Anna Antczak [1]

Bezpieczeństwo informacji jako jeden z istotnych elementów strategii bezpieczeństwa Unii Europejskiej

Abstract. ***Information safety as one of the essential elements of the European Union's safety strategy.*** The following article aims at answering the question of how the skillful use of information affects the system of state security, or even international organizations, including a special type of organization of transnational character, namely the European Union. It will be important to identify new threats to international security generated in the XXI century, and which are directly related to the information – means of acquiring, collecting, processing, conservation and most importantly – effective management and exploitation. With these elements raises the problem of misinformation – manipulation of information, misleading both the public and potential adversary (this applies equally to actions at governmental level and the activity of media). New technology gives unknown possibilities of extremely smooth and efficient flow of information, which also involves nontraditional threats (cyber terrorism and a new dimension of information war).

1) Dr Anna Antczak, analityk w Kancelarii Senatu RP.

Francis Fukuyama w swym dziele „Wielki wstrząs" w 1999 r. pisał: „weszliśmy w wiek informacji. Mamy więcej niż kiedykolwiek tego, co człowiek współczesny ceni sobie najbardziej: wolności i równości. A zarazem – wszystkie reguły rządzące dotychczas życiem społeczeństw zostały zakwestionowane." Społeczeństwo XXI wieku definiowane jest jako społeczeństwo informacyjne czy też społeczeństwo wiedzy. Może raczej lepiej byłoby je określić mianem społeczeństwa korzystającego z wiedzy. Warto zatem zadać pytanie o to, jakie znaczenie ma informacja w środowisku bezpieczeństwa XXI wieku.

W niniejszym artykule zostanie podjęta próba odpowiedzi na pytanie, w jaki sposób umiejętne wykorzystanie informacji wpływa na system bezpieczeństwa państw czy nawet szerzej – organizacji międzynarodowych, a w tym szczególnego typu organizacji o charakterze ponadnarodowym, czyli Unii Europejskiej. Istotne będzie zidentyfikowanie nowych zagrożeń, jakie generuje środowisko międzynarodowe XXI wieku, a które są bezpośrednio związane z informacją, sposobami jej zdobywania, gromadzenia, przetwarzania, ochrony i co najistotniejsze efektywnego zarządzania i wykorzystywania. Z powyższymi elementami wiąże się problem dezinformacji – manipulacji informacją, wprowadzania w błąd zarówno opinii publicznej jak i potencjalnego przeciwnika. Dotyczy to w równym stopniu działań na poziomie rządowym i aktywności mediów. Nowa technologia zaś daje nieznane do tej pory możliwości niezwykle sprawnego i skutecznego przepływu informacji, co też wiąże się z nietradycyjnym rodzajem zagrożeń (cyberterroryzm oraz walka informacyjna nowego wymiaru).

Na wstępie warto zastanowić się, czym jest informacja. Istnieją opinie, że informacja jest pojęciem pierwotnym, zatem niemożliwe jest jej zdefiniowanie za pomocą pojęć prostszych (Przybyłowicz, 2008: 1). Jednak w „Encyklopedii powszechnej PWN" (1974: t2, 281) można znaleźć następującą definicję: informacja (łac. *informatio* – wizerunek, zarys, pojęcie; *informare* – kształtować, tworzyć, przedstawiać, uczyć[2]) to każdy czynnik zmniejszający stopień niewiedzy o badanym zjawisku umożliwiający polepszenie znajomości otoczenia i w sprawniejszy sposób przeprowadzenie celowego działania. Jednak już „Nowy Leksykon PWN" (1998: 678) określa informację jako obiekt abstrakcyjny i niedefiniowalny.

Można wyróżnić dwa podstawowe rodzaje postrzegania informacji (Przybyłowicz, 2008: 1-6):

- obiektywny – informacja oznacza pewną właściwość fizyczną lub strukturalną obiektów, przyjmuje się pewne modele źródeł informacji i ustala

2) *Słownik łacińsko-polski*, PWN, Warszawa 1990, s. 260.

obliczeniowe miary jej ilości. Upraszczając nieco teorię C.E. Shannona[3], informacja może być określana poprzez poziom niepewności odbiorcy odnośnie do treści przekazu,

• subiektywny – informacja ma charakter względny i jest tym, co umysł jest w stanie przetworzyć i wykorzystać do własnych celów. Innymi słowy informację można analizować przez pryzmat użyteczności dla danego odbiorcy.

