Mateusz Karatysz
Uniwersytet im. Adama Mickiewicza w Poznaniu

Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski

Wprowadzenie

Tradycyjne definicje bezpieczeństwa podlegają coraz silniejszym tendencjom do poszerzania znaczenia[1]. Klasyczne ich rozumienie, prezentujące zespół działań zmniejszających wrażliwość na atak, podejmowanych za pomocą potencjału obronnego, rozszerzone zostało o czynniki gospodarcze, technologiczne, ekologiczne, demograficzne czy społeczne. Taki zakres przedmiotowy bezpieczeństwa sprawia, że jedną z jego istotnych części staje się obecnie polityka zwalczania zagrożeń w cyberprzestrzeni. Ta nowa płaszczyzna społecznych interakcji, traktowana jako przestrzeń nieskrępowana czasem i odległością, stanowi obecnie pole dla nowych jakościowo zagrożeń. Wirtualna rzeczywistość, pozbawiona geograficznego parametru mierzalności, nie tylko przekracza kategorię terytorialności, ale przede wszystkim, za sprawą nieograniczonej sfery wolności słowa, uniemożliwia pełną kontrolę nad nadawcą, przekazem oraz odbiorcą. Złudne przekonanie o pełnej anonimowości powoduje, że nowy obszar ludzkiej działalności, pozbawiony tradycyjnej kontroli, sprawdzonej w świecie organicznym, staje się areną coraz chętniej wykorzystywaną przez cyberprzestępców. W takich okolicznościach zjawisko cyberprzestępczości jest obecnie przedmiotem opracowywania komplementarnych rozwiązań prawnych zarówno na szczeblach międzynarodowych, jak i krajowych. I choć ustawodawstwo polskie sukcesywnie podejmuje próby uregulowania kwestii bezpieczeństwa w sieci, to skuteczna walka na tym gruncie napotyka na poważny problem wynikający z błędnej aksjologii, ignorującej to, że bezpieczeństwo państwa zależy od różnych systemów informacyjnych – nie tylko tych, będących we władaniu jednostek organizacyjnych administracji publicznej. Ponadto brak zrozumienia, iż Internet to przestrzeń oderwana od fizycznego

[1] Zob. J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

terytorium państwa, skutkuje ograniczeniem nie tylko pola ochrony, ale i samej definicji bezpieczeństwa. Założenia te wpływają na zredukowanie możliwości dostrzeżenia zagrożeń płynących z wirtualnej rzeczywistości, podważając tym samym zdolność do skutecznej obrony.

Cybersieć, cyberterroryzm, cyberprzestępstwo

Prace nad siecią internetową trwają od lat 60. XX w., jednak gwałtowny ich rozwój nastąpił dopiero na początku lat 90. wraz z pojawieniem się systemu WWW. Poza upowszechnieniem stron internetowych czy poczty elektronicznej, użytkownicy sieci weszli w posiadanie fizycznej infrastruktury umożliwiającej strumieniowe przesyłanie danych z olbrzymimi prędkościami. „Podstawowa konstrukcja Internetu opiera się na otwartości zarówno architektury jego infrastruktury, jak i kultury jego twórców i użytkowników. Prostota i łatwość łączenia różnych komputerów pozwoliła na ogromne rozszerzenie liczby użytkowników, a otwarta filozofia jego kształtowania stworzyła z niego ogromnie atrakcyjne, interakcyjne na wielu poziomach medium”[2]. Szacuje się, że liczba użytkowników Internetu przekroczyła w lipcu 2012 r. 2,4 mld osób, co stanowi 34% populacji całego świata[3]. Według najnowszych danych, w Polsce dostęp do Internetu posiada już 24,9 mln obywateli, co stanowi prawie 65% populacji kraju[4].

