PRZEGLĄD ZACHODNI
2012, nr 4

MIRON LAKOMY
Katowice

CYBERZAGROŻENIA NA POCZĄTKU XXI WIEKU

Pojęcie cyberprzestrzeni pojawiło się po raz pierwszy w powieści *science fiction* Williama Gibsona – *Neuromancer*. Oznaczało ono świat cyfrowych sieci, w którym ścierały się interesy wielkich koncernów. Wraz z rozwojem i upowszechnianiem technologii informatycznych, termin ten został podchwycony i wykorzystany przez naukowców. Pierre Delvy uznał ten nowy wymiar ludzkiej aktywności za przestrzeń otwartego komunikowania za pośrednictwem połączonych komputerów i pamięci informatycznych, pracujących na całym świecie. Inną definicję podała Marie Laure Ryan, według której cyberprzestrzeń to wygenerowana przez komputery wirtualna rzeczywistość[1]. Początkowo sieci teleinformatyczne były wykorzystywane głównie przez instytucje badawcze i wojskowe. Wraz z upowszechnianiem się komputerów osobistych oraz powstaniem Internetu, znaczenie cyberprzestrzeni zaczęło dynamicznie rosnąć. Proces komputeryzacji i informatyzacji zaczął obejmować kolejne dziedziny funkcjonowania państw i społeczeństw. Bez względu na ogromne korzyści, które się z tym wiązały, procesy te niosły ze sobą również coraz poważniejsze zagrożenia. Początkowo przybierały one formę pojedynczych ataków komputerowych, za którymi stali domorośli programiści, traktujący to zajęcie bardziej jako hobby. Z biegiem czasu jednak działalność ta zmieniła charakter. Na przełomie XX i XXI w. hakerzy zaczęli się organizować w niezależne grupy, za których działalnością coraz częściej stały rządy państw. Początkowo mało groźne włamania do systemów komputerowych zaczęły przekształcać się w zorganizowane akcje powiązanych ze służbami specjalnymi grup programistów, których celem było uzyskanie określonych korzyści politycznych, gospodarczych bądź militarnych. Co więcej ataki za pomocą sieci nie dotyczyły już tylko witryn internetowych, ale coraz częściej ich łupem padały serwery i sieci o fundamentalnym znaczeniu dla funkcjonowania struktur państwowych. Na początku XXI w. cyberprzestrzeń stała się więc płaszczyzną działań, które nie

[1] M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations", nr 3-4/2010, s. 56.

zagrażają tylko bezpieczeństwu informacji niejawnych, ale także funkcjonowaniu infrastruktury krytycznej[2]. Warto więc zadać pytanie, jakie środki podejmują państwa oraz organizacje międzynarodowe, aby dostosować się do nowej sytuacji bezpieczeństwa przełomu pierwszej i drugiej dekady XXI w.

NOWE WYZWANIA DLA CYBERBEZPIECZEŃSTWA PAŃSTW NA PRZEŁOMIE XX I XXI WIEKU

Aktywność państw i grup niepaństwowych w cyberprzestrzeni można generalnie podzielić na trzy grupy: cyberterroryzm, cyberszpiegostwo oraz wykorzystanie cyberprzestrzeni do działań militarnych.

Cyberterroryzm najczęściej określa się jako atak na komputery, sieci lub systemy informacyjne, mający na celu osiągnięcie określonych korzyści politycznych. Już w latach 80. XX w. tak Stany Zjednoczone, jak i Związek Radziecki dokonały pierwszych prób wykorzystania cyberprzestrzeni w ten sposób. Były to jednak bardzo sporadyczne przypadki o stosunkowo niewielkim znaczeniu. W latach 90. sytuacja nieco zmieniła się, na co wpływ przede wszystkim miało upowszechnienie Internetu oraz proces komputeryzacji, obejmujący kolejne dziedziny życia. Pierwsze zagrożenia powodowali z reguły tworzący wirusy komputerowe domorośli programiści. W drugiej połowie lat 90. coraz częściej zaczęło jednak dochodzić do przypadków włamań do sieci i komputerów instytucji rządowych, za czym stali już nie tylko pojedynczy hakerzy, ale zorganizowane grupy przestępcze. W pierwszej dekadzie XXI w. cyberprzestrzeń zaczęła być wykorzystywana przez państwa. Szczególną rolę zaczęły tu odgrywać grupy hakerów wynajmowanych przez rządy państw w celu realizacji określonych zadań w Internecie.

Przełomem w dyskusji na temat cyberzagrożeń stały się z pewnością wydarzenia w Estonii z kwietnia 2007 r. Wówczas ostry spór polityczny na linii Tallin-Moskwa, dotyczący usunięcia pomnika żołnierzy radzieckich, doprowadził do masowego ataku na estoński Internet. Grupy rosyjskich hakerów, wykorzystując na wcześniej niespotykaną skalę tzw. sieć botnet[3], były w stanie sparaliżować nie tylko strony najważniejszych instytucji państwowych i prywatnych, ale także np. system bankowy. Mimo iż według ekspertów atak na Estonię bardziej przypominał „cyberzamieszki" niż „cyberwojnę", to udowodnił rosnące znaczenie sieci teleinformatycznych dla bezpieczeństwa państw[4].

---

[2] *Ibidem*, s. 56.

[3] Botnet to grupa komputerów zainfekowanych złośliwym oprogramowaniem i kontrolowanych z ukrycia przez zarządzających daną siecią hakerów. B. Łącki, *Botnet od podszewki*, Heise Security, 13.06.2007. Adres URL: http://www.heise-online.pl/security. Dostęp: 25.01.2011.

[4] S. Waterman, *Who Cyber Smacked Estonia*, 11.06.2007. Adres URL: http://www.spacewar.com. Dostęp: 25.01.2011.

Rosnące znaczenie działalności cyberterrorystycznej w polityce państw potwierdził także konflikt gruziński. Podczas tego konfliktu zbrojnego, po raz pierwszy na dużą skalę, obok tradycyjnych instrumentów walki zbrojnej, wykorzystano również cyberprzestrzeń. Rosyjscy hakerzy z grupy *Russian Business Network*, podobnie jak w przypadku Estonii, byli w stanie na niemal cały okres konfliktu zablokować funkcjonowanie nie tylko witryn internetowych rządu gruzińskiego, instytucji naukowych czy najważniejszych mediów, ale także infrastrukturę komunikacyjną, np. sieć komórkową *VoIP*. Przykładowo na stronie prezydenta Gruzji Michaiła Saakaszwilego zamieścili materiały, które oskarżały o wybuch wojny Tbilisi. Zdjęcie prezydenta zastąpiono także fotografią Adolfa Hitlera, co miało silny efekt propagandowy. Podczas wojny Rosjanie udowodnili, iż dysponują bardzo dużym potencjałem w cyberprzestrzeni, który pozwolił w dużej mierze zablokować rządowi Gruzji zdolność informowania świata o wydarzeniach w Osetii. Minister spraw zagranicznych tego kraju zmuszony był korzystać z bloga Google. Podobne problemy miał również prezydent Saakaszwili, który nie mógł nawiązać kontaktu telefonicznego z dziennikarzami, chcącymi przeprowadzić z nim wywiad. Wydarzenia z Kaukazu z sierpnia 2008 r. zostały ochrzczone mianem „drugiej cyberwojny", podczas której na masową skalę wykorzystano przestrzeń teleinformatyczną przeciwko innemu państwu. Jak zauważył Kevin Coleman, ekspert ds. cyberbezpieczeństwa, udowodniło to, iż ten nowy aspekt bezpieczeństwa państw nie może być już dłużej ignorowany. Cyberprzestrzeń stała się bowiem integralną częścią nowoczesnych konfliktów zbrojnych. Podobnie wypowiedział się Bill Woodcock, zdaniem którego ataki w cyberprzestrzeni są niezwykle groźne, tanie i łatwe do przygotowania, przez co z pewnością staną się w przyszłości ważnym instrumentem prowadzenia wojny[5]. Co ciekawe trzecia „cyberwojna" rozpoczęła się już w kilka miesięcy później. Na początku 2009 r. doszło do masowych aktów cyberterroryzmu – tym razem w Kirgistanie. Powodem zablokowania niemal całego kirgiskiego Internetu – ponownie przez rosyjskich hakerów – była dyskusja w tym kraju nad dalszą przyszłością amerykańskiej bazy wojskowej[6].

