Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa

Jakub Kowalewski

Marian Kowalewski

W artykule zaprezentowano określenia związane z cyberterroryzmem oraz jego istotę. Następnie przedstawiono kategorie przestępstw popełnianych w cyberprzestrzeni, rodzaje, formy oraz scenariusz ataku w cyberprzestrzeni. Zwrócono uwagę na metody i sposoby przeciwdziałania temu szczególnemu zagrożeniu oraz na uwarunkowania prawne ochrony cyberprzestrzeni.

Ataki w cyberprzestrzeni, cyberterroryzm, ochrona cyberprzestrzeni

Wprowadzenie

Informacja jako zasób społeczeństwa informacyjnego jest nieodzownym elementem postępu i rozwoju cywilizacyjnego. Ten niezwykle istotny i ważny fakt niesie ze sobą znaczne zadania i problemy związane z bezpieczeństwem przetwarzania, przesyłania i gromadzenia informacji. Dzięki rozwojowi nauki oraz stosowania nowoczesnych technik i technologii informacyjnych, teleinformatycznych i telekomunikacyjnych problemy te są systematycznie przezwyciężane.

Proces ten byłby zbyt prosty, gdyby dotyczył tyko powstających w sposób naturalny problemów. Niestety, tak nie jest, informacja jako zasób współczesnych społeczeństw stała się także obiektem i środkiem niepożądanej modyfikacji, kradzieży, wywiadu i ataku. Co więcej, stała się środkiem prowadzenia wojny informacyjnej oraz ataku w cyberprzestrzeni. W swej istocie informacja poza dobrem, jakie ze sobą niesie, stwarza znaczne zagrożenia dla społeczeństw i ich obywateli. Stała się środkiem niebezpiecznym w rękach przestępców i terrorystów oraz środkiem walki i ataku wymagającym zdecydowanego przeciwdziałania organizacji, państw i narodów w wymiarze globalnym, regionalnym, krajowym i lokalnym.

Istota i określenie cyberterroryzmu

Z uwagi na różne określenia cyberterroryzmu [1]-[6] warto uznać za najbardziej trafne i obowiązujące definicje zawarte w Rządowym programie ochrony cyberprzestrzeni RP na lata 2011-2016 [4] i przyjąć do rozważań następujące definicje:

- cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami,
- cyberprzestrzeń Rzeczypospolitej Polskiej – cyberprzestrzeń w obrębie terytorium Państwa Polskiego i w lokalizacjach poza jego terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe),
- cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni;
- cyberterroryzm – cyberprzestępstwo o charakterze terrorystycznym,

- cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, bez angażowania personelu lub innych użytkowników,
- ochrona cyberprzestrzeni – zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni.

Cyberterroryzm powstał na gruncie terroryzmu z wykorzystaniem nowego obszaru działania, jakim jest cyberprzestrzeń. W przestrzeni tej funkcjonują najnowsze osiągnięcia współczesnej cywilizacji informacyjnej, techniki oraz technologie informacyjne, teleinformatyczne i telekomunikacyjne.

Terroryzm to metoda działania polegająca na przemocy wobec innych, pojedynczych ważnych osób, zbiorowisk ludzkich lub wobec przypadkowych grup ludzi znajdujących się w różnych obiektach na terenie kraju, np. w miejscach pracy, w środkach komunikacyjnych, w różnego rodzaju lokalach itp. Terroryzm ma różne formy, między innymi są to klasyczne akty kryminalne (morderstwa, podpalenia) i inne, które polegają na celowym wywołaniu terroru, tzn. wywołaniu niepewności, paniki, zastraszenia w celu osiągnięcia zamierzeń politycznych lub zmuszenia organu władzy publicznej do podjęcia lub zaniechania określonych czynności.

Wspólnymi cechami terroryzmu i cyberterroryzmu jest stosowanie przemocy w celu wywołania zamierzonych i wskazanych powyżej skutków i celów. Z uwagi na ich medialność w społeczeństwie, wspólnym składnikiem jest wywołanie lęku, niepewności i zastraszenia.