Istnieją zaś trzy powiązane ze sobą koncepcje (teorie) informacji, związane z jej aspektami semiotycznymi (Mynarski, 1979: 141):

- statystyczno-syntaktyczna - związana z aspektem probabilistycznym i składniowym,
- semantyczna – ze znaczeniowym,
- pragmatyczna – badanie stosunków między znakami słownymi a interpretatorami oraz interpretowanie wypowiedzi w zależności od kontekstu.

Informacja w odniesieniu do procesu komunikowania się ma charakter relatywny i jest nazywana informacją względną, którą można określić jako „odbitą różnorodność, jako różnorodność, którą obiekt odbijający zawiera o obiekcie odbijanym" (Ursuł, 1971: 44). Według Mariana Mazura (1996: 102) informacja jest to „transformacja poprzeczna komunikatów w torze sterowniczym", zaś informowanie to „transformacja informacji zawartej w oryginałach w informację zawartą w obrazach". Podsumowując tę część rozważań, warto przytoczyć definicję proponowaną przez L. Ciborowskiego (1999:185), z której wynika, że informacja to „bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, który w jego przekonaniu (świadomości) kojarzy się jakoś z bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni".

Należy pamiętać, że informacja może być bardzo niebezpieczną bronią, dlatego trzeba się nią posługiwać w sposób umiejętny (Jałoszyński, Skosolas, 2008: 83). Rola informacji we wszystkich sferach życia człowieka nieustannie wzrasta. Stanowi kluczowy element gospodarki, będąc jednocześnie towarem, elementem kreującym branżę informatyczną i telekomunikacyjną jak i strategicznym czynnikiem produkcji oraz przyczyną głębokich przemian w strukturach gospodarczych (Sienkiewicz, Jemioło, Zacher, 2001: 133-135). Jednak informacja i jej bezpieczeństwo to nie tylko sektor ekonomiczno-technologiczny. Era informacyjna odciska swoje piętno również na systemie międzynarodowym i relacjach między poszczególnymi aktorami. Jak zauważył sekretarz generalny NATO, Jaap de Hoop Scheffer, w ostatnich latach środowisko informacyjne zmieniło się w sposób gruntowny i w wielu

3) Więcej na temat tej teorii zob. C. E. Shannon, *A Mathematical Theory of Communication,* przedruk z poprawkami za *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, July-October 1948, s. 1-55.

aspektach technologii, ale także dostępności, odbiorców, szybkości a nawet samych źródeł informacji[4]. Z powodu wzrostu szybkości rozprzestrzeniania się informacji, już ani rządy państw, ani nawet same media nie są w stanie kontrolować przepływu informacji, a to z powodu powszechnego dostępu do Internetu i możliwości zamieszczania tam dowolnych treści przez dowolne osoby. Wzrost ilości informacji i metod jej rozpowszechniania wprowadził nową jakość w stosunkach międzynarodowych zarówno politycznych jak i ekonomicznych, społecznych oraz kulturalnych. Wzrost dostępności do informacji spowodował także rozwój postępowania decentralizacji procesu decyzyjnego (Sienkiewicz, Jemioło, Zacher, 2001: 140) szczególnie w sektorze biznesowym, bankowym, ale także na poziomie rządowym oraz w strukturach wysoce zhierarchizowanych, np. w służbach mundurowych (przede wszystkim w wojsku). Jednak szerokie i powszechnie dostępne nowe technologie informacyjne, prócz nieocenionych korzyści, generują także nowe zagrożenia. Nowe technologie (rozumiane jako nowoczesne środki i zaawansowane technologie) znacznie ułatwiają działania międzynarodowym grupom przestępczym i terrorystycznym zarówno w zakresie komunikacyjnym jak i poszerzają spektrum działań, dając nowe możliwości (np. cyberterroryzm, czy zamachy na infrastrukturę krytyczną). Ataki na systemy informatyczne zarówno rządowe, jak i sektora prywatnego, od których w znacznej mierze uzależnione jest społeczeństwo i jego funkcjonowanie, przede wszystkim w sferze ekonomicznej i finansowej, mogą mieć katastrofalne skutki o trudnym do przewidzenia zakresie i zasięgu. Przejęcie kontroli nad siecią (szczególnie, gdy zarządza ona infrastrukturą krytyczną) może doprowadzić albo do jej zniszczenia, albo (co może mieć gorsze skutki) do zakłócenia jej działania.

