JOANNA MAKOWSKA
Wyższa Szkoła Gospodarki Euroregionalnej w Józefowie

Cyberterroryzm kluczowym zagrożeniem dla bezpieczeństwa XXI wieku

The cyberterrorism as a key threat to the security of the XXI century

Streszczenie
Obecnie wciąż rozwijająca się technologia wywiera coraz to większy wpływ na życie i funkcjonowanie współczesnych ludzi. W społeczeństwie informatycznym zwycięzcą jest ten, kto ma dostęp do informacji oraz kto posiada umiejętności, by przetwarzać je w życiu codziennym. Obecnie informacja jest jedną z najistotniejszych wartości cywilizacyjnych, a dzięki dostępności do Internetu, będącego źródłem szeroko pojętej informacji, mamy do niej dostęp w zasadzie w każdej chwili. Szeroko pojętej informacji, ponieważ z jednej strony sieć jest potężnym źródłem wiedzy i korzystanie z niej przynosi wiele korzyści, lecz z drugiej – mieści się w niej także mnóstwo informacji fałszywych oraz niebezpieczeństw. Jednym z minusów sieci globalnej jest błyskawiczny rozwój cyberprzestępczości. Cyberterroryzm w dobie społeczeństwa informacyjnego jest jednym z najpoważniejszych zagrożeń, ponieważ w porównaniu z klasycznym terroryzmem ataki dokonywane są w cyberprzestrzeni. Zjawisko to stanowi poważne zagrożenie dla bezpieczeństwa teleinformatycznego państw oraz wspólnot międzynarodowych.

Słowa kluczowe: cyberterroryzm, cyberprzestrzeń, cyberprzestępczość, zagrożenie teleinformatyczne, system teleinformatyczny, ochrona systemu, ochrona informacji, infrastruktura krytyczna

Abstract
In today's world, the still growing technology exerts more and more influence on the life and functioning of modern humans. In the information society, the winner is the one who has access to information and who has the ability to process the information in everyday life. Currently, the information is one of the most important values of civilization and, due to the availability of the Internet being the source of widely understood information, we have access to it, in principle, at any time. It was said - widely understood informa-

tion, because on the one hand, the network is a powerful source of knowledge and the use of it brings many benefits. But, on the other hand, there are also a lot of false information and dangers. One of the disadvantages of the global network is the rapid development of cybercrime. The cyberterrorism, in the information society, is one of the most serious threats, because as compared to the classical terrorism, the attacks are carried out in the cyberspace. This phenomenon poses a serious threat to the ICT security of the states and the international communities.

Keywords: cyberterrorism, cyberspace, cybercrime, teleinformatic threat, teleinformatic system, system security, information security, critical infrastructure

Wprowadzenie

„Łamałem ludzi, nie hasła" – słowa te wypowiedział Kevin Mitnick, jeden z najpotężniejszych cyberprzestępców. Przy wykorzystaniu metod socjotechnicznych oraz używając swoich nadzwyczajnych umiejętności informatycznych, włamywał się do najważniejszych i najlepiej chronionych systemów informatycznych i wykradał z nich najważniejsze dane i informacje. Przez lata uciekał przed wymiarem sprawiedliwości Stanów Zjednoczonych. Skazano go łącznie na kilkaset lat pozbawienia wolności za przestępstwa komputerowe, zwolniono po zaledwie czterech latach, aby pełnił funkcję głównego doradcy ds. bezpieczeństwa w Pentagonie. Według niego to „Czynnik ludzki od wieków jest najsłabszym ogniwem bezpieczeństwa informacji" (Mitnick Simon, 2006). Słowa te nie brzmią zbyt groźnie, aczkolwiek zwracają uwagę na to, że to właśnie człowiek jest największym zagrożeniem w dostępie do informacji oraz w ich wycieku. Coraz większego znaczenia nabierają nowe kompetencje już nie tylko komunikacyjno-informacyjne, ale wprost ich wymiar cyfrowy (Andrzejewska, Bednarek, Ćmiel 3013, s. 24).