Aktorami cyberterroryzmu są głównie osoby i organizacje, grupy kryminalne, wspierane przez cyberterrorystów oraz państwa stosujące terroryzm.

Kategorie i rodzaje przestępstw oraz zagrożeń w cyberprzestrzeni

W literaturze spotyka się szereg informacji na temat kategorii i rodzajów przestępstw w cyberprzestrzeni. Na szczególna uwagę zasługuje pogląd Rady Europy wyrażony w Konwencji ETS 185 [7], w której wyróżnia się cztery zasadnicze grupy tego rodzaju przestępstw:

- przeciw poufności, integralności i dostępności danych, np.: nielegalny dostęp do systemów poprzez hacking, podsłuch, oszukiwanie uprawnionych użytkowników, szpiegostwo komputerowe (trojany i inne techniki), sabotaż i wymuszenia komputerowe (np. wirusy, ataki DDoS, spam),
- powiązane z komputerami i sieciami: od przestępstw klasycznych (np. manipulacja fakturami, kontami firmowymi, oszukańcze aukcje, nielegalne używanie kart kredytowych), poprzez komputerowe podróbki, po atak na życie ludzkie (np. manipulowanie systemami szpitalnymi, zdrowia ludzkiego, kontroli ruchu powietrznego),
- powiązane z zawartością (treścią), np.: dziecięca pornografia, dostarczanie przestępczych instrukcji, oferowanie popełnienia przestępstw, molestowanie i mobbing poprzez sieć, rozpowszechnianie fałszywych informacji, internetowy hazard,
- związane z naruszeniem prawa autorskiego i praw pokrewnych: np. nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych.

W literaturze przedmiotu podkreśla się wymienione przestępstwa i zagrożenia oraz wskazuje na szereg innych, które niesie z sobą cyberprzestepczość. Niektóre z nich to [8]:

- usługi finansowe on-line (wirtualny hazard, tzw. oszustwa nigeryjskie),
- cyberlaundering – wykorzystywanie e-bankowości i e-handlu internetowego do prania brudnych

pieniędzy, tzn. możliwości cyfrowego pieniądza i handlu w Internecie połączonych z anonimowością oraz brakiem uregulowań i kontroli w tym zakresie,

- cybersguatting (dziki lokator internetowy) – niedozwolona praktyka rejestrowania domen internetowych (o cechach znanych osób, firm, instytucji) i ich odsprzedaży właścicielowi (np. zarejestrowanego znaku towarowego) często po zawyżonej cenie,
- plagiaty, kradzież utworów chronionych prawami autorskimi,
- rozpowszechnianie pornografii i pedofilii, niedozwolonych treści, np. nazistowskich, rasistowskich,
- nielegalny handel, antykami, dziełami sztuki, zwierzętami, bronią, medykamentami, materiałami radioaktywnymi,
- szpiegostwo, nielegalny podsłuch, włamania do systemów komputerowych – hacking.

Ponadto, na uwagę zasługuje stanowisko Agencji Bezpieczeństwa Wewnętrznego [9], które do zagrożeń i ataków w cyberprzestrzeni zalicza:

- podmianę treści witryn internetowych,
- infekcję poprzez strony WWW,
- phishing – atak polegający na wyszukiwaniu poufnych informacji osobistych (np. haseł, danych kart kredytowych itp.) przez podszywanie się pod zaufaną osobę lub instytucję,
- botnety – grupy zainfekowanych komputerów (np. wirusami lub robakami komputerowymi), podstępnie – bez wiedzy ich użytkowników, w celu zdalnej penetracji i kradzieży informacji za pomocą tych komputerów,
- szpiegostwo komputerowe i przemysłowe oraz wywiad komputerowy – elektroniczny.

Powyżej przytoczone stanowiska i stwierdzenia świadczą o niebezpieczeństwie i skali zagrożeń, jakie niesie sobą cyberterroryzm. Analiza literatury wskazuje, że obecnie w cyberprzestrzeni stosuje się następujące rodzaje ataków:

- SYN flood,
- DoS (Denial of Service),
- DDoS (Distributed Denial of Service),
- DRDoS (Distributed Reflection Denial of Service),
- Fork-bomba (Fork Bomb).