Oprócz oczywistych korzyści, jakie płyną z rozwoju technologicznego, istnieje także wiele wyzwań i zagrożeń. Te, które dotyczą bezpieczeństwa informacyjnego występują w niemal wszystkich sferach (Sienkiewicz, Jemioło, Zacher, 2001: 167-182):

- społecznej: monopol państwa na informację i bariera technokratyczna, podatność na zakłócenia zewnętrzne, zróżnicowany dostęp do informacji/wiedzy, wzrost bezrobocia, konflikty społeczne (poczucie nierówności), ograniczona swoboda i nowe formy inwigilacji oraz przestępczości, uzależnienie od techniki, dehumanizacja, nowe choroby psychiczne, osłabienie więzi społecznych;
- ekonomicznej: migracja ludności do obszarów miejskich, redukcja zatrudnienia, zbyt duże uzależnienie od efektywności systemów informacyjnych;
- kulturalnej: ograniczenie twórczego myślenia, uzależnienie od mediów

4) Wypowiedź sekretarza generalnego NATO, Jaapa de Hoop Scheffera podczas seminarium na temat: Dyplomacja publiczna podczas operacji NATO (Public Diplomacy In NATO-led Operations), 7 października 2007, Kopenhaga, strona internetowa NATO: <http://www.nato.int/docu/speech/2007/s071008a.html>.

elektronicznych, negatywne zmiany w systemie wartości, prymat kultury masowej[5].

Informacja odgrywa także kluczową rolę w walce zbrojnej. Posiadanie odpowiedniej informacji w odpowiednim czasie i jej efektywne wykorzystanie może przesądzić o kompleksowym sukcesie bądź porażce. „Kto zna wroga i zna siebie, temu nic nie grozi, choćby w stu bitwach" (Sun Zi, 2004: 72), zatem posiadanie informacji może decydować o władzy podmiotu, który ją zdobył nad innymi podmiotami. (Ma to odniesienie zarówno do zachowań jednostkowych, jak i państw bądź całych grup państw czy nawet organizacji). Powodzenie w wojnie informacyjnej zależy od bardzo wielu czynników, począwszy od kampanii informacyjnej prowadzonej przed operacją, doboru wiadomości przekazywanych podczas jej trwania, relacji ze społecznością, przedstawicielami mediów, ale przede wszystkim od dobrej strategii na wszystkich szczeblach i poziomach oraz koordynacji polityki informacyjnej, która pozwoli na zdobycie przewagi nad przeciwnikiem. Przeciwnicy w wojnie medialnej są różni, nie tylko pojmowani w ujęciu klasycznym (czyli przedstawiciele drugiej strony konfliktu). Jak słusznie zauważa R. Kwećka (2001: 60), „zasadniczym celem wojen XXI wieku będzie uzyskanie kontroli nad informacją, mogącą wywierać bezpośredni wpływ na decyzje w wojnie". Oznacza to zdobycie szeroko pojętej przewagi informacyjnej nad przeciwnikiem, z czym wiąże się również wygranie wojny w mediach[6]. Tzw. wojna internetowa zaś daje wiele możliwości wykorzystania różnych środków m.in. propagandy, dezinformacji, wirusów, włamań do serwisów internetowych.