Obecnie informacja ma kluczowe znaczenie, a jej posiadanie jest wartością nadrzędną w sferze prywatnej, a przede wszystkim w strukturach państwowych. Gdy ściśle tajna informacja wpadnie w niepożądane ręce, może wywołać niebezpieczną w skutkach lawinę niebezpieczeństw zagrażających całemu społeczeństwu. Jest to najważniejszy problem całego społeczeństwa teleinformacyjnego, który wraz z szybkim rozwojem technologicznym wciąż przybiera nowe formy i nadal będzie ewoluował.

Zjawisko cyberterroryzmu jest znane od lat 80. XX wieku. Zainteresowanie terrorystów stosowaniem ataków cybernetycznych wzrosło po atakach na World Trade Center w Nowym Jorku. Od tego czasu w obronie przed cyberatakami

państwa zaczęły stosować bardziej zaawansowane systemy zabezpieczeń. Do najczęstszych celów ataków cyberterrorystów należą rządowe strony internetowe, infrastruktura krytyczna oraz infrastruktura bankowa.

Definicja oraz ogólne uwarunkowania cyberterroryzmu

Do tej pory nie przyjęto na świecie jednej definicji cyberterroryzmu. Specjaliści i naukowcy zajmujący się problematyką tego zjawiska wskazują na problem w zdefiniowaniu tego zagadnienia. W literaturze naukowej występuje kilkanaście różnych definicji cyberterroryzmu.

Oto kilka wybranych:

1. Cyberterroryzm jest to realna groźba lub bezprawny atak wymierzony w system informatyczny bądź zgromadzone dane w celu zastraszenia czy wymuszenia na władzach państwowych ustępstw lub oczekiwanych zachowań. Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu (Szubrycht 2005).
2. Według R. Kośli cyberterroryzm to działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy (Lichocki 2008).
3. Za cyberterroryzm należy uznać politycznie umotywowany atak lub groźbę ataku na komputery, sieci lub systemy informatyczne dla zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów (Liedel 2005, s. 36).

Dzięki szybkiemu rozwojowi technologicznemu pojawiają się w sposób dynamiczny i powszechny nowe zagrożenia, wynikające nie tylko z przebywania w sieci, ale także z jej inspiracji (Andrzejewska, Bednarek, Ćmiel 2013, s. 7). Do takich należy również cyberterroryzm, który przybiera nowe, coraz bardziej wyszukane oraz skomplikowane formy. Jednak już wyżej wymienione definicje potwierdzają, że cyberprzestrzeń stanowi nową płaszczyznę ataków między wrogimi sobie państwami. Sam cyberterroryzm stał się jednym z najważniejszych wyzwań XXI wieku (Bógdał-Brzezińska, Gawrycki 2003, s. 76). Wpływ na to ma kilka czynników:

a) niewielkie koszty materialne – przygotowanie ataku nie wymaga wysokich nakładów finansowych, lecz specjalistycznej wiedzy. Koszty przeprowadzenia cyberataku mogą być o wiele niższe niż w przypadku klasycznego zamachu terrorystycznego;
b) dostosowywanie środków do działań – istota teorii wyboru racjonalnego mówi, iż „kiedy ludzie mają do wyboru kilka sposobów działania, zwykle robią to, co w świetle ich przypuszczeń zapewni im najlepszy wynik" (Elster 1986, s. 22). Inaczej mówiąc, ludzie dostosowują swoje działania w taki sposób, by maksymalnie zwiększyć pozytywny dla nich wynik. Terroryści wybierając cyberatak, postrzegają go jako wybór najbardziej racjonalny prowadzący do skuteczności ich działań, a w konsekwencji osiągania zamierzonych efektów. Cyberataki ograniczają także konieczność narażenia życia, gdyż nie wymagają kroków tak drastycznych, jak np. ataki samobójcze;
c) anonimowość – cyberterroryści mogą być pewni, że prowadzone przez nich działania nie zostaną wykryte, a oni zlokalizowani. Powoduje to utrudnienie państwom odparcia ataku;
d) cechy środowiska działania – dzięki Internetowi cyberterroryści mają niczym nieograniczoną swobodę w planowaniu i koordynowaniu swoich działań. Terroryści mogą przygotowywać atak, będąc w różnych miejscach na świecie. Nie ogranicza ich ani czas, ani miejsce. Również dostęp do narzędzi potrzebnych do przeprowadzenia cyberataku nie jest problemem – komputer z dostępem do Internetu jest przedmiotem użytku codziennego;
e) zasięg globalny ataku – globalna sieć połączeń sprawia, iż można przeprowadzać ataki z każdego miejsca na ziemi, jak też uderzyć w niemal każdy obiekt na świecie.