Potwierdzeniem trendu pojawiania się nowych cyberterrorystycznych zagrożeń stały się również wydarzenia w Iranie. Jak wskazują eksperci, Izrael opracował bowiem najbardziej zaawansowany wirus w historii, przeznaczony specjalnie do sparaliżowania prac elektrowni atomowych Iranu. Program ten, nazwany *Stuxnet*, został wprowadzony do systemów komputerowych elektrowni w Natanz i Bushehr dzięki rosyjskim firmom podwykonawczym. Wysoki stopień skomplikowania programu pozwolił na zakłócenie działalności wirówek wzbogacania uranu, dzięki czemu – według niektórych informacji – irański program atomowy został znacząco

[5] J. Markoff, *Before the Gunfire, Cyberattacks*, „The New York Times", 12.08.2008; K. Coleman, *Cyber War 2.0 – Russia v. Georgia*, DefenseTech, 13.08.2008. Adres URL: http://defensetech.org. Dostęp: 12.03.2011; M. Lakomy, *Znaczenie cyberprzestrzeni...*, s. 61.

[6] K. Coleman, *Russia Now 3 and 0 in Cyber Warfare*, DefenseTech, 30.01.2009. Adres URL: http://defensetech.org. Dostęp: 12.03.2011.

spowolniony. Wyjątkowość wirusa *Stuxnet* polegała na jego wyspecjalizowanym charakterze. Został on zaprojektowany wyłącznie do ataków na systemy komputerowe kontrolujące procesy przemysłowe w elektrowniach atomowych, jednocześnie ukrywając swoje istnienie[7]. Warto także dodać, iż coraz częściej dochodzi do wykorzystywania cyberprzestrzeni przez organizacje terrorystyczne. Przykładowo możliwościami ataków komputerowych dla działalności propagandowej, szkoleniowej i rekrutacyjnej na początku XXI w. zainteresowały się *Al-Kaida* oraz *Hezbollah*[8].

Działalność cyberszpiegowską z kolei tłumaczy się jako próby wyprowadzania informacji niejawnych z serwerów bądź sieci sektora państwowego i prywatnego. Szczególną rolę odgrywa tu z pewnością Chińska Republika Ludowa, która jako pierwsza na masową skalę zaczęła wykorzystywać włamania komputerowe dla uzyskania nowych technologii bądź tajnych informacji. Już w latach 2003-2005 chińscy hakerzy przeprowadzili operację *Titan Rain*, w ramach której dokonano serii ataków na serwery instytucji badawczych i wojskowych w Stanach Zjednoczonych, dzięki czemu wyprowadzono dane dotyczące projektu myśliwca nowej generacji – F-35 *Joint Strike Fighter*. W innej z serii cyberataków z końca lat 90., określonej mianem *Moonlight Blaze*, rosyjscy hakerzy dokonali włamań do wielu serwerów amerykańskich instytucji badawczych i wojskowych, wyprowadzając m.in. informacje dotyczące amerykańskiego systemu kierowania rakietami[9].

W 2008 r. doszło do najpoważniejszego w historii włamania do amerykańskich sieci wojskowych, za czym stała prawdopodobnie Rosja. Nie podano ile tajnych danych utracono, jednak o znaczeniu tego incydentu świadczy fakt, iż usunięcie złośliwego oprogramowania zajęło amerykańskim informatykom aż 14 miesięcy[10]. W tym samym okresie miał miejsce również inny poważny atak, tym razem chińskich hakerów z grupy *Ghostnet*. Włamali się oni do niemal 1300 komputerów należących do instytucji państwowych, korporacji i instytucji badawczych ze 103 krajów. Był to, biorąc pod uwagę zasięg geograficzny, największy atak szpiegowski przeprowadzony za pomocą Internetu[11]. O wzroście aktywności ChRL świadczyła

---

[7] A. Aneja, *Under cyber-attack, Iran says*, „The Hindu", 26.09.2010; *Stuxnet heralds age of cyber weapons, virtual arms race*, „Homeland Security Newswire", 27.01.2011. Adres URL: http://homelandsecuritynewswire.com. Dostęp: 01.03.2011; *To był izraelski cyber-atak na Iran*, Dziennik.pl, 01.10.2010. Adres URL: http://wiadomosci.dziennik.pl. Dostęp: 01.03.2011.

[8] S. Moćkun, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, „Raport Biura Bezpieczeństwa Narodowego", Warszawa, lipiec 2009 r., s. 2; M. Łapczyński, *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pulaski Policy Papers", nr 7/2009, s. 1; P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, w: L.H. Haber (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Kraków 2003, s. 376-377.

[9] M. Łapczyński, *Zagrożenie cyberterroryzmem...*, s. 1; P. Sienkiewicz, *Wizje i modele...*, s. 376-377.

[10] W.J. Lynn III, *Defending a New Domain*, „Foreign Affairs", September/October 2010.

[11] S. Adair, R. Deibert, G. Walton, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Information Warfare Monitor, Shadowserver Foundation, 06.04.2010.

także operacja *Aurora* przeprowadzona w drugiej połowie 2009 r. Wówczas chińscy programiści dokonali cyberataków na serwery ok. 20 amerykańskich korporacji, m.in. Google, Yahoo i Symantec, których celem było wyprowadzenie nowych technologii[12].

Wreszcie warto wspomnieć o możliwości wykorzystania cyberprzestrzeni w warunkach konfliktu zbrojnego. W połowie lat 90. J. A. Warden uznał sieci teleinformatyczne za piąty wymiar walki zbrojnej[13]. Już podczas wojny w Kosowie doszło do pierwszych incydentów w cyberprzestrzeni, jednak nie miały one w zasadzie żadnego znaczenia. Po raz pierwszy cyberataki na masową skalę w warunkach konfliktu zbrojnego zastosowano w 2008 r. w Gruzji. Przeprowadzone przez rosyjskich hakerów działania nakierowane były jednak głównie na osiągnięcie korzyści o charakterze politycznym i propagandowym, przez co klasyfikuje się je z reguły jako działalność cyberterrorystyczną.

Ogromny potencjał wykorzystania cyberprzestrzeni przy prowadzeniu operacji militarnych potwierdził Izrael we wrześniu 2007 r. Lotnictwo *IDF* przeprowadziło wówczas operację *Orchard*, której celem było zniszczenie syryjskiego ośrodka, w którym prowadzono prace nad bronią atomową. Misja ta zakończyła się pełnym sukcesem, bowiem samoloty *IDF* nie zostały w trakcie przelotu nad syryjskim terytorium wykryte przez system obrony przeciwlotniczej. Wynikało to z zastosowania przez Izrael wirusa komputerowego, który został wprowadzony do syryjskich systemów wojskowych. Pozwolił on w odpowiednim momencie na przejęcie kontroli nad radarami, dzięki czemu samoloty *IDF* pozostały niewykryte. Wydarzenie to udowodniło, iż cyberprzestrzeń może być z powodzeniem wykorzystana w warunkach konfliktu zbrojnego. Zastosowanie przestrzeni teleinformatycznej pozwoliło bowiem na osiągnięcie rezultatu, który tradycyjnymi metodami byłby niemal niemożliwy do osiągnięcia[14].

Reasumując ten wątek, należy stwierdzić, iż w pierwszej dekadzie XXI w. można zauważyć tendencję lawinowego wzrostu zagrożeń dla bezpieczeństwa państw pojawiających się w cyberprzestrzeni. Mają one charakter nie tylko incydentów, za którymi stoją pojedyncze osoby bądź małe grupki programistów, lecz coraz częściej masowych, zorganizowanych ataków motywowanych bądź przeprowadzanych przez rządy poszczególnych państw, których celem jest osiągnięcie określonych korzyści politycznych, militarnych bądź ekonomicznych.

---

[12] K. Jackson Higgins, *'Aurora' Attacks Still Under Way, Investigators Closing in on Malware Creators*, Darkreading, 10.02.2010. Adres URL: http://www.darkreading.com. Dostęp: 10.03.2011.