Są to ataki, które nie doprowadzają intruza do uzyskania dostępu do informacji w systemie, nie powodują też utraty i kradzieży danych. Powodują zablokowanie pracy sieci i usług, co w efekcie ogranicza i uniemożliwia (na określony czas) funkcjonowanie organizacji i naraża ją na znaczne straty i koszty.

SYN Flood - celem ataku jest zablokowanie serwera sieci komputerowej przy wykorzystaniu protokółu TCP, a jego rezultatem jest znaczne przeciążenie sieci komputerowej. Sposób ataku polega na wysyłaniu dużej liczby pakietów z odpowiednią w nagłówku flagą w synchronizacji (SYN) i zazwyczaj ze sfałszowanym adresem IP nadawcy, w celu jego „zalania" dużą liczbą pakietów inicjujących połączenie.

DoS – celem ataku DoS jest uniemożliwienie działania sieci komputerowej i jej usług, poprzez wykorzystanie do tego celu błędów w protokołach i aplikacjach. Sposób ataku polega na przeciążeniu aplikacji serwującej określone dane poprzez wysyłanie dużej liczby pakietów w celu wyczerpania zasobów systemu, tak by doprowadzić do załamania pracy aplikacji. Inne metody to przeciążenie pracy łączy klientów o ograniczonej przepustowości do stanu takiego, że brak jest możliwości świadczenia

usług oraz ograniczenie dostępu do zasobów komputerowych (pamięci operacyjnej, mocy obliczeniowej procesora, przestrzeni dyskowej).

Rezultatem ataku jest załamanie pracy aplikacji świadczących usługi, blokowanie dostępu do zasobów sieci i usług, straty dla organizacji. DoS jest atakiem wykonanym z jednego komputera.

DDoS - to odmiana ataku DoS wykonana z kilkuset lub kilku tysięcy komputerów jednocześnie w celu wzmocnienia skuteczności ataku, czyli uniemożliwienia działania sieci komputerowej i jej usług. Atak rozpoczyna się z komputera klienta, który wysyła odpowiedni rozkaz do węzłów, te z kolei wysyłają go dalej do agentów, aby przeprowadzić atak na ofiarę. Rezultatem jest załamanie pracy aplikacji świadczących usługi, blokowanie dostępu do zasobów sieci i usług z większą skutecznością niż atak DoS, znaczne straty i koszty dla organizacji. W ataku typu DDoS stosuje się zombie – komputer podłączony do internetu z zainstalowanym oprogramowaniem, umożliwiającym bez wiedzy jego użytkownika, zdalne sterowanie z zewnątrz.

DRDoS - to jedna z nowszych odmian ataku DoS, którego celem jest uniemożliwienie dostępu do sieci komputerowej i jej usług. Przebieg ataku polega na generowaniu specjalnych pakietów SYN, których adres jest sfałszowany – jest nim adres ofiary. Duża liczba takich pakietów jest wysyłana do sieci. Komputery, do których one docierają, odpowiadają na adres pochodzący z fałszywego nagłówka. W ten sposób ofiara (zaatakowany komputer, system) otrzymuje wiele pakietów, w efekcie zostaje zablokowany i nie świadczy normalnych usług.

Fork-bomba – jest rodzajem ataku DoS na system komputerowy w celu jego zablokowania i uniemożliwienia świadczenia usług. Atak zakłada, że w środowisku rozproszonym – wieloprocesowym tylko część procesów może być uruchomiona równocześnie. Przebieg ataku to szybkie „rozmnożenie" kopii programu (aplikacji) w celu wypełnienia tablicy procesów systemu operacyjnego, tym samym jego zablokowanie – powstaje tzw. bomba. Wywołanie nowego procesu (np. w celu likwidacji procesu bomby) jest wstrzymane, ponieważ wymaga zwolnienia chociażby jednego z istniejących wpisów. Jest to mało prawdopodobne, ponieważ każdy proces bomby jest w tym momencie gotowy się rozmnożyć. Rezultat ataku to zablokowany system, znaczne straty i koszty.