Cyberterroryzm zawsze będzie przynosił straty materialne oraz ludzkie. Bezpieczeństwo dowolnego podmiotu, obiektu, stanu rzeczy występuje wtedy, gdy obiekt czy stan rzeczy może trwać bez większego ryzyka jego zniszczenia (Zawisza, Ćmiel 2012). Można postawić tezę, że prowadzenie cyberataku zawsze jest wielowymiarowe i kaskadowe. Bezpośrednio uderza on w bazy danych, przyczynia się do destrukcji i dezorganizacji życia danej społeczności. Ataki na systemy: energetyczne, zaopatrywania w żywność, zaopatrywania

w wodę, łączności, transportu, zdrowia, bankowości, urzędy państwowe są klasycznymi przykładami działań zagrażających życiu i zdrowiu ludzi. Tym samym sposobem można obezwładnić system obronny państwa. Procesy rozwoju wskazują, że najdoskonalszą instytucją zapewniającą potrzeby jednostki w zakresie bezpieczeństwa jest państwo ze wszystkimi jego atrybutami w układzie międzynarodowym (Pokruszyński 2011, s. 64).

Niejednokrotnie wiele krajów na świecie lekceważy fakt, iż ataki cyberterrorystyczne mogą stać się śmiertelnym zagrożeniem poprzez:

a) możliwość destrukcyjnego wpływu na działalność wielu instytucji zarówno państwowych, jak i niepaństwowych,
b) zakłócenia i przeciążenia linii komunikacji alarmowej,
c) zakłócenia w ruchu lotniczym,
d) uszkodzenie oprogramowania komputerowego używanego w ratownictwie medycznym,
e) zmiany ciśnienia w gazociągach mogące prowadzić do wybuchu,
f) kradzież tożsamości,
g) uzyskiwanie dostępu do sieci teleinformacyjnych i teleinformatycznych oraz zmianę krytycznych danych,
h) zakłócenie mediów i przedstawianie fałszywego obrazu sytuacji,
i) sabotaż danych na rynkach finansowych.

Działania w zakresie budowania bezpieczeństwa cybernetycznego

1. Prewencja
   a) wprowadzenie różnorodnych elementów zabezpieczających już na etapie projektowania danego systemu. Dawniej bezpieczeństwo nie było tak ważnym kryterium przy tworzeniu systemów, bardziej skupiano się na ich funkcjonalności. Obecnie owe proporcje winny zostać zmienione. Bezpieczeństwo powinno się stać najważniejszym komponentem projektowanych systemów teleinformatycznych;
   b) zabezpieczenie czynnika ludzkiego – wzmożenie ochrony przed niepożądanymi osobami, które mogą mieć dostęp do ważnych elementów systemu, oraz dokładne sprawdzanie osób, które ze względu na pełnioną funkcję mogą być narażone na werbowanie przez terrorystów;

c) zakazy prawne – stworzenie prawa, które będzie jasno określać karalność poszczególnych czynów. Konieczna jest tutaj koordynacja międzynarodowych rozwiązań prawnych prowadzących do większej współpracy przy zwalczaniu ataków międzynarodowych;
d) działania odstraszające – tworzenie i ogłaszanie aktów pokazujących osiągnięcia technologiczne i możliwości państw. Celem takich działań jest pokazanie potencjalnym cyberterrorystom, że ich próby ataków mogą zakończyć się fiaskiem bądź stanowczym odzewem.