Upowszechnianiu się technologii komunikacyjnych oraz wzrostowi zamożności obywateli świata towarzyszy rozwój społeczeństwa informacyjnego, który uzależniony jest od coraz bardziej zintegrowanych, konwergentnych narzędzi multimedialnych. „(...) Niemal każdy komputer oferuje użytkownikowi możliwość nagrywania CD-ROM i DVD, które łączą tekst, nieruchome obrazy z dźwiękowymi i wideoklipami, jak również możliwość połączenia się z siecią globalną (...)”[5]. Narzędzia te stają się źródłem swobodnego i nieskrępowanego dostępu do każdej informacji, o każdej porze i za pomocą każdego multimedium. „Wszystko to w oparciu o niewielkie koszty użytkowania sprawiło, że coraz więcej podmiotów (rządów, instytucji i firm), a także indywidualnych osób decyduje się przenosić różne elementy swojej

[2] T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

[3] *World Internet Usage and Population Statistics Jun 30, 2012*, http://www.internetworldstats.com/stats.htm, 10.11.2012 r.

[4] *Internet and Facebook Usage in Europe, Jun 30, 2012,* http://www.internetworldstats.com/stats4.htm#europe, 10.11.2012 r.

[5] T. Goban-Klas, op. cit., s. 146.

codziennej aktywności do cyberprzestrzeni. (...) Dostępny za pomocą komputerów, telefonów komórkowych, tabletów, a nawet samochodów czy lodówek Internet stał się jednym z podstawowych mediów, obok elektryczności, gazu i bieżącej wody. Stał się synonimem wolności słowa i nieskrępowanego przepływu informacji, a w pewnych przypadkach z powodzeniem służy jako narzędzie rewolucji i zmian społecznych"[6].

Nie ulega wątpliwości, że to właśnie powszechność dostępu oraz niewielka liczba regulacji prawnych stanowią o sile Internetu, jak i o jego słabości. Rację ma Debra Shinder twierdząc, że „bezpieczeństwo komputerów i sieci oparte jest na zachowaniu (...) równowagi między przeciwstawnymi czynnikami, zabezpieczeniem i dostępnością. Im bardziej system jest bezpieczny, tym trudniej dostępny i *vice versa*. Ponieważ jedną z najważniejszych cech sieci musi być dostępność, nigdy żadna sieć nie będzie w 100 proc. bezpieczna"[7]. Stanowi to ogromne wyzwania dla społeczności międzynarodowej, narażonej na przestępstwa cybernetyczne z coraz silniejszym akcentem na cyberterrorystyczne.

Samo zjawisko cyberterroryzmu doczekało się już kilku definicji. Za Tomaszem Szubrychtem, do najbardziej reprezentatywnych zalicza się następujące koncepcje:

– Dorothy Denning: „Groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu"[8];

– James Lewis: „Wykorzystanie sieci komputerowych jako narzędzi do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka,

[6] M. Grzelak, K. Riedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 126.

[7] D. Shinder, *Cyberprzestępczość*, Gliwice 2004, s. 61; cyt. za: A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia terroryzmem*, Warszawa 2010, s. 371.

[8] D. Denning, *Cyberterrorism*, Georgetown University 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, 11.11.2012 r.; cyt. za: T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego,* „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, nr 1, s. 175.

transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań”[9];

– Mark Pollitt: „Jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe”[10].

Zaprezentowane wyżej definicje nie wyczerpują oczywiście listy wszystkich prób wyznaczenia ram definicyjnych działań cyberterrorystycznych. Jednak już w oparciu o nie można zaobserwować określoną prawidłowość. Aby doszło do działania cyberterrorystycznego, musi zostać spełniony podstawowy warunek: narzędzie wykorzystane do przeprowadzenia ataku musi być, w chwili jego dokonywania, podłączone do Internetu tak samo, jak jego cel, a skutkiem takiego działania winny być znaczne straty.

Czy jednak każdy atak w sieci można sklasyfikować jako akt cyberterroryzmu? By odpowiedzieć na to pytanie, konieczne staje się wprowadzenie do dalszych rozważań definicji cyberprzestępczości. „Już w 2004 r. specjaliści zajmujący się badaniem przestępstw w cyberprzestrzeni poinformowali, że pierwszy raz w historii dochody z tej działalności były większe niż zyski z handlu bronią czy narkotykami. Niestety w polskim prawie nie ma legalnej, czyli jednolitej (...) definicji cyberprzestępczości”[11]. Kwestię tę regulują natomiast przepisy międzynarodowe.