[13] J.A. Warden, *Enemy as a System*, „Airpower Journal", nr 9/1995, s. 40-55.

[14] D.A. Fulgham, *Why Syria's Air Defense Failed to Detect Israelis*, „Aviation Week and Space Technology", 03.10.2007.

PERCEPCJA CYBERZAGROŻEŃ W POLITYKACH BEZPIECZEŃSTWA WYBRANYCH PODMIOTÓW MIĘDZYNARODOWYCH

Mając na uwadze omówione powyżej zagrożenia, warto zastanowić się, jak na początku XXI w. reagują na nie najpoważniejsi aktorzy na arenie międzynarodowej. Z pewnością liderem walki z cyberzagrożeniami są Stany Zjednoczone, państwo które obecnie doświadcza największej liczby ataków hakerskich na świecie. W 2008 r. tylko na serwery Departamentu Stanu dokonywano niemal 6 milionów ataków dziennie, co dobitnie obrazuje skalę problemu[15]. Jak wspomniano wcześniej, pierwsze kroki w cyberprzestrzeni amerykańskie służby postawiły jeszcze w latach 80., jednak miało to raczej symboliczne znaczenie i nie spotkało się z większym zainteresowaniem decydentów. Skalę cyberzagrożeń zauważono w USA jednak dość wcześnie, gdyż już w styczniu 1995 r. Departament Obrony USA powołał wówczas *Information Warfare Executive Board*, odpowiedzialny za obronę amerykańskich interesów w środowisku informacyjnym. To także w USA po raz pierwszy podjęto prace badawcze nad skutkami wykorzystania cyberprzestrzeni w tradycyjnym konflikcie zbrojnym. Przełomem dla amerykańskiej polityki cyberbezpieczeństwa z pewnością okazała się jednak prezydentura George'a W. Busha, którego administracja w lutym 2003 r. wydała *The National Strategy to Secure Cyberspace*. W dokumencie tym uznano, iż zabezpieczenie cyberprzestrzeni jest jednym ze strategicznych wyzwań Stanów Zjednoczonych. Stwierdzono także: „Naszą główną troską jest zagrożenie zorganizowanymi cyberatakami, zdolnymi zakłócić krytyczną dla naszego narodu infrastrukturę, gospodarkę czy bezpieczeństwo narodowe". Amerykańską strategię oparto na 5 filarach:

– stworzeniu narodowego systemu reagowania na zagrożenia pochodzące z cyberprzestrzeni, obejmującego tak instytucje państwowe, jak i prywatne;

– wprowadzeniu programu zmniejszającego zagrożenia z cyberprzestrzeni opartego na współpracy poszczególnych agencji rządowych oraz na systemie obserwacji prawidłowości ataków w sieciach teleinformatycznych;

– wprowadzeniu narodowego programu edukacyjnego, którego celem byłoby uświadomienie Amerykanom zagrożeń płynących z Internetu;

– wprowadzeniu nowych rozwiązań technologicznych przy zabezpieczaniu rządowych sieci teleinformatycznych;

– rozwijaniu współpracy w dziedzinie cyberbezpieczeństwa nie tylko pomiędzy poszczególnymi agencjami rządowymi, ale także z innymi państwami w ramach tzw. *Safe Cyber Zone*[16].

Do przełomu w amerykańskiej polityce cyberbezpieczeństwa doszło jednak – podobnie jak w innych krajach – dopiero po „pierwszej cyberwojnie" w Estonii.

---

[15] M. Łapczyński, *Zagrożenie cyberterroryzmem...*, s. 1; P. Brągoszewski, *Świat żywych trupów*, „PC World", maj 2007.

[16] M. Lakomy, *Znaczenie cyberprzestrzeni...*, s. 61-64.

W styczniu 2008 r. rozpoczęto prace nad projektem *Comprehensive National Cybersecurity Initiative*, która miała stanowić spójną odpowiedź amerykańskiego rządu na zagrożenia płynące z sieci. *CNCI* składało się z 12 osobnych projektów, dotyczących m.in. utworzenia systemów ostrzegania o intruzach w sieciach rządowych, rozwoju badań nad cyberbezpieczeństwem czy koordyncji poszczególnych agencji zajmujących się tą dziedziną. Warto także wspomnieć o szerokim raporcie *Center for Strategic and International Studies* (*CSIS*) przygotowanym w grudniu 2008 r. dla Baracka Obamy, gdzie stwierdzono, iż cyberprzestrzenne zagrożenia są w XXI w. jednym z najpoważniejszych wyzwań dla bezpieczeństwa państw. Autorzy postulowali sformułowanie nowej strategii, obejmującej już nie tylko tradycyjne elementy polityczne, ekonomiczne czy militarne, ale także cyberprzestrzenne. Ich zdaniem walka z cyberzagrożeniami powinna być oparta na działaniach wielokierunkowych. Po pierwsze, ze względu na charakter zagrożeń, instytucje rządowe powinny zawiązać współpracę z sektorem prywatnym. Po drugie, rząd powinien wprowadzić minimalne standardy bezpieczeństwa w sieciach teleinformatycznych, w celu zapewnienia, iż podstawowe usługi w cyberprzestrzeni będą nadal świadczone. Po trzecie, USA powinny pracować nad technologiami, które zapewnią lepszą identyfikację użytkowników w sieci. Po czwarte, zaktualizowane powinno zostać również amerykańskie ustawodawstwo, które w dużej mierze nie przewidywało przypadków przestępczości w sieci. Po piąte, administracja amerykańska powinna dokonać zakupu niezbędnych technologii teleinformatycznych. Po szóste wreszcie, USA powinny także prowadzić pogramy badawcze i edukacyjne, wzmacniające amerykańskie przywództwo w cyberprzestrzeni [17].

Prezydent Barack Obama w znacznej mierze zastosował się do wymienionych wyżej wskazówek. Cyberbezpieczeństwo stało się bowiem jednym z priorytetów nowej administracji. Jedną z pierwszych decyzji podjętych przez Obamę było powołanie urzędu doradcy ds. cyberprzestrzeni. Efektem prac nowego organu był raport *Cyberspace Policy Review*, w którym określono najważniejsze cele polityki cyberbezpieczeństwa Stanów Zjednoczonych. Wymieniono m.in. utworzenie struktur do zwalczania cyberprzestępczości, powołanie przedstawiciela zajmującego się przestrzeganiem wolności obywatelskich w sieci, prowadzenie akcji uświadamiających na temat zagrożeń w sieci oraz przygotowanie planów reagowania kryzysowego na ataki w amerykańskiej cyberprzestrzeni [18].

Bezpośrednim rezultatem podjętych od 2008 r. prac koncepcyjnych było utworzenie jednostek i struktur stojących na straży amerykańskiej cyberprzestrzeni. Departament Bezpieczeństwa Narodowego oraz Narodowa Agencja Bezpieczeństwa stworzyły jednostkę składającą się z ok. 2000 informatyków, mających realizować w cyberprzestrzeni zadania tak defensywne, jak i ofensywne. Powołano

[17] *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies, grudzień 2008.

[18] M. Lakomy, *Znaczenie cyberprzestrzeni...*, s. 64-65.

także *National Cyber Security Division*, który działając w ramach Departamentu Bezpieczeństwa Narodowego, ma monitorować, analizować i ochraniać amerykański Internet. Najistotniejszą jednak decyzją było stworzenie w czerwcu 2009 r. *United States Cyber Command*, do którego zadań należy m.in.: koordynacja sieci obronnej USA w cyberprzestrzeni oraz przeprowadzanie ataków. W skład dowództwa weszła m.in. 10. Flota oraz *Marine Corps Forces Cyberspace Command*[19]. Ciekawym efektem prac koncepcyjnych nad cyberbezpieczeństwem stał się także zapis, według którego w razie ataku na istotne z punktu widzenia interesu państwa serwery część sieci teleinformatycznych może zostać odcięta od reszty Internetu przez amerykańską administrację[20]. Mimo opisanych powyżej wysiłków, według byłego szefa amerykańskiego wywiadu Mike'a McDonnella, USA nadal nie mają wystarczającego potencjału, aby obronić się przed najpoważniejszymi atakami np. na elementy infrastruktury krytycznej[21].