2. Zarządzanie incydentami, łagodzenie ataków oraz minimalizowanie szkód
   a) zwiększenie efektywności ostrzegania – wprowadzenie efektywnych systemów alarmowania oraz wskaźników szybko wykrywających atak;
   b) wzmożenie ochrony systemu – zwłaszcza w kwestii ochrony infrastruktury krytycznej istotne jest budowanie mocniejszych barier ochronnych, rozumianych zarówno w sensie cybernetycznym, jak i fizycznym. W pierwszym przypadku najpowszechniejsze jest zastosowanie systemu haseł. Innymi możliwościami są zapory sieciowe (*firewalls*) i serwery proxy;
   c) tworzenie wersji zapasowych i kopii danych. W przypadku uszkodzenia informacji utworzone kopie najistotniejszych elementów systemu pozwalają na szybkie przywrócenie jego funkcjonowania;
   d) opracowywanie i bieżące aktualizowanie polityki obronnej. Każdy podmiot powinien mieć przygotowaną oraz wdrożoną politykę ochronną systemu, która określa podstawowe funkcje i zadania wszystkich zaangażowanych.
3. Minimalizowanie zaistniałych szkód;
   a) regeneracja – zrekonstruowanie uszkodzonych elementów najszybciej jak to możliwe;
   b) odpowiedź – ukaranie sprawcy ataku oraz przeprowadzenie akcji odwetowej. Większa efektywność międzynarodowej współpracy
   c) wytworzenie i koordynowanie prawnych rozwiązań, które nie tylko pozwolą na zidentyfikowanie i ściganie przestępstw, lecz także umożliwią przeprowadzanie natychmiastowej, wspólnej reakcji w przypadku zaistnienia ataku;
   d) utworzenie wspólnej, jednakowej terminologii, która pozwala na szybką wymianę informacji potrzebną do zidentyfikowania zagrożenia oraz jego zwalczenia;

e) upowszechnianie wiedzy o technicznych możliwościach partnerów zaangażowanych w zwalczanie cyberataków;
f) tworzenie porozumień międzynarodowych w celu walki z cyberprzestępczością.

4. W porozumienia te powinno angażować się jak najwięcej podmiotów
   a) tworzenie otwartych struktur organizacyjnych porozumień międzynarodowych kierowanych na zwiększenie bezpieczeństwa w cyberprzestrzeni – dających podmiotom biorącym w nich udział możliwość zgłaszania sytuacji niepokojących i werbalizowania ich obaw;
   b) tworzenie oraz przestrzeganie standardów, które nie będą dopuszczały do sytuacji, w których jednostki poprzez dostęp do grupowych informacji oraz osiągnięć swych sojuszników będą działać na szkodę innych.
5. Efektywniejsza ochrona technologicznej infrastruktury krytycznej państwa
   Sprowadza się do ulepszania i zwiększania ilości rozwiązań technologicznych chroniących systemy, które obsługują tę infrastrukturę. Znacznie więcej systemów chroniących teleinformatyczną infrastrukturę krytyczną państwa posiadają podmioty prywatne. A zatem w interesie państwa, jak również w zakresie jego obowiązków jest zadbanie o to, by spełniały one najwyższe standardy cyberochrony. Konieczne jest również doskonalenie komunikacji pomiędzy podmiotami prywatnymi a państwowymi, bowiem w przypadku ataku tylko prawidłowo skoordynowana akcja może zapobiec stratom bądź je zminimalizować.
6. Profesjonalizacja sektora zwalczającego cyberprzestępczość
   Dostosowanie przepisów prawa do ewoluujących zagrożeń, a zwłaszcza dostosowanie możliwości organów zajmujących się ściganiem i sądzeniem cyberprzestępców, polega między innymi na angażowaniu specjalistów z branży IT, którzy dzięki swojej wiedzy i doświadczeniu są w stanie realnie wesprzeć osoby zaangażowane w ten proces.

Działania Polski dotyczące walki z cyberterroryzmem

W Polsce, jak również w innych krajach Unii Europejskiej obserwuje się stały rozwój technologii teleinformatycznej, a co za tym idzie – rozwój sieci bezprzewodowych. Brak uświadomienia niebezpieczeństw wynikających z nieodpowiednich zabezpieczeń teleinformatycznych sieci bezprzewodowych przed atakiem cyber-

netycznym jest największym zagrożeniem dla bezpieczeństwa teleinformatycznego państwa polskiego. Brak odpowiedniego wykształcenia i wyobraźni administratorów sieci może prowadzić do tragicznych w skutkach efektów.

W celu przeciwdziałania zagrożeniom cyberterrorystycznym oraz zapewnienia bezpieczeństwa teleinformatycznego kraju na odpowiednim poziomie powołano 1 lutego 2008 r. Rządowy Zespół Reagowania na Incydenty Komputerowe (RZRnIK) CERT.GOV.PL.

Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni funkcję głównego zespołu CERT w obszarze administracji rządowej oraz obszarze cywilnym. Jego podstawowym zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą sieci i systemy teleinformatyczne, których zakłócenie bądź zniszczenie może stanowić zagrożenie dla zdrowia lub życia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa[1]. Do zadań CERT.GOV.PL należy:

1. Koordynowanie reagowania na incydenty.
2. Publikowanie alertów i ostrzeżeń.
3. Obsługiwanie i analizowanie incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych).
4. Publikowanie powiadomień (biuletynów zabezpieczeń).
5. Koordynowanie reagowania na luki w zabezpieczeniach.
6. Obsługiwanie zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV.
7. Przeprowadzanie testów bezpieczeństwa.

Celami RZRnIK są:

1. Kreowanie polityki bezpieczeństwa w kwestii ochrony przed cyberzagrożeniami.

[1] Pozyskano z http://www.cert.gov.pl/cer/o-nas/15,O-nas.html, dostęp: 17.06.2014.

2. Koordynacja przepływu informacji pomiędzy podmiotami w związku z cyberatakami.
3. Wykrywanie cyberataków, ich rozpoznawanie i przeciwdziałanie im.
4. Międzynarodowa współpraca w zakresie ochrony cyberprzestrzeni.
5. Pełnienie nadrzędnej roli w stosunku do wszelkich krajowych organizacji, instytucji oraz podmiotów resortowych w zakresie ochrony cyberprzestrzeni.
6. Gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla IKP.
7. Reagowanie na incydenty bezpieczeństwa teleinformatycznego, głównie z uwzględnieniem IKP.
8. Analiza powłamaniowa przy wykorzystaniu narzędzi informatyki śledczej.
9. Tworzenie polityki ochrony cyberprzestrzeni RP.
10. Prowadzenie szkoleń dla administracji rządowej i samorządowej.
11. Doradztwo i konsulting w zakresie cyberbezpieczeństwa.

Ministerstwo Spraw Wewnętrznych i Administracji opracowało rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, będący kontynuacją wcześniejszego projektu rządowego opracowanego przez tę samą jednostkę na lata 2009–2011, którego strategicznym celem jest zapewnienie ciągłości bezpieczeństwa cyberprzestrzeni państwa.

Celami szczegółowymi programu są:

1. Zwiększenie poziomu bezpieczeństwa teleinformatycznej infrastruktury krytycznej kraju.
2. Zmniejszenie skutków naruszenia bezpieczeństwa w cyberprzestrzeni.
3. Zdefiniowanie kompetencji odpowiedzialnych za ochronę cyberprzestrzeni podmiotów.
4. Stworzenie oraz realizowanie spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.
5. Stworzenie trwałego systemu koordynacji oraz wymiany informacji pomiędzy zarówno podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni, jak i przedsiębiorcami dostarczającymi usługi w cyberprzestrzeni i operatorami teleinformatycznej infrastruktury krytycznej.

6. Zwiększenie świadomości użytkowników w kwestii metod i środków bezpieczeństwa w cyberprzestrzeni.

Cele programu realizowane będą poprzez:

1. Stworzenie systemu koordynacji reagowania i przeciwdziałania cyberzagrożeniom, w tym atakom o charakterze cyberterrorystycznym.
2. Powszechne wdrożenie do jednostek administracji publicznej, jak również podmiotów niepublicznych, mechanizmów służących do zapobiegania zagrożeniom i wczesnego ich wykrywania dla bezpieczeństwa cyberprzestrzeni oraz do właściwego postępowania w przypadku stwierdzonych incydentów.
3. Powszechną edukację społeczną oraz edukację specjalistyczną w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej.