Komisja Wspólnot Europejskich definiuje cyberprzestępstwo jako „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom”[12], wyróżniając jednocześnie ich trzy grupy:

– pierwsza obejmuje „tradycyjne” formy przestępstw takie, jak: oszustwo czy fałszerstwo popełnione przy użyciu elektronicznych sieci informatycznych i systemów informatycznych;

– druga publikację nielegalnych treści w mediach elektronicznych;

[9] J. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies 2002, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, 11.11.2012 r.; cyt. za: ibidem, s. 175.

[10] M. Pollit, *Cyberterrorism – Fact or Fancy?*, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html, 11.11.2012 r., cyt. za: ibidem, s. 175.

[11] R. Szymkiewicz, *Czym jest cyberprzestępstwo?*, http://prawo-karne.wieszjak.pl/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html, 12.11.2012 r.

[12] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, Bruksela, z dnia 22 maja 2007 r., KOM(2007) 267, cyt. za: M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prawo i prokuratura” 2012, nr 7–8, s. 247.

– trzecia dotyczy przestępstw typowych dla sieci łączności elektronicznej[13].

Organizacja Narodów Zjednoczonych proponuje z kolei, by w rezultacie definicji wypracowanej podczas Dziesiątego Kongresu Narodów Zjednoczonych mówić o cyberprzestępczości w wąskim znaczeniu – jako działaniach wymierzonych przeciw bezpieczeństwu systemów komputerowych oraz procesowanych przez nie danych, a także w szerokim znaczeniu – wszelkich nielegalnych działaniach popełnionych lub dotyczących systemów i sieci komputerowych[14].

W związku z brakiem jednolitej definicji działań cyberprzestępczych i cyberterrorystycznych, linia pomiędzy internetowym terroryzmem a wykroczeniem poza prawnie przyjęte normy zachowań w sieci jest nie tylko cienka, lecz także trudna do wytyczenia. Pamiętać należy o jednym: dopóki atakujący nie zamierza za pomocą swoich działań uśmiercać czy powodować zniszczeń newralgicznych sfer działalności państwa, a jego jedynymi pobudkami jest wyrażenie sprzeciwu wobec aktualnie panujących porządków, trudno jednoznacznie sklasyfikować jego działalność jako terrorystyczną.

Rada Europy i Unia Europejska a problem cyberbezpieczeństwa

Kwestie dotyczące problematyki cyberbezpieczeństwa na gruncie europejskim od początku poprzedniej dekady poruszane były w sposób dwutorowy. Działania zmierzające ku dostosowaniu przepisów prawa do zmieniającego się otoczenia jako pierwsze podjęły Rada Europy oraz Unia Europejska.

Już w listopadzie 2001 r. Rada Europy przyjęła *Konwencję o Cyberprzestępczości*, która uznana została za jedno z najważniejszych osiągnięć Rady w obszarze ochrony społeczeństwa przed zagrożeniami w cyberprzestrzeni[15]. To pierwszy tego typu dokument, który poświęcony został przeciwdziałaniu przestępstwom związanym z wykorzystaniem Internetu. W jego treści zdefiniowane zostały pojęcia: przestępstw przeciwko poufności, integralności i dostępności danych informatycznych oraz systemów. Konwencja zobowiązała ponadto jej sygnatariuszy do przyjęcia wszelkich środków prawnych umożliwiających zabezpieczenie danych informatycznych, gdy istnieje ryzyko ich utraty lub modyfikacji. Co ważne, w części ogólnej

[13] M. Siwicki, op. cit., s. 247.
[14] Ibidem, s. 248.
[15] A. Suchorzewska, op. cit., s. 152.

konwencji zdefiniowano zasady dotyczące ekstradycji czy przekazywania informacji między stronami konwencji, kładąc duży nacisk na współpracę międzynarodową w przedmiocie dokumentu. Mimo iż dokument zawiera szereg sformułowań natury ogólnej, stanowi on podstawę do tworzenia wspólnej polityki bezpieczeństwa w cyberprzestrzeni.