Zagrożenia płynące z cyberprzestrzeni w ostatnich latach zostały dostrzeżone również przez polskich decydentów. Podobnie jak w innych przypadkach, momentem zwrotnym były tu wydarzenia z Estonii i Gruzji, które udowodniły, iż ryzyko wybuchu konfliktu w cyberprzestrzeni jest znaczne. Pierwsze wzmianki na temat cyberbezpieczeństwa znalazły się już w Strategii Bezpieczeństwa Narodowego RP z 2007 r., jednak kwestie te potraktowano dość ogólnikowo. Mając na uwadze doświadczenia Estonii i Gruzji, oraz systematycznie rosnącą liczbę ataków w polskim Internecie, w 2008 r. Agencja Bezpieczeństwa Wewnętrznego podjęła działania zmierzające do sprawdzenia stanu zabezpieczeń serwerów i witryn internetowych należących do instytucji rządowych. Kolejnym krokiem było rozpoczęcie prac nad Rządowym programem ochrony cyberprzestrzeni RP na lata 2009-2011, który został zatwierdzony przez premiera 9 marca 2009 r. We wprowadzeniu stwierdzono, iż cyberterroryzm stał się obecnie „kluczową i stale rosnącą postacią ataków terrorystycznych". Za główny cel programu przyjęto podniesienie poziomu bezpieczeństwa cyberprzestrzeni państwa. Do celów szczegółowych zaliczono natomiast: zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa, stworzenie i realizację spójnej dla wszystkich organów państwowych polityki bezpieczeństwa w cyberprzestrzeni, zmniejszenie skuteczności cyberataków, stworzenie stałego systemu koordynacji między sektorem prywatnym a organami rządowymi, zwiększenie kompetencji w dziedzinie cyberbezpieczeństwa podmiotów zaangażowanych w ochronę infrastruktury teleinformatycznej państwa oraz zwiększenie świadomości użytkowników sieci teleinformatycznych w tym zakresie[22]. Dokument ten stał się w zasadzie

[19] *Memorandum for Secretaries of the Military Departments*, The Secretary of Defense, Washington D.C., 23.05.2009.

[20] T. Romm, *NCTA praises Rockefeller-Snowe cybersecurity bill*, „The Hill", 18.03.2010.

[21] M. Bosacki, *Cyberwojna: Chiny vs USA*, „Gazeta Wyborcza", 02.02.2010.

[22] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011*, CERT, Warszawa, marzec 2009. Adres URL: www.cert.gov.pl. Dostęp: 02.02.2011.

pierwszą państwową strategią, która podjęła całościowo problem cyberbezpieczeństwa.

W czerwcu 2010 r. zakończyły się prace ekspertów MON, ABW, Straży Granicznej i NASK nad kolejnym dokumentem, obejmującym plany rządu na kolejne 6 lat. Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016 został zdecydowanie wzbogacony w stosunku do poprzedniej wersji. We wstępie stwierdzono, iż „W obliczu globalizacji, ochrona cyberprzestrzeni państwa stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa". Według autorów w XXI w. granica między pokojem a wojną staje się coraz bardziej umowna, wskutek czego istnieje rosnąca potrzeba współpracy między sektorem publicznym (wojskowym) a prywatnym (cywilnym). Założenia nowego programu objęły więc nie tylko systemy i sieci teleinformatyczne należące do instytucji państwowych, ale także do przedsiębiorstw o strategicznym znaczeniu dla funkcjonowania państwa oraz indywidualnych użytkowników cyberprzestrzeni. Co ciekawe dokument ten pominął sieci i systemy informatyczne o charakterze niejawnym, których ochrona regulowana jest odrębnymi przepisami. W odróżnieniu od wcześniejszej wersji, dokonano definicji najważniejszych terminów:

– cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez sieci i systemy informatyczne;

– cyberterroryzm – cyberprzestępstwo o charakterze terrorystycznym;

– cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni;

– incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji;

– krytyczna infrastruktura teleinformatyczna – infrastruktura krytyczna wyodrębniona w systemie łączności i sieciach teleinformatycznych.

Za cel strategiczny dokumentu uznano zapewnienie ciągłego bezpieczeństwa cyberprzestrzeni państwa. Do celów szczegółowych natomiast zaliczono:

– zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa;

– zniwelowanie skutków naruszeń bezpieczeństwa cyberprzestrzeni;

– zdefiniowanie podmiotów odpowiedzialnych za ochronę cyberprzestrzeni państwa;

– stworzenie spójnego systemu zarządzania bezpieczeństwem cyberprzestrzeni RP;

– stworzenie systemu koordynacji między poszczególnymi podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz dostawcami usług internetowych;

– zwiększenie świadomości użytkowników w zakresie bezpieczeństwa teleinformatycznego.

Za głównych realizatorów programu uznano Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej, Agencję Bezpieczeństwa

Wewnętrznego oraz Służbę Kontrwywiadu Wojskowego. Do najważniejszych założeń dokumentu należy zaliczyć m.in.:

– wprowadzenie obowiązku przedstawiania przez odpowiednie organy państwowe sprawozdań MSWiA dotyczących zagrożeń i problemów w cyberprzestrzeni,

– podjęcie działań legislacyjnych w celu dostosowania ustawodawstwa do zadań określonych w Programie,

– reorganizację mającą na celu optymalizację wykorzystania istniejącej infrastruktury cyberprzestrzennej państwa,

– działalność edukacyjną wobec obecnych i przyszłych użytkowników sieci,

– działania o charakterze technicznym mające na celu ograniczenie ryzyka wystąpienia cyberzagrożeń,

– ustalenie organów odpowiedzialnych za ochronę cyberprzestrzeni RP,

– umocowanie prawne Rządowego Zespołu Reagowania na Incydenty Komputerowe,

– powołanie Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP,

– powołanie w jednostkach organizacyjnych pełnomocników ds. ochrony cyberprzestrzeni,

– racjonalizację programów kształcenia na wyższych uczelniach w zakresie ochrony cyberprzestrzeni w celu uzyskania wysoko wykwalifikowanych kadr,

– kształcenie kadry urzędniczej,

– przeprowadzenie kampanii społecznej dla uświadomienia zagrożeń pojawiających się w cyberprzestrzeni,

– podjęcie krajowych programów badawczych w zakresie cyberbezpieczeństwa,

– rozbudowę zespołów reagowania na incydenty w cyberprzestrzeni, systemów wczesnego ostrzegania o zagrożeniach oraz stałe testowanie poziomu zabezpieczeń,

– rozwój Rządowych Zespołów Reagowania na Incydenty Komputerowe,

– oraz opracowanie Planów Ciągłości Działania[23].

Do dokumentu dodano aż 26 załączników omawiających m.in. rozwój zespołów *CERT* czy współpracę Agencji Bezpieczeństwa Wewnętrznego z *NATO*. Program ten został więc znacząco wzbogacony w stosunku do wersji z lat 2009-2011. Wydaje się, iż stanowi on prawidłową odpowiedź na najpoważniejsze wyzwania dla bezpieczeństwa teleinformatycznego RP.

Najistotniejszym efektem zainteresowania rządu sprawami cyberbezpieczeństwa była decyzja o powołaniu 1 lutego 2008 r. Rządowego Zespołu Reagowania na Incydenty Komputerowe (*CERT*), utworzonego na mocy porozumienia między Ministerstwem Spraw Wewnętrznych i Administracji oraz Agencją Bezpieczeństwa

[23] Zob. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji RP, Wersja 1.1., Warszawa, czerwiec 2010.