Istotne jest, aby we właściwy sposób dobierać informacje przekazywane na temat działań podejmowanych przez żołnierzy w celu zyskania zrozumienia i poparcia społecznego. Społeczeństwo nie ma możliwości poznania i zrozumienia, na czym dokładnie polegają zadania żołnierzy i jak wygląda ich codzienność w czasie pokoju, ale przede wszystkim kryzysu i wojny. Do powyższego katalogu dochodzi jeszcze konieczność ochrony informacji niejawnych bądź takich, których ujawnienie szerokiej opinii publicznej może mieć negatywne skutki dla całej operacji[7]. Powyższe stwierdzenie nie musi się zresztą odnosić wyłącznie do działań militarnych, ale także do innych aspektów działalności państw, zarówno w sferze wewnętrznej jak i na arenie międzynarodowej oraz informowania o nich opinii publicznej w obszarze politycznym, ekonomicznym, społecznym, kulturalnym czy technologicznym. Kluczową rolę odgrywa kwestia odpowiedniej interpretacji informacji, sposobu i czasu jej dostarczenia, ograniczanie jej, wreszcie manipulacja. Zabiegi, jakim poddawa-

5) Nie jest to zamknięty katalog konsekwencji „informatyzacji". Podane przykłady są wyselekcjonowanym zbiorem elementów, które autorka uznała za najistotniejsze.
6) Siły zbrojne państw zaawansowanych technologicznie prowadzą prace nad opanowaniem przeciwnika za pomocą sieci informatycznych (paraliż systemów dowodzenia, radarów, elektrowni, łączności itp.).
7) Szerzej zob. A. Antczak, L. Elak, *Żołnierze CIMIC i oficerowie prasowi w operacjach międzynarodowych – wybrane aspekty*, Akademia Obrony Narodowej, Warszawa 2009, rozdział 4.

na jest informacja mogą być stosowane na każdym etapie i przez każdego dysponenta – nadawcę i odbiorcę. W praktyce oznacza to, że informacją mogą manipulować zarówno jej pierwotni nadawcy (np. rządy państw), jak i dystrybutorzy pośredni przede wszystkim media. Oznacza to, że społeczeństwo może otrzymać komunikat dalece zmieniony, przetworzony, zinterpretowany, zmanipulowany. W kwestii przepływu czy też „zdobywania" informacji kluczowym aspektem jest czas. Ma on znaczenie zarówno w przypadku dostarczenia właściwej informacji w odpowiednim czasie. W sektorze finansowym (giełda), w przypadku wszelkiego rodzaju sytuacji kryzysowych, wojny, ale także w obszarze polityki – podejmowanie istotnych decyzji oraz informowania społecznego – luki („poślizgi") czasowe mogą być wykorzystane przez media, przeciwnika czy terrorystę.

Państwa członkowskie UE zdają sobie sprawę, jak istotne jest bezpieczeństwo sieci i informacji, dlatego w 2005 r. powstała „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – dialog, partnerstwo i przejmowanie inicjatywy"[8]. Ma ona pomóc w stworzeniu jednolitej europejskiej przestrzeni informacyjnej. Strategia formułuje ramy dla rozwoju spójnego podejścia do kwestii bezpieczeństwa informacyjnego, koncentrując się w sposób szczególny na trzech elementach:

- środkach związanych z bezpieczeństwem sieci i informacji,
- ramach regulacyjnych dla łączności elektronicznej (z uwzględnieniem zagadnień dotyczących ochrony prywatności oraz danych) oraz
- zwalczaniu przestępczości internetowej.

Bezpieczeństwo sieci i informacji zdefiniowane jest jako „zdolność sieci lub systemu informatycznego do oparcia się, w określonym stopniu, skutkom przypadkowych zdarzeń lub złośliwych działań obniżających dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych oraz związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci lub systemy"[9]. W strategii zostały zidentyfikowane główne wyzwania w sferze bezpieczeństwa społeczeństwa informacyjnego:

- ataki na systemy informatyczne powodowane chęcią zysku[10] oraz zakłócania/uniemożliwienia pracy systemu[11],
- nielegalne wykorzystywanie danych uzyskanych w wyniku ataku na system informatyczny,
- spam jako nośnik wirusów i szkodliwego oprogramowania (programy wywiadowcze, wyłudzanie informacji itp.),
- ataki na elektroniczne urządzenia przenośne oraz
- utrudniona ochrona prywatności.