Analiza sposobów i metod prowadzonych ataków w cyberprzestrzeni wskazuje na metodę i schemat ataku stosowany w cyberprzestrzeni, który najogólniej biorąc można sprowadzić do czterech faz – rekonesans obiektu ataku, jego skanowanie, uzyskanie dostępu oraz zacieranie śladów [2].

Rekonesans polega na rozpoznaniu i poszukiwaniu danych o obiekcie ataku, o zasobach teleinformatycznych umożliwiających przeprowadzenie ataku. Skanowanie to sprawdzanie stopnia wiarygodności pozyskanych w rekonesansie informacji, próbkowanie sieci, obserwacja obiektu ataku, tworzenie narzędzi do przeprowadzenia ataku. Uzyskanie dostępu polega na przejęcie kontroli nad obiektem ataku (systemem), np. poprzez nadanie sobie uprawnień administratora systemu. Z kolei zacieranie śladów to niszczenie wszelkich śladów w systemie, które rejestrowały nielegalne działania.

Ataki w cyberprzestrzeni mają charakter nagły, często niespodziewany i zaskakujący, utrudnione jest wskazanie źródła ataku, szczególnie takich, które mają charakter kryminalny, psychologiczny i terrorystyczny.

Obszary zainteresowania i ataku cyberterroryzmu

Obszarem zainteresowania cyberterroryzmu jest każdy obiekt funkcjonujący w cyberprzestrzeni, który umożliwi realizowanie celu cyberterrorystów. Najczęściej mogą to być ważne węzły informacyjne, teleinformatyczne oraz telekomunikacyjne, które mogą spowodować zakłócenia zasobów teleinformatycznych i telekomunikacyjnych, niepewność w społeczeństwie, strach, panikę i podobne następstwa.

Jest oczywistym, że zagrożeniem szczególnym w działalności ceberterrorystycznej jest infrastruktura krytyczna państw, wspólnot i różnego rodzaju organizacji [10], [11], [4], czyli systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [12].

Infrastruktura krytyczna obejmuje w szczególności systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, bankowe i finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające funkcjonowanie administracji publicznej, produkcji, stosowania, przechowywania i składowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Elementami, które w szczególności zostały zaklasyfikowane do krytycznej infrastruktury telekomunikacyjnej są systemy i sieci telekomunikacyjne, teleinformatyczne niezbędne do wykonywania statutowych zadań organów administracji rządowej oraz wymiany informacji w siłach zbrojnych i rejestry państwowe w warstwie aplikacyjnej, a także sieci telekomunikacyjne wykorzystywane przez administrację publiczną (rządową i samorządową) i siły zbrojne w warstwie medium transmisyjnego.

Przewidywane miejsca występowania zagrożeń bezpośrednich krytycznej infrastruktury teleinformatycznej to miejsca lokalizacji kluczowych elementów systemów teleinformatycznych, takich jak:

- centra zarządzania i utrzymania infrastruktury teleinformatycznej: własnych zasobów administracji, w szczególności urzędów, wydziałów i biur bezpieczeństwa i zarządzania kryzysowego oraz przedsiębiorców telekomunikacyjnych dostarczających usługi telekomunikacyjne,
- centrale telekomunikacyjne przedsiębiorców telekomunikacyjnych, obsługujące instytucje państwowe, urzędy oraz organizacje przewidywane do likwidacji zagrożeń,
- miejsca przebiegu telekomunikacyjnych linii międzycentralowych i podstawowych linii telekomunikacyjnych,
- stacje bazowe i satelitarne,
- inne ważne obiekty telekomunikacyjne (np. wyniesione koncentratory, stacje czołowe, węzły dostępowe itp.).

Przewidywane miejsca występowania zagrożeń bezpośrednich krytycznej infrastruktury teleinformatycznej to także miejsca posiadające serwery zarządzające systemami i bazami danych i kluczowe bazy danych (rejestry państwowe), wykorzystywane przez administrację publiczną (np. PESEL, Regon, CEPIK, Kataster, rejestry sądowe i inne systemy).