Wewnętrznego. Do zadań *CERT* zaliczono: koordynację reagowania na incydenty kryzysowe w sieciach teleinformatycznych, publikację ostrzeżeń i alarmów o zagrożeniach, obsługę i analizę incydentów, publikację biuletynów zabezpieczeń, koordynację reagowania na luki w zabezpieczeniach, obsługę zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV oraz przeprowadzanie testów bezpieczeństwa. Warto przy tym zauważyć, że w gestii *CERT* znajdują się jedynie serwery rządowe oraz infrastruktura krytyczna państwa[24]. W sierpniu 2009 r. ujawniono plany utworzenia pierwszej polskiej jednostki wojskowej przeznaczonej do prowadzenia działań w cyberprzestrzeni oraz ochrony MON i dowództw wojskowych przed cyberatakami. W połowie 2010 r. powołano Centrum Bezpieczeństwa Cybernetycznego, działającego w ramach 9. Batalionu Łączności w Białobrzegach, którego funkcjonowanie objęte jest ścisłą tajemnicą. W 2010 r. pojawiły się również informacje, iż MON przewiduje utworzenie pierwszego „cyfrowego" batalionu WP[25]. Rząd planuje także powołanie stanowiska pełnomocnika ds. cyberprzestrzeni, którego głównym zadaniem ma być koordynacja prac wszystkich służb zajmujących się ochroną sieci teleinformatycznych[26]. Ponadto ważnym wydarzeniem świadczącym o rosnącym zainteresowaniu RP cyberprzestrzenią było podpisanie polsko-amerykańskiej umowy o wymianie informacji i bezpieczeństwie sieciowym z 21 czerwca 2010 r. Dyrektor generalny Ministerstwa Obrony Narodowej Jacek Olbrycht skomentował to wydarzenie następująco: „Jestem głęboko przekonany, że to porozumienie pozwoli obu stronom na zwiększenie zdolności prewencji, wykrywania i reagowania na cyberataki oraz umożliwi odpowiednią ochronę informacji przetwarzanych w systemach informacyjnych i komunikacyjnych"[27].

Znaczenie cyberprzestrzeni doceniło także *NATO*, co wiązało się przede wszystkim z wydarzeniami w Estonii z 2007 r. Pierwszą reakcją paktu na kryzys estoński było wysłanie do Tallina kilku najlepszych ekspertów ds. cyberbezpieczeństwa. Problematyczny był wówczas fakt, iż zobowiązania sojusznicze wynikające z art. 5 traktatu waszyngtońskiego nie obejmowały cyberprzestrzeni. Dopiero po tych wydarzeniach sekretarz generalny Jaap de Hoop Scheffer zadeklarował, iż sojusz włączy kwestie cyberbezpieczeństwa do nowej koncepcji strategicznej. Konkretną reakcją na kryzys estoński było natomiast powołanie w Tallinie *Cooperative Cyber Defence Centre of Excellence* (*CCDCE*), którego zadaniem jest

[24] M. Lakomy, *Znaczenie cyberprzestrzeni...*, s. 64-65.

[25] *Wojsko polskie tworzy cyfrowy batalion*, Polskie Radio, 01.12.20101. Adres URL: http://www.polskieradio.pl. Dostęp: 02.02.2011; *Armia ma sposoby na ataki hakerów*, Newsweek.pl, 01.12.2010. Adres URL: http://www.newsweek.pl. Dostęp: 02.02.2011.

[26] S. Czubkowska, *Polska cyberprzestrzeń będzie pod specjalnym nadzorem*, Forsal.pl, 14.09.2010. Adres URL: http://forsal.pl. Dostęp: 10.02.2011.

[27] *Polish-US MoU on information exchange and network security*, Ministerstwo Obrony Narodowej RP, 21.06.2010.

prowadzenie badań nad bezpieczeństwem w sieci. Udział w pracach *CCDCE* wzięły: Stany Zjednoczone, Słowacja, Włochy, Hiszpania oraz państwa bałtyckie[28]. W pełni kwestie cyberbezpieczeństwa udało się uregulować dopiero w nowej koncepcji strategicznej Sojuszu Północnoatlantyckiego, uchwalonej na szczycie w Lizbonie w listopadzie 2010 r. Stwierdzono w nim, iż jednym z głównych zagrożeń dla bezpieczeństwa państw *NATO* w XXI w. będzie terroryzm w cyberprzestrzeni. Ponieważ cyberataki stają się coraz częstsze, lepiej zorganizowane i coraz bardziej szkodliwe dla administracji rządowych, biznesu, gospodarki, potencjalnie także sieci transportowych i zaopatrzeniowych oraz innej infrastruktury krytycznej; mogą osiągnąć próg, gdzie będą zagrażać narodowej i euroatlantyckiej stabilności i bezpieczeństwu. W związku z tym szefowie państw członkowskich zadeklarowali, iż *NATO* musi rozwinąć instrumenty, pozwalające na reakcję na każdy rodzaj zagrożenia. Stwierdzono, iż Sojusz będzie rozwijał w przyszłości zdolności do zapobiegania, wykrywania i obrony przed cyberatakami, m.in. poprzez koordynowanie działalności rządowych agencji oraz stworzenia scentralizowanych struktur *NATO*[29]. Obecnie polityka cyberbezpieczeństwa Paktu oparta jest na 4 filarach:

– Koordynacja i doradztwo w cyberprzestrzeni – w jego ramach utworzono *Cyber Defence Management Authority* (*CDMA*), na którego czele stoi *Cyber Defence Management Board*, składający się z szefów agencji państw członkowskich zajmujących się cyberbezpieczeństwem. Głównym zadaniem tej instytucji jest koordynacja działań państw członkowskich w zakresie obrony sieci teleinformatycznych *NATO*.

– Badania i szkolenia – odbywają się one w ramach utworzonego w Tallinie CCDCE, działającego w ramach komórki *Emerging Security Challenges Division NATO*. W jego skład wchodzi ok. 30 specjalistów.

– Pomoc dla państw członkowskich – Sojusz rozwija mechanizmy pozwalające na udzielenie natychmiastowej pomocy dla państw członkowskich zaatakowanych w cyberprzestrzeni przy wykorzystaniu tzw. *Rapid Reinforcement Teams* (*RRT*) – grup specjalistów w zakresie cyberbezpieczeństwa. Przejawem tej polityki było wsparcie udzielone Estonii w 2007 r.

– Współpraca z innymi partnerami i organizacjami międzynarodowymi – mająca na celu przede wszystkim wymianę doświadczeń i informacji oraz w niektórych przypadkach udzielanie sobie wzajemnej pomocy[30].

Znaczenie tego wymiaru bezpieczeństwa dla Sojuszu potwierdziły także konsultacje, jakie odbyły się w styczniu 2011 r. w Brukseli między zastępcą sekretarza

---

[28] C.C. Chivvis, *Considerations on NATO'S Future Direction*, „Politique étrang?re", nr 4/2009, s. 65.

[29] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, Adopted by Heads of State and Government, NATO, Lizbona, 19.11.2010.

[30] *NATO's cyber defence policy and activities*, North Atlantic Treaty Organisation. Adres URL: http://www.nato.int. Dostęp: 04.02.2011.

obrony USA Williamem J. Lynnem a przedstawicielami organizacji oraz państw członkowskich. Podczas rozmów podkreślono szczególnie znaczenie kooperacji między agencjami rządowymi a sektorem prywatnym[31].

Niewielkie zainteresowanie rozwiązaniami w tej dziedzinie wykazywała natomiast Unia Europejska, która dopiero w 2010 r. zintensyfikowała swoje prace nad strategią przeciwdziałania cyberzagrożeniom. Szczególną rolę pełni tu Komisja Europejska, która pracuje nad pakietem legislacji regulujących ten wymiar bezpieczeństwa. Jedną z propozycji KE jest m.in. pełna penalizacja wszystkich programów służących do cyberataków[32]. Organem UE zajmującym się bezpieczeństwem cyberprzestrzeni jest utworzona w 2004 r. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*ENISA*), której głównym zadaniem jest pomoc państwom członkowskim, Komisji Europejskiej i sektorowi prywatnemu w przewidywaniu, odpowiadaniu i zapobieganiu zagrożeniom pojawiającym się w sieciach teleinformatycznych. Pewne prerogatywy w tej dziedzinie ma również Wspólne Centrum Badawacze, które wraz z *ENISĄ* zorganizowało w 2010 r. pierwszą europejską symulację cyberataku[33]. Warto także wspomnieć o unijnym projekcie *FISHA* (*A Framework for Information Sharing and Alerting*), którego głównym celem stało się wypracowanie *European Information Sharing and Alerting System*, ogólnoeuropejskiego systemu wymiany i dostępu do informacji z zakresu bezpieczeństwa sieci teleinformatycznych[34].