8) Dialogue, partnership and empowerment: A Strategy for a Secure Information Society, Bruksela 31 maja 2005.
9) *Ibidem*, s. 1.
10) Sprzedaż danych osobowych czy informacji poufnych.
11) Sterowanie działalnością infrastruktury krytycznej może odgrywać ogromną rolę w działalności zorganizowanych grup przestępczych i/lub terrorystycznych, dając im praktycznie nieograniczone możliwości.

Oznacza to, że te same technologie, które pozytywnie stymulują gospodarkę, usprawniają komunikację społeczną oraz działania wielu sektorów, w szczególności finansowego[12] i infrastrukturalnego[13] oraz służb bezpieczeństwa, generują nowego rodzaju zagrożenia, które do tej pory nie były znane i nie wypracowano środków zapobiegania i walki z nimi. Jednocześnie w strategii podkreśla się niezwykle istotną rolę, jaką odgrywają technologie teleinformatyczne, będące decydującym elementem innowacyjności, ale także w znacznym stopniu przyczyniają się do wzrostu gospodarczego, powstawania nowych miejsc pracy oraz są stałą częścią stosunków społecznych. Jak podaje Eurostat, w 2007 r. 95% przedsiębiorstw w UE korzystało z Internetu, ponad 50% gospodarstw domowych posiada do niego dostęp, zaś średnie wydatki na technologie informatyczne (IT) w państwach UE wynosiły 2,7% PKB. Interesujący jest też fakt, że prawie 85% wniosków składanych do Europejskiego Biura Patentowego z zakresu zaawansowanych technologii dotyczyło obszaru komunikacji i łączności (52,4%) oraz komputeryzacji i zautomatyzowanego sprzętu wykorzystywanego w biznesie (32,1%)[14].

W strategii podkreśla się, że na bezpieczeństwo informacyjne ma wpływ wiele elementów składowych, tworzących łańcuch bezpieczeństwa: jednostki administracji publicznej (ochrona informacji sektora publicznego), przedsiębiorcy (zapewnienie bezpieczeństwa jako element przewagi konkurencyjnej) oraz użytkownicy indywidualni. Bezpieczeństwo sieci i informacji powinno być promowane jako zaleta. Aby skutecznie przeciwdziałać zagrożeniom, konieczna jest rzetelna wiedza na temat naruszania bezpieczeństwa. Wiele instytucji i przedsiębiorstw jednak niechętnie udostępnia takie dane w obawie o spadek zaufania i problemy, jakie może generować rozpowszechnienie tego typu informacji. Ważne jest jednak szerzenie świadomości społecznej w zakresie bezpieczeństwa informacyjnego, co w znacznym stopniu może się przyczynić do zmniejszenia liczby ataków i wytworzyć swoistą kulturę bezpieczeństwa.

Unia Europejska podejmowała szereg działań mających na celu z jednej strony szerzenie świadomości oraz informowanie na temat wyzwań i zagrożeń, a z drugiej – metod przeciwdziałania im. Jedną z ważniejszych była inicjatywa *eEurope – An Information Society for All* z 1999 r., która wyznaczała dziesięć obszarów tematycznych mających na celu dostosowanie państw UE do wymagań społeczeństwa informacyjnego a następnie eEurope 2002 (Bógdał-Brzezińska, Gawrycki, 2003: 231-232). W 2004 r. została utworzona Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*European Network and Information Security Agency – ENISA*). Jest ona

12) Systemy bankowe, funkcjonowanie giełdy czy zakładów ubezpieczeniowych.
13) Przede wszystkim infrastruktura krytyczna: transport, dostawy żywności, gospodarka wodna, telekomunikacja i energetyka, ale także przemysł o znaczeniu strategicznym.
14) Dane statystyczne za: *Europe in Figures. Eurostat yearbook 2009, Office for Official Publications of the European Communities*, Luxemburg 2009, s. 33, 54, 501, 508.

