieczeństwa, wymaga terroryzm (patrz np. [4], [9], [10], [13]). W tym artykule to zagrożenie nie będzie analizowane. Warto jedynie zasygnalizować, że z punktu widzenia pewnej grupy użytkowników Internetu związanych z przestępstwami, w tym przestępstwami o charakterze terrorystycznym, Internet może być:

- *środkiem logistycznym* do osiągnięcia założonych celów (patrz motto; także jako witryna do oddziaływania psychologicznego na innych użytkowników Internetu);
- *przedmiotem ataku*, który ma uniemożliwić z jednej strony korzystanie z Internetu innym użytkownikom, z drugiej – oddziaływać np. na te elementy infrastruktury krytycznej państwa, które są zależne od niezakłóconego działania Internetu.

W rozdziale XIV *Objaśnienie wyrażeń ustawowych kodeksu karnego* [14] znajduje się definicja „przestępstwa o charakterze terrorystycznym":

„§20. Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.

W definicji używane są rozmyte[13] sformułowania, utrudniające prawidłowe rozpoznanie zagrożeń (szczególnie w obszarze przetwarzania informacji), którym można przypisać miano terrorystycznych. Z drugiej strony nie ma znaczenia czy np. zawalenie budynku i w efekcie zniszczenie systemu teleinformatycznego nastąpiło na

[13] Np. od jakiej liczby zaczyna się „wiele osób"?

skutek jego wysadzenia przez terrorystę, czy też w wyniku wybuchu gazu z powodu nieszczelności instalacji gazowej (spowodowanej zaniedbaniami w jej konserwacji). W obu przypadkach zostaną uruchomione procedury awaryjne odpowiednie dla katastrofy budowlanej. Związki pomiędzy realizacją polityki informacyjnej w Internecie a kryteriami jakości informacji przedstawia tabela 1.

Tabela 1

Powiązania działań w zakresie polityki informacyjnej z kryteriami jakości

Lp.	Rodzaj działania	Zależność lub wpływ na kryterium jakości informacji	Możliwość przeciwdziałania
1	Prezentowanie informacji własnych	Informacje opisujące oraz wszystkie kryteria jakości i bezpieczeństwa	Działania 5-8
2	Pozycjonowanie informacji własnych	Informacje opisujące oraz wszystkie kryteria jakości i bezpieczeństwa	
3	Kształtowanie pozytywnych opinii użytkowników Internetu nt. informacji własnych	Informacje opisujące oraz wszystkie kryteria jakości i bezpieczeństwa	Działania 6-8
4	Polemizowanie z informacjami przeciwnika	Informacje opisujące oraz wszystkie kryteria jakości i bezpieczeństwa	Działania 6-8
5	Uniemożliwienie prezentacji informacji przez przeciwnika:	Aktualność, kompletność, integralność, dostępność	
	5.1. Blokowanie stron WWW z określonymi treściami	Aktualność, kompletność, dostępność	Przenoszenie pomiędzy serwerami hostującymi, zwiększanie przepustowości łącza, wczesne wykrywanie ataków DoS
	5.2. Usuwanie (całości lub części) treści ze stron WWW:	Kompletność, integralność, dostępność	Sumy kontrolne i podpisy cyfrowe (jako mechanizm detekcji), monitorowanie i zatwierdzanie zmian
	5.2.1. Współpraca z administratorem strony lub serwera	Kompletność, integralność, dostępność	
	5.2.2. Włamanie na stronę lub serwer i usunięcie wskazanych treści	Dostępność	
	5.2.3. Fizyczne zniszczenie serwera udostępniającego określone treści	Dostępność	Dobra ochrona fizyczna obiektu z serwerami

Lp.	Rodzaj działania	Zależność lub wpływ na kryterium jakości informacji	Możliwość przeciwdziałania
6	Zmienianie informacji przeciwnika poprzez włamanie na konkretną stronę lub serwer i podmianę wskazanych treści	Autentyczność	Sumy kontrolne i podpisy cyfrowe, monitorowanie i zatwierdzanie zmian
7	Podszywanie się pod przeciwnika i prezentowanie fałszywych treści	Autentyczność	Sumy kontrolne i podpisy cyfrowe, monitorowanie i zatwierdzanie zmian
8	Kształtowanie negatywnych opinii użytkowników Internetu nt. informacji zamieszczonych przez przeciwnika:	Informacje opisujące	
	8.1. Trolling	Informacje opisujące i wszystkie kryteria jakości	Wykluczanie trolli z forów przez moderatorów[1]
	8.2. Generowanie negatywnych opinii	Informacje opisujące	Wykonanie działań z punktu 5
	8.3. Wskazanie fałszywych treści	Informacje opisujące	

4. Podsumowanie

Istotnym zagadnieniem w prowadzeniu dobrej polityki informacyjnej jest korelacja informacji prezentowanych za pomocą różnych środków masowego przekazu: prasa, radio, Internet, telewizja. Problemy w przypadku braku właściwego nadzoru mogą wystąpić także przy rozpatrywaniu prezentowania określonych treści tylko w Internecie – z punktu 32 Decyzji wynika, że każda jednostka organizacyjna może mieć własną stronę WWW. Spośród wymienionych we wstępie parametrów jakości informacji najważniejsze będą w tym przypadku spójność, a w dalszej kolejności wiarygodność i autentyczność.