Swój potencjał w cyberprzestrzeni rozwijają również państwa poza strefą euroatlantycką. Dobrym przykładem nowoczesnego podejścia do kwestii bezpieczeństwa teleinformatycznego jest Izrael. Według szefa wywiadu wojskowego izraelskiej armii gen. A. Yadlina wykorzystanie sieci komputerowych w celach szpiegowskich jest obecnie tak istotne dla sztuki wojennej, jak wprowadzenie wsparcia lotniczego do działań zbrojnych w XX w. Dodał on także, iż Tel Awiw dysponuje jednostką wojskową zajmującą się wyłącznie walką w środowisku cyberprzestrzennym. Wymiar ten stał się więc nowym narzędziem w ręku Sił Obronnych Izraela. Oprócz wojskowych grup reagowania w środowisku teleinformatycznym, państwo to dysponuje także specjalistami pracującymi dla wywiadu *SzinBet*, *Mossadu* oraz – co dość niezwykłe – dla ministerstwa finansów. Nie jest to jednak kompletna lista organów zajmujących się tym wymiarem bezpieczeństwa. W kwietniu 2011 r. pojawiła się bowiem informacja, iż w planach rządu jest

---

[31] J. Garamone, *Lynn Discusses Cybersecurity with NATO, U.S. leaders*, U.S. Department of State, American Forces Press Service, 24.01.2011.

[32] M. Chudziński, *KE boi się ataków DDoS*, „Dziennik Internautów", 06.12.2010. Adres UL: http://di.com.pl. Dostęp: 09.02.2011.

[33] M. Maj, *Pierwsza europejska symulacja cyberataku*, „Dziennik Internautów", 05.11.2010. Adres URL: http://di.com.pl. Dostęp: 09.02.2011; *UE: Nowym prawem w cyberprzestępczość*, „Dziennik Internautów", 01.10.2010. Adres URL: http://di.com.pl. Dostęp: 09.02.2010.

[34] *CERT Polska w projekcie FISHA*, „Dziennik Internautów", 01.04.2010. Adres URL: http://di.com.pl. Dostęp: 09.02.2011.

stworzenie kolejnej specjednostki przeznaczonej wyłącznie do zwalczania aktów cyberterroryzmu. Działałaby ona jako wsparcie istniejących już struktur izraelskiego wywiadu. Informacje te udowadniają, iż Tel Awiw jest obecnie jednym ze światowych liderów rozwiązań w zakresie cyberbezpieczeństwa. Czynnikiem ułatwiającym rozwój izraelskiego potencjału jest z pewnością wysoki poziom technologii opracowanych w tym kraju, szczególnie w zakresie zabezpieczeń komputerowych i systemów komunikacyjnych. O zaawansowaniu tych rozwiązań świadczy chociażby stworzony prawdopodobnie przez Tel Awiw wirus *Stuxnet* oraz wykorzystanie z sukcesem złośliwego oprogramowania do zakłócenia prac syryjskich radarów we wrześniu 2007 r.[35]

Obok Stanów Zjednoczonych, *NATO* i Izraela, podmiotami o zasadniczym znaczeniu dla bezpieczeństwa w cyberprzestrzeni są oczywiście Rosja i Chiny, które – zdaniem ekspertów korporacji *McAfee* – prowadzą najbardziej zaawansowane prace nad „cyberbronią", czyli oprogramowaniem zdolnym sparaliżować sieci teleinformatyczne innych państw. Mimo iż niewiele oficjalnych informacji na ten temat ujawniają rządy obu krajów, warto odwołać się do danych publikowanych w mediach i specjalistycznych raportach. Stosunek Federacji Rosyjskiej do cyberprzestrzeni trafnie oddał gen. W. Szerstujuk, szef rosyjskiego Instytutu Spraw Bezpieczeństwa Informacyjnego. Zapytany w jednym z wywiadów, czy Rosja prowadzi prace nad rozwojem cyberbroni, stwierdził: „To nie tylko Rosja. To XXI wiek. I wynika to z rozwoju technologicznego". Zdaniem generała, rosyjska polityka bezpieczeństwa teleinformatycznego skupia się głównie na zwalczaniu zagrożenia ze strony grup terrorystycznych. Co prawda rosyjska cyberprzestrzeń nie doświadczyła jeszcze poważnych aktów cyberterroryzmu, jednak – jak stwierdził – poważne zagrożenie rodzi wykorzystanie Internetu przez zorganizowane grupy fundamentalistów do rekrutacji nowych członków oraz organizacji i planowania zamachów[36]. Warto dodać, iż Federacja Rosyjska stała się jednym z pierwszych krajów, który zaproponował podpisanie międzynarodowego porozumienia w sprawie kontroli zbrojeń w sieci[37]. Nieoficjalnie jednak wiadomo, iż Federacja Rosyjska od dawna rozwija swoje zdolności ofensywne w cyberprzestrzeni. O rosyjskim potencjale świadczyły wydarzenia z Estonii, Gruzji i Kirgistanu, które udowodniły, iż kraj ten należy do światowych potęg w tej dziedzinie. Kevin Coleman, ekspert *DefenseTech*, odnosząc się do tego problemu stwierdził, iż „Rosja posiada zaawansowane zdolności (...) wymagane do przeprowadzenia cyberataku w każdym miejscu i w każdej chwili". Ocenił on, iż Kreml na rozwój swojego potencjału

[35] D. Eshel, *Israel Adds Cyber-Attacks to IDF*, „Aviation Week DTI", 10.02.2010; Israel May Create Elite Cyber Security Unit, eSecurity Planet, 07.04.2011. Adres URL: http://www.esecurityplanet.com. Dostęp: 08.04.2011; D. Lev, *Experts: Israel's Cyber-Defense Can Stop Stuxnet Worm*, „Israel National News", 04.10.2010. Adres URL: http://www.israelnationalnews.com. Dostęp: 08.04.2011.

[36] D. Talbot, *Russia's Cyber Security Plans*, „Technology Review", MIT, 16.04.2010.

[37] J. Markoff, A.E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, „The New York Times", 12.12.2009.

wydaje ok. 127 milionów dolarów rocznie, zatrudniając ok. 7300 specjalistów. Do najsilniejszych jego stron Coleman zaliczył sieć botnet oraz dysponowanie zaawansowanym złośliwym oprogramowaniem, w tym wirusami opartymi na zasadzie „bomb logicznych", trojanami oraz innymi narzędziami przeznaczonymi do przeprowadzania wywiadu elektronicznego[38]. Działalność Rosji w cyberprzestrzeni opiera się na tzw. *Russian Business Network*, która kontroluje największą na świecie sieć botnet, liczącą według *DefenseTech* od 150 do 180 mln komputerów. Świadczy to o tym, jak ogromnym potencjałem w cyberprzestrzeni dysponuje Moskwa[39].