instytucją o charakterze doradczym – dla wspierania państw członkowskich w ich wysiłkach na rzecz wzmacniania bezpieczeństwa i zdolności przeciwdziałania oraz reagowania na problemy związane z siecią i systemami informatycznymi. Zbiera ona także dane dotyczące bezpieczeństwa informacyjnego i analizuje je. Różnorakie działania polityczne uzupełniają inicjatywy podejmowane na rzecz osiągania celów zapisanych w Zielonej Księdze w sprawie europejskiego programu ochrony infrastruktury krytycznej *European Programme for Critical Infrastructure Protection (EPCIP*), który ma umożliwić wypracowanie kompleksowego podejścia do jej ochrony. UE rozważała także możliwość stworzenia europejskiego wielojęzycznego systemu ostrzegania i wymiany informacji.

Strategia zawiera postulat, by „przemysł europejski był zarówno użytkownikiem, jak i konkurencyjnym dostawcą produktów i usług związanych z bezpieczeństwem”[15]. Sprawą kluczową jest bezpieczne administrowanie systemami informatycznymi, szczególnie w przypadku instytucji bezpośrednio związanych z bezpieczeństwem i obroną oraz mających dostęp do tajemnicy państwowej[16]. Strategia identyfikuje także trzy kluczowe narzędzia bezpieczeństwa informacyjnego:

- dialog (wypracowanie najlepszych rozwiązań na postawie wymiany doświadczeń pomiędzy państwami członkowskimi),
- partnerstwo (utworzenie strategicznego partnerstwa, w którego skład wchodziłyby państwa członkowskie – sfera rządowa, sektor prywatny oraz środowiska naukowe),
- przejmowanie inicjatywy (większa aktywność poszczególnych grup).

Istotą strategii jest zaangażowanie wielu zainteresowanych podmiotów i wspólne, synergiczne działanie mające na celu umacnianie bezpieczeństwa informacyjnego.

Bezpieczeństwo sieci i systemów informatycznych jest kluczowym elementem wspierającym najistotniejsze aspekty sfery ekonomiczno-społecznej w XXI wieku. Pomijając nawet obszar administracji państwowej, w codziennym życiu systemy informatyczne i pokrewne muszą podlegać ochronie w celu podtrzymywania przewagi konkurencyjnej, pozytywnego wizerunku na rynku, utrzymania ciągłości w firmie, zapobiegania oszustwom i spełniania wymogów prawnych (ochrona prywatności i danych osobowych). Oznacza to zapewnienie, że informacja wprowadzona drogą elektroniczną pozostanie dostępna (tylko dla osób do tego upoważnionych), rzetelna, autentyczna i poufna.

Istotną rolę odgrywa także program badawczy „Technologie społeczeń-

15) Dialogue, partnership…, op.cit., s. 6.

16) Dobrym przykładem może być atak na niezabezpieczony serwer internetowy Ministerstwa Obrony Narodowej w styczniu 2007 r., który dał możliwość wprowadzania zmian na stronie internetowej urzędu. Na szczęście brak zabezpieczeń wykryła osoba, która nie miała złych intencji i jedynie poinformowała MON o tym, że na serwer można się włamać bez większego wysiłku.

stwa informacyjnego", w ramach którego prowadzone są badania naukowe dotyczące zarządzania tożsamością cyfrową i prywatnością, biometryki oraz ochrony dóbr cyfrowych. Prowadzone są także prace nad elastyczną infrastrukturą, która jest w stanie aktywnie odpowiadać, zarówno na przewidziane jak i niespodziewane obciążenia i nadwerężenia (spowodowane działalnością człowieka, uszkodzeniem jakiejś części lub katastrofą naturalną), a także nowymi krypto-technologiami, odpornością sieci i bezpieczną wymianą dóbr cyfrowych.