W projekcie dużą wagę obok działań proceduralno-organizacyjnych przywiązuje się do szeroko pojętej edukacji. Zaliczane są do niej szkolenia, specjalnie tworzone programy, jak też kampanie społeczne, prowadzone na różnych szczeblach. Odbiorcami są zarówno pracownicy administracji publicznej, jak i inni użytkownicy cyberprzestrzeni. Program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej zwraca również szczególną uwagę na dopływ odpowiednio wyszkolonych specjalistów w dziedzinie bezpieczeństwa teleinformatycznego. Projekt zakłada zaangażowanie uczelni wyższych w program ochrony cyberprzestrzeni. Zagadnienia związane z bezpieczeństwem cyberprzestrzeni powinny stać się stałym elementem każdego programu nauczania. Zadanie propagowania zmian w kwestii programów nauczania należy do obowiązków Ministra Nauki i Szkolnictwa Wyższego[2].

Międzynarodowy system walki z cyberprzestępczością

1. NATO

Na szczycie NATO w Pradze, w listopadzie 2002 roku podjęto decyzję o uruchomieniu Programu Obrony Cybernetycznej – *The Cyber Defense Program* oraz rozwoju Zdolności Reagowania na Incydenty Komputerowe – *The Com-*

[2] Pozyskano z http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf, dostęp: 18.06.2014.

puter Incident Response Capability. W styczniu 2008 roku przyjęto Strategię Obrony Cybernetycznej – *The Policy on Cyber Defence*, a w maju 2008 roku w Brukseli szefowie Sztabów Generalnych Łotwy, Estonii, Litwy, Niemiec, Hiszpanii, Włoch i Słowacji oraz Sojusznicze Dowództwo Transformacji (*The Allied Command Transformation* – ACT) podpisali Memorandum o utworzeniu w Tallinie Centrum Kompetencyjnego do spraw Obrony Teleinformatycznej – *The Concept for Cooperative Cyber Defense Centre of Excellence* (CCD-COE). W październiku 2008 roku Rada Północnoatlantycka przyznała Centrum Kompetencyjnemu pełną akredytację jako *The NATO Centre of Excellence* i status *The International Military Organization* – IMO. Centrum nie jest jednostką operacyjną ani nie podlega strukturom dowodzenia NATO. W listopadzie 2011 roku do CCDCOE przystąpiła Polska oraz Stany Zjednoczone. Stosowne zapisy dotyczące bezpieczeństwa w cyberprzestrzeni znalazły się również w nowej Koncepcji Strategicznej NATO z listopada 2010 roku. W czerwcu 2011 roku ministrowie obrony państw członkowskich NATO przyjęli dokument pod nazwą Polityka NATO w obszarze cyberobrony (*The NATO Policy on Cyber Defence*) oraz Plan działania (*The Cyber Defence Action Plan*).

2. ONZ

Organizacja Narodów Zjednoczonych także posiada swoją wyspecjalizowaną agencję do spraw cyberbezpieczeństwa – ITU International Telecommunications Union. Należą do niej tak państwa (także Polska), jak podmioty gospodarcze (polskie – Polkomtel S.A., Telekomunikacja Polska S.A. oraz NASK). W 2007 roku ITU ogłosiło plan pn. „Global Cybersecurity Agenda", będący projektem wprowadzenia współpracy międzynarodowej w celu wzmocnienia bezpieczeństwa w środowisku informatycznym. Dokument ten ukazuje strategię opierającą się na pięciu filarach. Są nimi:

a) prawne środki – GCA zawiera przykładowe słowa użyteczne np. przy wprowadzaniu legislatury, a także przewodnik dla krajów rozwijających się;
b) środki proceduralne i techniczne – ITU dąży do wprowadzenia standaryzacji rozwiązań stosowanych w telekomunikacji;
c) struktury organizacyjne – ITU współpracuje z krajami członkowskimi we wprowadzaniu lepszych procedur zabezpieczających przed cyberincydentami, także z innymi organizacjami, np. z IMPACT;

d) budowanie potencjału – ITU dąży do szerzenia świadomości cyberzagrożeń wśród użytkowników serwisów sieciowych. GCA zawiera narzędzia pozwalające określić możliwości państw członkowskich do reagowania na wyzwania w zakresie cyberbezpieczeństwa;
e) międzynarodowa współpraca – ITU współpracuje z wieloma organizacjami w obszarze bezpieczeństwa telekomunikacyjnego, m.in. z IMPACT czy z High Level Expert Group.

3. IMPACT

IMPACT, czyli International Multilateral Partnership Against Cyber-Terrorism, to międzynarodowy projekt współpracy sektora publicznego w celu implementacji najskuteczniejszych metod zwalczania cyberterroryzmu.