Działalność Unii Europejskiej w obszarze bezpieczeństwa w cyberprzestrzeni datowana jest jeszcze na 1997 r., kiedy to Parlament Europejski oraz Rada Unii Europejskiej wydały dyrektywę w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym[16]. Na jej uszczegółowienie trzeba było czekać do lipca 2002 r. Powstał wtedy nowy akt, który objął swoim zasięgiem cały sektor komunikacji elektronicznej. *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej*[17] zobowiązuje państwa członkowskie do zapewnienia ekwiwalentnego stopnia ochrony podstawowych praw i wolności osób fizycznych, a w szczególności prawa do prywatności w odniesieniu do przetwarzania danych osobowych oraz do zapewnienia swobodnego przepływu tych danych osobowych we wspólnocie. Dyrektywa ta była reakcją na coraz szerszy zasięg komunikacji elektronicznej – a co za tym idzie – na szerszy wachlarz usług opartych o przetwarzanie danych dotyczących użytkowników.

W 2003 r., decyzją Rady przyjęta została *Europejska Strategia Bezpieczeństwa – Bezpieczna Europa w Lepszym Świecie*[18] uznająca terroryzm za główne i narastające zagrożenie dla całej Europy. Już w 2004 r. Parlament Europejski i Rada Unii Europejskiej powołały Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, a głównym jej zadaniem uczyniły formułowanie ekspertyz wysokiej szczegółowości, będących pomocą dla państw członkowskich w przypadkach sytu-

[16] *Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym*, s. 1. http://*www.giodo.gov.pl/plik/id_p/340/t/pdf/j/pl/*, 15.11.2012 r.

[17] *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej*, s. 1. http://www.giodo.gov.pl/568/id_art/607/j/pl/, 15.11.2012 r.

[18] *Bezpieczna Europa w Lepszym Świecie – Europejska Strategia Bezpieczeństwa z dnia 12 grudnia 2003 r.*, http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIPL.pdf, 15.11.2012 r.

acji kryzysowych związanych z informatyką. Uzupełnieniem tych działań stała się ramowa decyzja Rady z dnia 24 lutego 2005 r.: *W sprawie ataków na systemy informatyczne*[19].

Kolejnym krokiem w walce z cyberprzestępczością stał się Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów *W kierunku ogólnej strategii zwalczania cybeprzestępczości* z dnia 22 maja 2007 r.[20], wydany w celu poprawy skuteczności w zwalczaniu cyberprzestępczości na szczeblu krajowym, unijnym i międzynarodowym. Dokument, poza wprowadzeniem właściwej sobie definicji cyberprzestępczości, posiada trzy cele operacyjne zakładające: 1) poprawę i ułatwienie koordynacji i współpracy między zespołami ds. przestępczości internetowej, innymi właściwymi organami oraz ekspertami w całej Unii; 2) stworzenie przy współpracy z państwami członkowskimi, właściwymi organizacjami unijnymi i międzynarodowymi oraz innymi zaangażowanymi podmiotami spójnej strategii ramowej UE w sprawie zwalczania cyberprzestępczości; 3) zwiększenie wiedzy na temat kosztów i niebezpieczeństw związanych z cyberprzestępczością.

Jednym z ostatnich efektów prac nad problematyką bezpieczeństwa, w ramach programu ogólnego *Bezpieczeństwo i ochrona wolności*, Unii Europejskiej jest ustanowiony na lata 2007–2013, decyzją Rady, specjalny program *Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa*[21] sygnalizujący głęboką potrzebę poszukiwania rozwiązań komplementarnych o wymiarze krajowym, europejskim i międzynarodowym.

Polityka ochrony cyberprzestrzeni RP

W polskim ustawodawstwie nie istnieje jedna regulacja prawna zawierająca wszystkie przepisy dotyczące odpowiedzialności za nadużycia w sieci. Przepisy te zostały rozproszone w kilku aktach prawnych,

[19] *Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF, 15.11.2012 r.

[20] *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, W kierunku ogólnej strategii zwalczania cybeprzestępczości z dnia 22 maja 2007 r.*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:PL:HTML, 15.11.2012 r.