Komisja Europejska podejmuje także wiele inicjatyw mających na celu ochronę danych osobowych, nadanie ram regulacyjnych dla łączności elektronicznej, zwalczanie przestępczości w cyberprzestrzeni (w tym cyberterroryzmu) oraz ochronę infrastruktury krytycznej, włączając w to krytyczną infrastrukturę informacyjną. Przykłada się dużą wagę do współpracy międzynarodowej w tym zakresie oraz wprowadzania przez państwa członkowskie koniecznych zmian w przepisach prawnych dotyczących tej sfery. Poszczególne polityki sektorowe podlegają częstym rewizjom z jednej strony w celu oceny ich dotychczasowej efektywności i stopnia wdrożenia w poszczególnych państwach członkowskich. Z drugiej strony, z uwagi na niezwykle szybkie tempo i dynamikę rozwoju nowej technologii w tej dziedzinie dla poszerzenia spektrum działalności. Komisja Europejska zachęca także do zacieśniania współpracy w zakresie wymiaru sprawiedliwości, która dotyczyłaby przestępstw w obszarze nielegalnego dostępu do systemów informatycznych oraz nieprawnej ingerencji w systemy i dane .

Ataki w cybeprzestrzeni są często określane jako nowa broń masowego rażenia (Bógdał-Brzezińska, Gawrycki, 2003: 74), na które narażone są przede wszystkim państwa zaawansowane technologicznie. Powody, dla których cyberterrroryzm staje się popularną formą walki, to przede wszystkim możliwość dokonania anonimowego, nagłego i nieprzewidzianego ataku o niewielkim ryzyku wykrycia przygotowań do jego przeprowadzenia, a także fakt, że nie powoduje on śmierci ludzi. Paraliż systemu jest zaś bardzo spektakularny, a jego negatywne skutki docierają do opinii publicznej, zatem efekt propagandowy zostaje osiągnięty. Terroryści pragną osiągnąć swe cele, manipulując strachem, wykorzystując z jednej strony wyolbrzymiony przez media obraz zagrożenia zamachem, z drugiej zaś tworzącą się swoistą spiralę niemocy społeczeństwa wobec terroryzmu (Jałoszyński, Skosolas, 2008: 43).

Tabela 1. *Przyczyny cyberterroryzmu i jego wpływ na bezpieczeństwo*

przyczyny cyberterroryzmu	wpływ na bezpieczeństwo
niskie koszty	powszechność (potrzebny jest komputer, dostęp do Internetu i określone umiejętności)
działania ponad granicami państw	nieznane źródło ataku (skąd on pochodzi i kto jest zleceniodawcą)
trudna identyfikacja zagrożenia	zagrożenie realne *versus* wirtualne
utrudnione wykrycie cyberataku	nieznane umiejętności i intencje atakującego
nieznany cel ataku	nieznany sposób oraz oczekiwany efekt końcowy ataku
skomplikowana budowa struktury koalicji przeciwnika	nie wiadomo, kto jest „swój", a kto „obcy"

Źródło: *opracowanie na podstawie B. Bógdał-Brzezińska, M. Gawrycki: 88.*

Internet jest dodatkowo wykorzystywany przez terrorystów jako (Jałoszyński, Skosolas, 2008: 45):
- narzędzie umożliwiające dostęp do grup dyskusyjnych o określonej ideologii,
- źródło wiedzy o treningu i szkoleniu terrorystów,
- sposób utrzymywania kontaktów między organizacjami i ich strukturami,
- sposób nawiązywania kontaktu przywódców organizacji terrorystycznych z osobami zainteresowanymi z całego świata.

Do powyższego katalogu należy jeszcze dodać, że Internet jest dla terrorystów także źródłem wiedzy na temat potencjalnych celów ataku.

Odrębną kwestię stanowi posiadanie rzetelnej informacji albo nawet wiedzy na temat własnych możliwości (potencjału, zdolności, sił, środków), systemu wymiany informacji, informacji nt. przeciwnika. „Przewaga w dziedzinie informacji albo przewaga w dziedzinie wiedzy mogą przesądzić o losach wojny. Jednakże przewaga ta jest w największej mierze krucha"[17]. W tym kontekście niezwykle istotne są różnorodne metody i źródła zdobywania gromadzenia, przetwarzania oraz dystrybucji informacji, a także jej wykorzystywanie i ochrona (w tym systemy zabezpieczeń).