Ochrona cyberprzestrzeni

W okresie rozwoju cyberterroryzmu, ochrona cyberprzestrzeni to niezwykle ważne, ale zarazem trudne i złożone przedsięwzięcie. Wymaga ono zaangażowania znacznych potencjałów państw i organizacji w wymiarze międzynarodowym i krajowym oraz stosowania nowych rozwiązań technik i technologii skutecznie przeciwdziałających temu niezwykle szkodliwemu i niebezpiecznemu zagrożeniu.

Analiza literatury przedmiotu dotycząca zagrożeń i metod przeciwdziałania zagrożeniom oraz obserwacje działań państw i różnego rodzaju organizacji wskazuje, że proces ten, poza działaniami specjalistycznymi, powinien być wspierany metodami stosowanymi w obszarze bezpieczeństwa informacji i systemów teleinformatycznych oraz telekomunikacyjnych, zarówno publicznych, jak i tych mających zastosowania specjalne w obszarze bezpieczeństwa państwa i zarządzania kryzysowego. Do metod tych i sposobów zaliczamy metody administracyjno-organizacyjne, fizyczne, techniczne oraz specjal-

ne, które profesjonalnie wdrożone są skutecznym narzędziem zabezpieczenia informacji i systemów teleinformatycznych organizacji i ochrony cyberprzestrzeni i mogą zapewnić wysoki stopień ochrony informacji organizacji przed wszelkimi zagrożeniami w cyberprzestrzeni, jeśli zostaną zastosowane w sposób kompleksowy. Metody te są prezentowane w bogatej na ten temat literaturze przedmiotu stąd ich analizowanie i prezentacja w niniejszej publikacji została pominięta.

Ochrona cyberprzestrzeni jest jednym z podstawowych zadań administracji państwowej i podmiotów odpowiedzialnych za tego typu zadania. Ochrona ta jest zadaniem priorytetowym dla organizacji międzynarodowych i różnego rodzaju kooperacji w skali globalnej i regionalnej. Jako przykład, świadczą o tym działania administracji Unii Europejskiej, Paktu Północnoatlantyckiego NATO oraz państw stanowiących te organizacje. NATO przypisuje szczególne znaczenie zwalczaniu cyberterroryzmu i ochrony cyberprzestrzeni i jej funkcjonowania. Przykładem tego stanu rzeczy są:

- decyzja NATO podjęta w Pradze, w listopadzie 2002 r., o uruchomieniu Programu Obrony Cyberprzestrzeni (*The cyber defense program*) i zdolności reagowania na incydenty komputerowe (*The computer incident response capability*) – jako rezultat cyberataków na systemy NATO w Wojnie Bałkańskiej,
- decyzja NATO podjęta w Brukseli, w styczniu 2008 r., polegająca na przyjęciu Strategii Obrony Cyberprzestrzeni (*The policy on cyber defense*) oraz w maju 2008 r., przyjęcie Memorandum, o utworzeniu w Talinie Centrum Kompetencyjnego ds. Obrony Teleinformatycznej (*The concept for cooperative cyber defense of excellence*) – jako rezultat cyberataku na Estonię.

Obecnie w naszym kraju brak jest uregulowań prawnych w postaci np. ustawy, która normowałyby kompleksowo problem zwalczania cyberterroryzmu i ochrony cyberprzestrzeni. Nie oznacza to, że zagadnienia cyberterroryzmu są pomijane, są one wprowadzane do różnych dziedzinowych aktów prawnych oraz przepisów.

Ważnym jest to, że istnieją dwa istotne dokumenty – *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016 oraz Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* [13], [4], które stanowią podstawy realizacji procesu ochrony cyberprzestrzeni RP i wypracowania postanowień prawnych w tym zakresie.

Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016 to podstawowy dokument ujmujący w sposób zwarty problemy związane z ochroną cyberprzestrzeni RP. Program stanowi sobą propozycje działań prawno-organizacyjnych, technicznych i edukacyjnych, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Celem strategicznym programu jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa.