Głównym powodem powstania organizacji IMPACT było przeświadczenie, że jedyną odpowiedzią na światowe zagrożenie cyberterroryzmem może być stworzenie organizacji globalnej. Dlatego IMPACT – formacja, która działa od 2008 roku – zrzesza państwa z całego świata, w tym także należące do ITU (również Polskę). Główna kwatera IMPACT jest też miejscem pracy grupy operacyjnej Global Cybersecurity Agenda formalnie należącego do ITU. Obie te organizacje współpracują ze sobą bardzo ściśle, co służy nie tylko ich interesom, ale głównie interesom podmiotów należących do obu lub tylko jednego systemu członkostwa.

IMPACT podzielony jest na następujące działy tematyczne: Global Response Center, Centre for Training & Skills Development, Centre for Policy & International Cooperation, Centre for Security Assurance & Research[3]. Koncentruje się na trzech najważniejszych obszarach działalności: szkolenia, certyfikaty bezpieczeństwa oraz badania i rozwój.

4. Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (ENISA)

Celem ENISA jest rozszerzenie możliwości UE, krajów członkowskich oraz sektora biznesu w kwestii ochrony, określania problemów dotyczących bezpieczeństwa sieci i informacji oraz reagowania na nie.

[3] Pozyskano z http://www.impact-alliance.org/download/pdf/about-us/IMPACT-organization-chart2014.pdf, dostęp: 18.06.2014.

Poza tym ENISA oferuje państwom Unii Europejskiej pomoc oraz doradztwo. Na żądanie państw wspiera je w technicznych pracach przygotowawczych odnoszących się do aktualizacji, jak też rozwoju ustawodawstwa europejskiego. Ułatwia także oraz rozszerza współpracę pomiędzy różnymi podmiotami działającymi w sektorze prywatnym i publicznym w celu osiągnięcia odpowiednio wysokiego poziomu bezpieczeństwa w państwach Unii Europejskiej.

Jej zadaniami są:

a) zbieranie właściwych informacji w celu analizowania bieżącego oraz powstającego ryzyka i przekazywanie wyników państwom UE,
b) oferowanie doradztwa, a w niektórych przypadkach pomoc Parlamentowi Europejskiemu oraz właściwym organom krajowym i europejskim,
c) rozszerzanie współpracy pomiędzy różnymi instytucjami w sektorze (np. poprzez tworzenie sieci kontaktów i konsultacje),
d) ułatwianie współpracy pomiędzy Komisją a państwami Unii Europejskiej w zakresie rozwoju wspólnych metodologii w celu zapobiegania problemom dotyczącym bezpieczeństwa,
e) przyczynianie się do wzrostu świadomości i dostępności aktualnych, celowych oraz wszechstronnych informacji na temat bezpieczeństwa sieci i informacji w stosunku do wszystkich użytkowników (m.in. poprzez promowanie wymiany najlepszych praktyk, w tym metod ostrzegania użytkowników, i poszukiwanie współdziałania między inicjatywami w sektorze prywatnym i publicznym),
f) wspieranie państw UE w ich dialogu z przemysłem w celu określania problemów dotyczących bezpieczeństwa oprogramowania i sprzętu,
g) śledzenie rozwoju norm bezpieczeństwa w zakresie usług i produktów oraz promowanie działania w zakresie oceny ryzyka i zarządzania nim, uczestniczenie w wysiłkach UE zmierzających do współpracy z organizacjami międzynarodowymi i krajami trzecimi w celu promowania globalnej propozycji dotyczącej bezpieczeństwa[4].

[4] Pozyskano z http://europa.eu/legislation_summaries/information_society/internet/l24153_pl.htm, dostęp: 18.06.2014.

Podsumowanie

Cyberprzestrzeń wraz z Internetem stworzyła bardzo ważne zależności, które w sposób poważny i nieprzewidywalny zmieniają swoją naturę. Systemy teleinformatyczne, a w szczególności zawarte w nich oprogramowanie mają wiele słabych punktów mogących umożliwić przeprowadzenie cyberataku i obniżyć tym samym w sposób bardzo istotny bezpieczeństwo teleinformatyczne i informacyjne.