[21] Decyzja Rady 2007/124/WE z dnia 12 lutego 2007 r. ustanawiająca na lata 2007-2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa".

m.in. w Kodeksie karnym oraz Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 nr 133 poz. 883), Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994 nr 24 poz. 83), Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz. 1204). Ponadto, zgodnie z obowiązującymi zasadami, polskie ustawodawstwo musi uwzględniać rozwiązania odpowiednich aktów prawa europejskiego w tym Konwencji o Cyberprzestępczości oraz ramowej decyzji Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne. Zgodnie z powyższym, ustawodawca przyjął więc zasadę uzupełniania istniejących przepisów o kwestie związane z tym zagadnieniem[22].

W ramach krajowych zadań realizowanych w celu poprawienia bezpieczeństwa cyberprzestrzeni RP, rząd podjął działania m.in. w celu stworzenia dwóch programów, tj. Rządowego programu obrony cyberprzestrzeni RP na lata 2009–2011 oraz na lata 2011–2016. Ponadto 28 sierpnia 2012 r. Ministerstwo Administracji i Cyfryzacji przedstawiło dokument pt. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, który stworzony został w oparciu m. in. o założenia programu obrony cyberprzestrzeni RP na lata 2009–2011.

Jako główne przesłanki przyświecające nowej propozycji, Ministerstwo Administracji i Cyfryzacji wskazuje wzrost zagrożeń dla systemów teleinformatycznych, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne. Ponadto, jak wskazano w dokumencie, „w czasie, gdy panuje swoboda przepływu osób, towarów, informacji i kapitału – bezpieczeństwo demokratycznego państwa zależy od wypracowania mechanizmów pozwalających skutecznie zapobiegać i zwalczać zagrożenia dla bezpieczeństwa cyberprzestrzeni”[23].

Adresatami dokumentu są więc wszyscy użytkownicy cyberprzestrzeni w obrębie państwa oraz przedstawicielstw kraju poza jego terytorium.

„Polityka Ochrony Cyberprzestrzeni RP obowiązuje administrację rządową:

– urzędy obsługujące naczelne organy administracji rządowej: Prezesa Rady Ministrów, Radę Ministrów, ministrów i przewodniczących określonych w ustawach komitetów;

[22] A. Suchorzewska, op. cit., s. 206, 294.

[23] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, wrzesień 2012, s. 4.

– urzędy obsługujące centralne organy administracji rządowej: organy inne niż ww., tj. organy podporządkowane Prezesowi Rady Ministrów, bądź poszczególnym ministrom;

– urzędy obsługujące terenowe organy administracji rządowej: wojewodów, organy administracji zespolonej i niezespolonej;

– Rządowe Centrum Bezpieczeństwa.

Jednocześnie jest ona rekomendowana dla administracji samorządowej szczebla gminnego, powiatowego i wojewódzkiego oraz innych urzędów, w tym: Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu Rzeczypospolitej Polskiej, Kancelarii Senatu Rzeczypospolitej Polskiej, Biura Krajowej Rady Radiofonii i Telewizji, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Biura Krajowej Rady Sądownictwa, urzędów organów kontroli państwowej i ochrony prawa, Narodowego Banku Polskiego, urzędu Komisji Nadzoru Finansowego, państwowych osób prawnych i innych niż wymienione wyżej państwowe jednostki organizacyjne”[24].

Dokument, poza celem strategicznym, za jaki uważa się osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa, koncentruje się m.in. na: zwiększeniu poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa, zwiększeniu zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, zmniejszeniu skutków incydentów godzących w bezpieczeństwo teleinformatyczne, określeniu kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

Główne kierunki działań określone w *Polityce Ochrony Cyberprzestrzeni RP* wynikają z kolejności przedstawionych tam działań i obejmują:

– ocenę ryzyka związaną z funkcjonowaniem cyberprzestrzeni;

– zapewnienie odpowiedniego poziomu bezpieczeństwa portali administracji rządowej;

– przegląd obecnych rozwiązań legislacyjnych i przygotowanie rozwiązań zwiększających bezpieczeństwo użytkowników cyberprzestrzeni;

– uruchomienie oddzielnych projektów szczegółowych w celu optymalizacji CRP;

– powołanie przez Premiera zespołu przygotowującego rekomendacje dla właściwego ministra z zakresu wykonania lub koordynacji działań zapewniających bezpieczeństwo CRP;

[24] Ibidem, s. 9-10.