Podobny cel prezentuje dokument Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Jest to dokument, którego treści są zgodne z wskazanym programem rządowym oraz z obowiązującymi w Unii Europejskiej i naszym kraju różnego rodzaju strategiami związanymi z bezpieczeństwem narodowym.

W zakresie ochrony cyberprzestrzeni na uwagę zasługuje inicjatywa administracji USA, w ramach której opublikowano w 2009 r. tzw. Zgodne wytyczne do audytu (*Consensus Audit Guideline*) [14]. Wytyczne te przedstawiono w formie dwudziestu głównych przedsięwzięć do stosowania i audytu w zakresie bezpieczeństwa informacji oraz systemów teleinformatycznych, jako zabezpieczenie przed cyberatakami.

Podsumowanie

Cyberterroryzm to zagrożenie szczególne, współcześnie istniejące, rozwijające się, na które są narażone organizacje międzynarodowe, państwa i narody. Szczególnie niebezpiecznym jest cyberterroryzm o podłożu finansowym, fundamentalistycznym i ideologicznym.

W obliczu jego powszechnego istnienia często powstaje pytanie, czy dotyczy ono nas, naszego państwa. Odpowiedz może być tylko jedna – tak, dotyczy, a świadczą o tym zagrożenia i przestępstwa, jakich doznają obywatele korzystający z powszechnie dostępnych i publicznych zasobów teleinformatycznych. Uważa się, że z powodu uczestnictwa Polski w misjach i wojnach NATO oraz przyłączenia się do koalicji antyterrorystycznej zorganizowanej przez USA po ataku z 11 września 2011 r., Polska znajduje się w obszarze zainteresowania atakami terrorystycznymi ze strony sił fundamentalizmu islamskiego. Prawdziwym wydają się stwierdzenia, że dążą oni do ukarania Polski za współudział w ich zwalczaniu, stąd zagrożenie terrorystyczne zewnętrzne istnieje i może narastać [15]. Rzecz jednak w tym, by zagrożenia terrorystyczne i cyberterrorystyczne dostrzegać, liczyć się z nimi i zdecydowanie im przeciwdziałać.

Uogólniając prezentowane treści można sprecyzować następujące wnioski:

- cyberterroryzm to zagrożenie szczególne cywilizacji, społeczeństwa informacyjnego, bezpieczeństwa narodowego i obywateli i wymaga przeciwdziałania i zdecydowanego zwalczania,
- formy cyberterroryzmu, rodzaje ataków i metody ich prowadzenia są znane oraz powtarzające się. Przygotowanie na wymaganym poziomie zasobów osobowych i materialnych państwa i różnorodnych organizacji umożliwia skuteczną ochronę cyberprzestrzeni,
- metody i sposoby zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji powinny być stosowane w sposób kompleksowy. Taka praktyka działania wychodzi naprzeciw potrzebom ochrony cyberprzestrzeni,
- w naszym kraju istnieje pilna potrzeba ustanowienia aktu prawnego stwarzającego kompleksowe prawne podstawy osiągnięcia akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni.

Współcześnie szereg organizacji i instytucji o charakterze międzynarodowym i narodowym prowadzi prace badawcze w zakresie zagrożeń i ochrony cyberprzestrzeni oraz cyberteroryzmu, np. NATO, Unia Europejska, Interpol, Agencja Bezpieczeństwa Wewnętrznego RP, uczelnie techniczne i instytuty naukowo-badawcze w kraju. Prace tego typu realizowane są przez wyspecjalizowane zespoły badawcze w kraju, miedzy innymi w Instytucie Łączności – Państwowym Instytucie Badawczym. Zagrożenia informacji i systemów teleinformatycznych w cyberprzestrzeni oraz metody im przeciwdziałania są obiektami zainteresowania i badania autorów publikacji.