Podobny posiadają również Chiny, które udowodniły swoje zdolności dokonując wielokrotnych, udanych ataków na amerykańskie sieci sektora publicznego i prywatnego. Tak jak w przypadku Rosji, niewiele jest oficjalnych informacji na temat polityki cyberbezpieczeństwa Chińskiej Republiki Ludowej. Przede wszystkim należy mieć na uwadze, iż ChRL jest jednym z nielicznych krajów, w którym kontrola korzystania z Internetu jest tak wysoka. Podstawowym założeniem chińskiej polityki cyberbezpieczeństwa, przynajmniej oficjalnie, jest zwalczanie incydentów komputerowych i nielegalnego bądź szkodliwego oprogramowania. Tylko w 2010 r. w Chinach aresztowano ponad 460 osób pod zarzutami udziału we włamaniach komputerowych. Pekin stał także za wieloma międzynarodowymi inicjatywami zmierzającymi do regulacji wykorzystania sieci, m.in. rezolucją 57/539 Zgromadzenia Ogólnego ONZ dotyczącą utworzenia globalnej kultury cyberbezpieczeństwa. Innym przejawem ich aktywności było zawarcie w 2009 r. porozumienia z państwami *ASEAN* w sprawie wspólnego reagowania na incydenty teleinformatyczne[40]. Z drugiej strony, od podawanych publicznie wiadomości należy odróżnić rzeczywiste działania podejmowane przez Chiny. Zdaniem ekspertów *DefenseTech*, obecnie posiadają one drugi największy potencjał w cyberprzestrzeni na świecie. Co prawda na jego rozwój przeznacza się tylko ok. 55 mln dolarów, jednak rekompensowane jest to dużą grupą wysokiej klasy specjalistów pracujących dla rządu – szacowaną na ok. 10 tys. osób. Kevin Coleman do najsilniejszych stron chińskiego potencjału zaliczył, podobnie jak w przypadku Rosji: niezwykle rozwinięte sieci botnet oraz zaawansowane złośliwe oprogramowanie każdego typu. Ponadto – jego zdaniem – Chiny są obecnie najpoważniejszym zagrożeniem dla cyberbezpieczeństwa państw zachodnich[41]. O rosnących możliwościach ChRL świadczy także ujawniony przez „The Sunday Times" chiński

[38] K. Coleman, *Russia's Cyber Forces*, DefenseTech, 27.05.2008. Adres URL: http://defensetech.org. Dostęp: 04.02.2011.

[39] K. Coleman, *Russia Now 3 and 0 in Cyber Warfare*, DefenseTech, 30.01.2009. Adres URL: http://defensetech.org. Dostęp: 05.02.2011.

[40] *China's Cybersecurity and Pre-Emptive Cyber War*, China Defense Mashup, 13.03.2011. Adres URL: http://www.china-defense-mashup.com. Dostęp: 04.02.2011; *China's Faltering Cybersecurity Efforts Offer Chance for Engagement*, China Defense Mashup, 10.12.2010. Adres URL: http://www.china-defense-mashup.com. Dostęp: 04.02.2011.

[41] K. Coleman, *China's Cyber...*

plan działań w cyberprzestrzeni w wypadku wojny z USA, który zakładał nie tylko zablokowanie systemu finansowego czy telekomunikacyjnego Stanów Zjednoczonych, ale także sparaliżowanie funkcjonowania floty amerykańskich lotniskowców[42].

Warto również pamiętać, iż coraz większymi możliwościami w cyberprzestrzeni dysponują Iran oraz Korea Północna. Reżim w Phenianie już kilkukrotnie był oskarżany o przeprowadzanie ataków na południowokoreańskie i amerykańskie witryny internetowe. Najpoważniejszy miał miejsce w lipcu 2009 r. Tylko w Korei Południowej zainfekowanych zostało ok. 18 tys. komputerów oraz 11 witryn rządowych. Zdaniem eksperta *American Enterprise Institute* Nicholasa Eberstadta, ataki te stanowią dowód, iż Korea Północna stara się uzupełnić swój potencjał nuklearny o zdolności ofensywne w cyberprzestrzeni[43]. Ocenia się, iż Phenian zatrudnia ok. 12 tys. specjalistów i na działania w cyberprzestrzeni wydaje ok. 56 milionów dolarów rocznie, co stawia go – według specjalistów – na 8 pozycji na świecie[44]. Podobnie wygląda polityka Iranu, który zaliczany jest przez *CIA* do 5 państw zdolnych do prowadzenia wojny w cyberprzestrzeni. O zdolnościach irańskich specjalistów świadczą działania tzw. *Iran Cyber Army*, stojącej za regularnymi atakami na amerykańskie i europejskie serwery. W jednym z takich ataków, w październiku 2010 r. włamano się na ponad tysiąc francuskich, brytyjskich i amerykańskich stron internetowych[45]. *ICA* dysponuje przy okazji jedną z największych sieci botnet – liczącą ok. 400 tys. komputerów[46]. Zdaniem *DefenseTech*, Iran posiada ok. 2400 specjalistów pracujących dla korpusu Islamskiej Gwardii Rewolucyjnej. Budżet tych sił wynosi – zdaniem Kevina Colemana – ok. 76 milionów dolarów[47]. Ponadto, o zaawansowaniu irańskich rozwiązań w tej dziedzinie świadczy fakt, iż Iran stworzył na początku 2011 r. jednostkę policyjną przeznaczoną wyłącznie do ścigania przestępstw w sieci[48].

---

[42] T. Reid, *China's cyber army is preparing to march on America, says Pentagon*, „The Sunday Times", 08.09.2007. Szerzej na temat amerykańsko-chińskiego konfliktu w cyberprzestrzeni w: C. Bartholomew, L.M. Wortzel, *Report to Congress 2009*, U.S.-China Economic and Security Review Commission; N. Hachigan, *China's Cyber-Strategy*, „Foreign Affairs", March/April 2001.

[43] D. Kirk, *What's behind cyber attacks on South Korea, US?*, „The Christian Science Monitor", 08.07.2009; S. Gorman, E. Ramstad, *Cyber Blitz Hits U.S., Korea*, „The Wall Street Journal", 09.07.2009.

[44] *North Korea Waging Cyber Warfare?*, CBS News, 09.07.2009. Adres URL: http://www.cbsnews.com. Dostęp: 04.02.2011; C. Clark, *North Korea: Cyber Mad Dogs or Bluster Kings?*, „Dod Buzz", 20.04.2009. Adres URL: http://www.dodbuzz.com. Dostęp: 04.02.2011.

[45] *Iran's Cyber Army Hacks 1,000 US, British, French Govt Websites*, FARS News Agency, 30.08.2010. Adres URL: http://english.farsnews.com. Dostęp: 04.02.2011.

[46] *Irańska Cyber Army tworzy botnet*, „Dziennik Internautów", 31.10.2010. Adres URL: http://di.com.pl. Dostęp: 09.02.2011.

[47] K. Coleman, *Iranian Cyber Warfare Threat Assessment*, DefenseTech, 23.09.2008. Adres URL: http://defensetech.org/. Dostęp: 04.02.2011.

[48] *1st Cyber police unit launched in Iran*, Press TV, 24.01.2011. Adres URL: http://previous.presstv.ir. Dostęp: 04.02.2011.

ZAKOŃCZENIE

Cyberzagrożenia, które pojawiły się wraz z procesem komputeryzacji i upowszechnianiem Internetu, podlegają nieustannej ewolucji. Początkowo ich przejawem były niezbyt poważne ataki, za którymi stali domorośli hobbyści. W drugiej połowie lat 90. charakter działań hakerów zaczął się zmieniać, wraz z rosnącym zainteresowaniem państw tym obszarem. Cyberprzestrzeń zaczęła bowiem umożliwiać realizowanie interesów, które były niezwykle trudne do osiągnięcia tradycyjnymi metodami. Czynnikiem wzmacniającym tę tendencję jest specyficzny charakter sieci teleinformatycznych: łatwa do osiągnięcia anonimowość, brak tradycyjnych granic oraz niewielkie koszty działalności w tej przestrzeni. Ponadto zainteresowaniu państw sprzyjają także niejasności związane z zastosowaniem do cyberzagrożeń istniejących rozwiązań politycznych (np. traktatów sojuszniczych) oraz zapisów prawa międzynarodowego. Przełomowym momentem dla percepcji nowych wyzwań dla bezpieczeństwa stały się z pewnością lata 2007/2008. Wydarzenia z Estonii, Gruzji czy Iranu udowodniły, iż cyberprzestrzeń może być wykorzystywana do działań zakłócających realizowanie podstawowych funkcji państw.