Większość kryzysów, jakie mają miejsce w obecnym stuleciu, jest powiązana z terroryzmem, problemami humanitarnymi, zdobywaniem

17) H. i A. Toffler, *Wojna i antywojna*, Świat Książki, Warszawa 1998, s. 184.

bogactw naturalnych, bezpieczeństwem obywateli oraz stabilnością niezbędną do utrzymania demokratycznych rządów. Z powodu wzrostu szybkości rozprzestrzeniania się informacji już ani rządy państw, ani nawet same media nie są w stanie kontrolować jej przepływu. Przyczyną jest powszechny dostęp do Internetu i możliwości zamieszczania tam dowolnych treści przez dowolne osoby. Dzielenie się informacją z opinią publiczną to sprawa wieloaspektowa w kwestii bezpieczeństwa (jedno źródło informacji jest łatwiejsze do kontrolowania niż kilka – (Jałoszyński, Skosolas, 2008: 83)). Z jednej strony przekaz może być zmanipulowany, z drugiej zaś – wykorzystany np. przez terrorystów. Znaczny rozwój technologii daje niespotykane dotychczas możliwości zdobywania, gromadzenia oraz transferu informacji. Może to być wykorzystywane zarówno w celu lepszego ich zabezpieczenia, jak i do szantażu czy nawet zamachów terrorystycznych. Era informatyzacji daje zatem wiele nowych możliwości w dziedzinie walki informacyjnej, ale także dostarcza potencjalnemu przeciwnikowi nowych obszarów ataku (cyberprzestrzeń oraz sterowana poprzez sieć komputerową infrastruktura krytyczna). Z tych powodów konieczna jest ścisła współpraca państw członkowskich Unii Europejskiej w zakresie kontroli sposobu przepływu informacji (na szczeblu państwowym) oraz bezpieczeństwa sieci teleinformatycznych (w tym dostępu do nich). Kluczowe jest także budowanie świadomości w społeczeństwie (zarówno na poziomie instytucjonalnym, jak i jednostki) dotyczące rozwoju nowych technologii oraz tego, jakie to niesie ze sobą możliwości i ułatwienia, ale także zagrożenia. Unia Europejska koncentruje również znaczne wysiłki w obszarze wspólnej strategii ochrony infrastruktury krytycznej, co powinno być oparte na efektywnej współpracy transgranicznej, a także na wypracowaniu skutecznych mechanizmów na poziomie ponadnarodowym, gdyż tylko w ten sposób można przeciwstawić się zagrożeniom o charakterze asymetrycznym.

Bibliografia:

1. Antczak A., L. Elak, *Żołnierze CIMIC i oficerowie prasowi w operacjach międzynarodowych – wybrane aspekty*, Akademia Obrony Narodowej, Warszawa 2009.
2. Bógdał-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Warszawa 2003.
3. Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999.
4. Dudek W., *Międzynarodowe aspekty mass mediów*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 1991.
5. Jałoszyński K., Skosolas J., *Media wobec współczesnego zagrożenia terroryzmem*, Collegium Civitas, Warszawa 2008.
6. Mazur M., *Cybernetyka i charakter*, Wydawnictwo AULA, Podkowa Leśna 1976.
7. Mynarski S., *Elementy teorii systemów i cybernetyki*, Państwowe Wydawnictwo Naukowe, Warszawa 1979.
8. Kwećka R., *Informacja w walce zbrojnej*, Akademia Obrony Narodowej, Warszawa 2001.
9. Przybyłowicz P., *Wstęp do teorii informacji i kodowania*, Centrum Modelowania Matematycznego Sigma, Stalowa Wola 2008.
10. Sienkiewicz P., Jemioło T., Zacher L. (red.), *Szanse i zagrożenia rozwojowe w warunkach społeczeństwa informacyjnego*, Akademia Obrony Narodowej, Warszawa 2001.
11. Sun Zi, *Sztuka wojny*, Helion, Gliwice 2004.
12. Tipton H.F., Krause M. (red.), *Information Security Management*, Auerbach Publications, New York 2003.
13. Toffler H. i A., *Wojna i antywojna*, Świat Książki, Warszawa 1998.
14. Ursuł A. D., *Informacja*, 1971 za: Kulikowski J. L., *Informacja i świat w którym żyjemy,* 1978.
15. Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, Warszawa 2006.