Bibliografia

[1] Denning D. E.: *Wojna informacyjna i bezpieczeństwo informacji*, PWN, Warszawa, 2002

[2] Denning D. E.: *Cyberterrorism,* www.cs.georgetown.edu, 2004

[3] Garison L., Grand M.: *Cyberterrorism, an evolving concept*, NIPC highlights, 2004

[4] Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, RCB, Warszawa, czerwiec 2010

[5] Sienkiewicz P.: *Terroryzm w cybernetycznej przestrzeni*, w: *Cyberterroryzm nowe wyzwanie XXI wieku*, red. Jemioła T., Kisielnicki J., Rajchel K., WSIZiA, Warszawa, 2009

[6] Strużak R.: *Problemy ochrony sieci teleinformatycznych przed narażeniami i terroryzmem elektromagnetycznym*, TiTI 3-4/2010, Warszawa, 2010

[7] Convention on Cybercrime, Budapest, 23.09.2001

[8] Czepielewski M.: *Cyberterroryzm jako element społeczeństwa informacyjnego, na przykładzie Estonii*, w: *Cyberterroryzm nowe wyzwanie XXI wieku*, red. Jemioła T., Kisielnicki J., Rajchel K., WSIZiA, Warszawa, 2009

[9] ABW, www.cert.gov.pl

[10] Dela P.: *Cyberterroryzm jako zagrożenie dla infrastruktury krytycznej państwa*, Wykład habilitacyjny, AON, Warszawa, 2012

[11] Europejski Program Ochrony Infrastruktury krytycznej (EPOIK) – KOM(2006) 786 wersja ostateczna – komunikat Komisji Wspólnot Europejskich z dnia 12.12.2006 r.

[12] Szubrycht T.: *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, ZN AMW, rok XLVI nr 1 (160), 2005

[13] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, MAiC, ABW, Warszawa, 25 czerwca 2013

[14] Consensus Audit Guideline, www.sans.org/cag

[15] Biała Księga Bezpieczeństwa Narodowego RP, BBN, Warszawa, 2013

[16] Bógdał-Brzezińska A., Gawrycki M.: *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa, 2003

[17] Czyżak M.: *Wybrane aspekty zjawiska cyberterroryzmu*, TiTI, 1-2/2010, Warszawa, 2010

[18] Duda D.: *Terroryzm islamski*, UJ, Kraków, 2002

[19] Hołys B.: *Cyberterroryzm jako zagrożenie XXI wieku*, WSM, Warszawa, 2010

[20] Kisielnicki J.: *Cyberterrpryzm jako element zagrożenia współczesnej cywilizacji*, UW, Warszawa, 2009

[21] Lewis J. A.: *Assessing the risk of cyber terrorism, cyber war and other cyber threats,* Center for Strategic and International Studies, 2004

[22] Liderman K.: *Normy i standardy w zakresie bezpieczeństwa informacyjnego i teleinformacyjnego*, BIAiR, nr 26/2006, Warszawa, 2006

[23] Sienkiewicz P.: *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, Automatyka, tom 13, zeszyt 2, 2009

[24] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r., nr 89 poz. 590 z późniejszymi zmianami

Jakub Kowalewski

Mgr inż. Jakub Kowalewski – absolwent Wyższej Szkoły Informatyki Stosowanej i Zarządzania, specjalista konstruktor elektronik w zespole łączności satelitarnej WZŁ Nr 1 S.A., a także uczestnik nadzoru i monitorowania systemów łączności satelitarnej dla WP i organizacji komercyjnych. Jego zainteresowania naukowe to: projektowanie i eksploatacja systemów satelitarnych, bezpieczeństwo informacji i systemów teleinformatycznych.

e-mail: J.Kowalewski@wz1.com.pl

Marian Kowalewski

Prof. nzw. dr hab. inż. Marian Kowalewski – absolwent Wyższej Szkoły Oficerskiej Wojsk Łączności, nauczyciel akademicki i pracownik naukowy Instytutu Łączności – Państwowego Instytutu Badawczego (od 1997) i Politechniki Warszawskiej (od 2011). Prof. Kowalewski jest autorem wielu podręczników, skryptów akademickich i artykułów. Jego zainteresowania naukowe: planowanie, projektowanie, efektywność oraz bezpieczeństwo systemów telekomunikacyjnych.

e-mail: M.Kowalewski@itl.waw.pl