Powszechność korzystania z Internetu, jak też wciąż zwiększająca się ilość dostępnych usług oferowanych przez sieć sprawiają, iż konieczne jest uwrażliwienie społeczeństwa na problem bezpieczeństwa teleinformatycznego oraz podniesienie jego świadomości odnośnie do bezpiecznego korzystania z Internetu. Każdy użytkownik komputera powinien pamiętać o tym, że korzystanie z sieci globalnej, oprócz korzyści, niesie również szereg zagrożeń, że wcześniej czy później zetknie się z nimi, nawet tego nie zauważając. Dlatego tak istotne jest szerzenie wśród społeczeństwa świadomości istnienia wielu niebezpieczeństw w globalnej sieci oraz konieczności przeciwdziałania cyberzagrożeniom. Wiedza na temat sposobów przeciwdziałania cyberzagrożeniom i ich zwalczania stanowi kluczowy element walki z nimi.

Jedynie odpowiedzialne zachowanie użytkownika może skutecznie zminimalizować ryzyko wynikające z istniejących zagrożeń. W świecie współczesnym zapewnienie bezpieczeństwa teleinformatycznego nie zależy wyłącznie od specjalistów do spraw bezpieczeństwa teleinformatycznego działalności oraz wyspecjalizowanych instytucji rządowych. Odpowiedzialność za bezpieczeństwo w cyberprzestrzeni spoczywa na każdym użytkowniku komputera, bez pozwalania sobie na niewiedzę bądź niefrasobliwość, gdyż taka nieuwaga może nie zakończyć się dobrze.

Wobec tego pedagogika, a zwłaszcza edukacja medialna powinna zwrócić uwagę na zagrożenia, jakie niesie cyberterroryzm. Istotne znaczenie ma także poszukiwanie nowych metod działania wobec współczesnych wyzwań i zagrożeń bezpieczeństwa (Pokruszyński 2012, s. 30), także bezpieczeństwa w cyberprzestrzeni.

Bibliografia

Andrzejewska A., Bednarek J., Ćmiel S., *Człowiek w świecie rzeczywistym i wirtualnym. Nowy wymiar zagrożeń w świecie realnym i wirtualnym.* Wydawnictwo WSGE w Józefowie, Józefów 2013.

Andrzejewska A., Bednarek J., Ćmiel S., *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*. Wydawnictwo WSGE w Józefowie, Józefów 2013.

Bógdał-Brzezińska A., Gawrycki F.M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Wydawnictwo ASPRA-JR, Warszawa 2003.

Elster J., *Nuts and Bolt for the Social Sciences.* Cambridge, UK 1986.

Lichocki E., *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*. Wydawnictwo PAN, Warszawa 2008.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Wydawnictwo Adam Marszałek, Toruń 2005.

Mitnick K.D., Simon W.L., *Sztuka infiltracji, czyli jak włamywać się do sieci komputerowych.* Wydawnictwo Albatros, Gliwice 2006.

Pokruszyński W., *Bezpieczeństwo – teoria i praktyka.* Wydawnictwo WSGE w Józefowie, Józefów 2012.

Pokruszyński W., *Polityka i strategia bezpieczeństwa.* Wydawnictwo WSGE w Józefowie, Józefów 2011.

Suchorzewska A., *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzmem*. Wydawnictwo Wolters Kluwer 2010.

Szubrycht T., *Zeszyty naukowe Akademii Marynarki Wojennej*, Rok XLVI (2005) nr 1 (160).

Zawisza J., Ćmiel S., *Filozoficzne aspekty bezpieczeństwa strukturalnego w kontekście bezpieczeństwa narodowego i międzynarodowego.* Wydawnictwo WSGE w Józefowie, Józefów 2012.

Źródła internetowe

http://bip.msw.gov.pl/download/4/7445/RPOC__24_09_2010.pdf, dostęp: 18.06.2014.

http://europa.eu/legislation_summaries/information_society/internet/l24153_pl.htm, dostęp: 18.06.2014.

http://www.cert.gov.pl/cer/o-nas/15,O-nas.html, dostęp: 17.06.2014.

http://www.impact-alliance.org/download/pdf/about-us/IMPACT-organization-chart2014.pdf, dostęp: 18.06.2014.