Najwcześniej potencjał przestrzeni teleinformatycznej odkryły Stany Zjednoczone, Federacja Rosyjska oraz Chińska Republika Ludowa. Strategia polityczna oraz rozwiązania technologiczne opracowane w tych krajach nie zakładały jedynie wykorzystania cyberprzestrzeni do działań defensywnych (np. ochrony infrastruktury krytycznej), ale także ofensywnych. Stany Zjednoczone już w latach 90. dostrzegły potencjalne problemy wiążące się z szybko postępującymi procesami komputeryzacji i informatyzacji wszystkich dziedzin życia. Wynikało to przede wszystkim z faktu, iż USA już w tamtym okresie były najczęstszym celem ataków hakerskich. Wpłynęło to na stosunkowo szybkie rozpoczęcie prac badawczych, które trafnie przewidziały dalszy rozwój cyberprzestrzeni oraz specyfikę działań w tym wymiarze (m.in. wątpliwości natury prawnej i politycznej)[49]. Co ważne, USA były jednym z nielicznych krajów, które podjęły konkretne działania w tej dziedzinie zanim doszło do ataków na Estonię i Gruzję. Doprowadziły one do powołania pierwszego na świecie dowództwa wojsk w cyberprzestrzeni, co w perspektywie czasu zapewni USA odpowiednie możliwości wykorzystania sieci teleinformatycznych w warunkach konfliktu zbrojnego. Stąd można stwierdzić, iż USA są z pewnością liderem nowoczesnych rozwiązań w dziedzinie cyberbezpieczeństwa.

Na doświadczeniach oraz rozwiązaniach amerykańskich z pewnością wzorują się inne państwa strefy euroatlantyckiej. Początkiem polskiej polityki cyberbezpieczeństwa był z pewnością kryzys w Estonii. Doświadczenia rządu w Tallinie sprawiły, iż polskie służby podjęły działania zmierzające do oceny stanu

[49] Zob. B.W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, U.S. Army War College.

zabezpieczeń serwerów rządowych. Pozwoliło to również na opracowanie pierwszego rządowego dokumentu, który całościowo ujął problematykę wpływu cyberprzestrzeni na bezpieczeństwo państwa. Polskie rozwiązania w tej dziedzinie w dużej mierze opierają się na doświadczeniach USA i innych państw europejskich. Obok powołania instytucji zajmującej się ochroną sieci rządowych (*CERT*), co staje się już powoli standardem, Warszawa utworzyła również pierwszą jednostkę wojskową przeznaczoną do działań w cyberprzestrzeni, co należy uznać za spory sukces. Właściwy kierunek rozwoju tej dziedziny bezpieczeństwa nakreślił także Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016. Za niezrozumiały natomiast należy uznać brak zainteresowania polskich służb uczestnictwem w natowskim *CCDCE* w Tallinie.

Jeśli chodzi o państwa sojusznicze, z pewnością jednym z najbardziej zaawansowanych państw jest Izrael. Mimo iż oficjalne informacje na temat polityki cyberbezpieczeństwa Izraela są bardzo rzadkie, potencjał Tel Awiwu można oceniać na podstawie wykorzystania sieci teleinformatycznych wobec krajów Bliskiego Wschodu. Zastosowanie wirusa do oślepienia syryjskich radarów było pierwszym w historii przykładem operacji wojskowej, której sukces zawdzięczano przede wszystkim wykorzystaniu przestrzeni teleinformatycznej. Zdecydowanie większe znaczenie ma jednak opracowanie wirusa *Stuxnet*. Według ekspertów, jego użycie przeciwko Iranowi należy oceniać w podobnych kategoriach jak wybuch pierwszej bomby atomowej[50]. Program ten stał się najbardziej zaawansowaną cyberbronią kiedykolwiek stworzoną, stanowiącą wejście w nowy etap „wyścigu zbrojeń" w środowisku cyberprzestrzennym. Jego znaczenie potwierdził sukces przynajmniej częściowego spowolnienia irańskiego programu atomowego.

Co ciekawe zdecydowanie mniejszą dynamikę w tej dziedzinie wykazują organizacje międzynarodowe. Sojusz Północnoatlantycki jest organizacją o zaawansowanych rozwiązaniach w dziedzinie cyberbezpieczeństwa. W głównej mierze wynika to z ataku na Estonię, co wymusiło m.in. uwzględnienie tego wymiaru w nowej koncepcji strategicznej Sojuszu. Mimo to należy zauważyć, iż rozwiązania proponowane przez Sojusz są dość ograniczone. Wynika to z jednej strony z nadal niewielkiej koordynacji między państwami, a z drugiej powodem są także poważne wątpliwości natury politycznej i prawnej. Wykorzystanie sieci teleinformatycznych nadal bowiem wymyka się tradycyjnym rozwiązaniom polityczno-prawnym, na których oparte jest funkcjonowanie Paktu. *NATO* wypracowało mechanizmy pomocy zaatakowanym za pomocą sieci państwom członkowskim, co jednak nie wynika z zapisów traktatu waszyngtońskiego. Zdecydowanie mniejsze znaczenie ma ta dziedzina we Wspólnej Polityce Zagranicznej i Bezpieczeństwa Unii Europejskiej. UE dopiero niedawno zauważyła wagę cyberprzestrzeni, przez co jej rozwiązania w tej dziedzinie są zdecydowanie zapóźnione.

[50] *Stuxnet heralds age of cyber weapons, virtual arms race*, „Homeland Security Newswire", 27.01.2011. Adres URL: http://homelandsecuritynewswire.com. Dostęp: 01.03.2011.

Federację Rosyjską należy uznać za prekursora wykorzystania nowego wymiaru bezpieczeństwa na masową skalę dla uzyskania określonych korzyści politycznych. Trzykrotnie w ostatnich latach rosyjscy specjaliści dokonywali cyberataków na infrastrukturę sieciową swoich sąsiadów, za każdym razem realizując założone cele. Zwycięstwo w trzech „cyberwojnach" udowodniło, iż Rosja jest obecnie jedną z największych potęg w cyberprzestrzeni. Ponadto – w odróżnieniu od państw strefy euroatlantyckiej – Rosja wykorzystuje cyberprzestrzeń przede wszystkim do realizacji swoich interesów na arenie międzynarodowej. Podobnie należy oceniać politykę Chin, które również od przełomu XX i XXI w. stoją za znaczną częścią najpoważniejszych cyberataków w sieci (*Aurora*, *Titan Rain*). W odróżnieniu jednak od Federacji, która specjalizuje się w aktach cyberterroryzmu, ChRL zasłynęła przede wszystkim akcjami cyberszpiegowskimi. Większość głośnych ataków chińskich hakerów miało na celu przede wszystkim wyprowadzenie informacji niejawnych o charakterze politycznym, gospodarczym bądź militarnym. Warto także pamiętać, iż coraz większymi zdolnościami w tej dziedzinie mogą się pochwalić Iran oraz Korea Północna. Co prawda ich dotychczasowa aktywność w Internecie jest niewielka, jednak rosnący potencjał może stanowić pewne zagrożenie w przyszłości.

Reasumując należy stwierdzić, iż procesy komputeryzacji i informatyzacji, które leżą u podstaw rozwoju cyberprzestrzeni, oprócz niezaprzeczalnych korzyści, będą w przyszłości stanowiły coraz poważniejsze zagrożenie dla bezpieczeństwa państw. Potwierdzają to wydarzenia z początku XXI w., kiedy doszło do pierwszych przypadków ofensywnego wykorzystania sieci na masową skalę. Odpowiednia percepcja i reakcja na cyberzagrożenia jest obecnie jednym z najpoważniejszych problemów stojących przed polityką bezpieczeństwa poszczególnych rządów. Szybkość reakcji na nowe wyzwania oraz właściwa ścieżka rozwoju będą w przyszłości determinowały nie tylko sytuację bezpieczeństwa, ale częściowo również status państw na arenie międzynarodowej.

ABSTRACT

The article tackles the problem of sensitivity to threats that appear in cyber space in the security policies of selected international agents, including among others: the USA, Poland, Israel, Russia, the European Union and the North Atlantic Treaty. Cyber threats intensified with the development of information technology and the popularization of the Internet. Initially they were not very serious attacks done by self-taught programmers. Since mid-1990s the character of the hackers' activity evolved with growing interest of individual countries in cyber space issues. Many countries, including the USA, Russia and China, began to focus on the development of their potential in this area in order to ensure maximum protection of their critical infrastructure against cyber attacks. In the 21st century the significance of cyber space for international security is constantly increasing. The promptness of response to new problems and the most appropriate path of development of the potential in this area will in the future determine not only the security but to some extent also the status of particular countries on the international arena.