„Polityka informacyjna" przedstawiona w Decyzji obejmuje jedynie zestaw organizacyjnych i administracyjnych postanowień i zadań prasowych zespołów resortu, których celem jest „zaspokojenie potrzeb informacyjnych społeczeństwa oraz uzyskanie zrozumienia i akceptacji społecznej dla celów i działań podejmowanych przez resort". Nie ma w tej Decyzji mowy o „walce" w zakresie kształtowania świadomości i woli, nie jest zdefiniowany „przeciwnik" i zagrożenia.

Jednak autorzy tego artykułu uważają, że w domenie informacyjnej, wbrew poglądom naszych decydentów, nie ma takiego stanu jak „pokój". W tej domenie

jesteśmy w stanie permanentnej wojny. Warto zatem zwrócić uwagę, że np. w USA problem ten już dostrzeżono [15] i opracowano STRATCOM[14] – Strategię Komunikacyjną (często w literaturze polskiej błędnie nazywaną Komunikacją Strategiczną), która obejmuje operacje informacyjne INFOPS (w ramach wojny czy walki informacyjnej), oddziaływanie psychologiczne PSYOPS, informowanie medialne PA (Public Affairs), dyplomację oraz wpływ działań kinetycznych i niekinetycznych na sposób postrzegania wydarzeń.

W Polsce, ze względu na różne zaszłości historyczne i przepisy prawa, zdolności np. odpowiednich komórek sił zbrojnych oddziaływania na świadomość i wolę społeczeństwa (co kojarzy się ciągle z niechcianą manipulacją i propagandą) są, niestety, niewielkie i z definicji mogą one być użyte jedynie w czasie wojny (INFOPS, PSYOPS). W siłach zbrojnych RP dopiero od początku bieżącego (2013) roku są prowadzone prace nad przywróceniem tych zdolności również w czasie pokoju przez właściwą koordynację wszystkich form możliwego oddziaływania, co jest właśnie rolą STRATCOM. Dlatego autorzy uważają, że w odniesieniu do użytego w [5] określenia „polityka informacyjna" właściwsze byłoby określenie „polityka informowania".

LITERATURA:

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: *Achievements and next steps: towards global cyber-security*. Brussels, 31.3.2011 COM(2011) 163 final.
2. Decyzja Nr 108 /MON z dnia 7 kwietnia 2009 r. *w sprawie zasad realizacji polityki informacyjnej w resorcie obrony narodowej*. Dz.Urz. MON Nr 7, poz. 82 oraz z 2011 r. Nr 2, poz. 25.
3. *Emerging Cyber Threats Report 2013*. Presented by Georgia Information Center and the Georgia Research Tech Institute. Dostępny: http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf.
4. *Europejska Agenda Cyfrowa w pracach i planach polskich instytucji rządowych*, Ministerstwo Spraw Wewnętrznych i Administracji, Departament Społeczeństwa Informacyjnego, Wydanie I, 2011.
5. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Europejska Agenda Cyfrowa* z 26 sierpnia 2010 r., KOM(2010) 245 wersja ostateczna/2.
6. *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, Lizbona 19-20 listopada 2010 r.
7. L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, EAS, Kraków 2008.

[14] Ang. STRATCOM – *Strategic Communications*; nie mylić z STRATCOM – *US Strategic Command*!

8. K. Liderman, *Bezpieczeństwo informacyjne*, WN PWN, Warszawa 2012.
9. K. Liderman, A. Malik, *Bezpieczeństwo informacyjne jako cel ataku terrorystycznego*, (w:) P. Majer, M. Sitek (red.), *Jakość w działaniach na rzecz bezpieczeństwa państw Grupy Wyszehradzkiej z perspektywy europejskiej*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, Józefów 201, s. 17-27.
10. *NATO Strategic Communications Policy* SG(2009)0794.
11. *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016*, Wersja 1.1. Warszawa, czerwiec 2010.
12. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2007.
13. *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, Ministerstwo Spraw Wewnętrznych i Administracji, grudzień 2008.
14. *Strategy for Operating in Cyberspace*, USA Department of Defense, lipiec 2011.
15. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (znowelizowany, 2010 r.).

THE POLITICS OF INFORMATION AND INFORMATIONAL SECURITY

Abstract. The article focuses on problems concerning information policy, especially in reference to information policy of the Polish Ministry of Defense. One of its topics concentrates specifically on agenda and evidence applicable to the Internet. In an overview autor presents different means of propaganda technics for specifically planned outcomes, with an explanation on posibilities of manipiulation with different information atribiutes (in part 2 and 3). There is also a describtion of agenda referring to Internet possibilities, in respect to working out the means of planned shaping of the consciousness of its users.