– zobowiązanie kierowników jednostek administracji rządowej do wprowadzenia systemu zarządzania bezpieczeństwem informacji;

– powołanie w ramach struktur jednostek administracji rządowej pełnomocników ds. bezpieczeństwa cyberprzestrzeni;

– wdrożenie działań edukacyjnych w zakresie szkolenia pełnomocników ds. bezpieczeństwa cyberprzestrzeni, kształcenia kadry urzędniczej administracji rządowej, prowadzenie kampanii edukacyjnych oraz wprowadzenia tematyki bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia na uczelniach wyższych.

Główne kierunki działań zapisane w projekcie posiadają charakter komplementarny, a ich realizacja powinna być prowadzona równolegle na kilku płaszczyznach. Biorąc pod uwagę dane z raportu przygotowanego przez Dynamics Markets Limited UK, według których aż 17% dorosłych Polaków padło ofiarą kradzieży tożsamości, a średnia strata z tytułu skradzionych danych wyniosła w Polsce 35 tys. zł[25], uzasadnione jest, by prace nad wdrażaniem programu, istniejącego w różnych wersjach już od 2009 r., znacząco przyspieszyły.

Podsumowanie

Specyfika sieci opartej na przeciwstawnych czynnikach dostępności i zabezpieczenia stanowi jedno z najpoważniejszych wyzwań związanych z zapewnieniem bezpieczeństwa, z jakim przyszło się aktualnie zetknąć uczestnikom stosunków międzynarodowych. Jeśli przyjąć, że bezpieczeństwo stanowi fundamentalną treść każdego państwa, to nowy wymiar państwowości, który buduje się wraz z kolejnymi warstwami sieci, staje się przestrzenią wymagającą przynajmniej minimum działań zapewniających ochronę jej użytkownikom.

Prace nad bezpieczeństwem w cyberprzestrzeni na gruncie europejskim trwają. W ciągu ostatniej dekady ich tempo znacząco wzrosło po to, by jak najszybciej uzupełnić lukę prawną, powstałą na skutek nagłego rozprzestrzeniania się nowoczesnych technologii komunikacyjnych. W wyniku tego liczba generowanych obecnie rozwiązań prawnych, choć duża, nie przekłada się w pełni na poziom bezpieczeństwa w sieci. Dokumenty formułowane przez organy międzynarodowe – mimo coraz większej szczegółowości – pozostawiają przestrzeń do podejmowania decyzji przez ustawodawstwa krajowe.

[25] Agencja Informacyjna NEWSERIA, *Polak średnio po roku dowiaduje się, że padł ofiarą kradzieży danych osobowych*, http://www.newseria.pl/news/polak_sredni o_po_roku,p618488561?nws=791196194&mws=bWdvbmlzemV3c2tpQGdiLnBs 7.12.2012 r.

W warunkach polskich brak optymalnej ochrony przed zagrożeniami w Internecie uwypukliła publikacja kolejnej wersji dokumentu *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*. Przyjęcie błędnego założenia wyjściowego, ograniczającego cyberprzestrzeń do granic terytorium kraju doprowadziło w rezultacie do zmniejszenia ochrony przez zawężenie samej definicji bezpieczeństwa. Z pola zainteresowań ustawodawcy zniknęły istotne z punktu widzenia interesów państwa i obywateli systemy zarządzane przez właścicieli prywatnych, wpływające na prawidłowe funkcjonowanie sektora bankowego, finansów czy energetyki. Brak ogólnej i systemowej analizy rodzaju zagrożeń, wskazania podmiotów odpowiedzialnych za realizację zadań oraz jasno sprecyzowanego czasu na realizację wytycznych zawartych w dokumencie powodują, że zdolność do skutecznej obrony pozostaje ograniczona.

Summary

In the last decade there has been a sudden and rapid development of the Internet. Together with its improvement, the issue of network security has become an important topic of a discussion over the international security mechanisms. The Internet, nowadays considered as space unrestricted by time or distance, has become an ideal place for new, previously unknown offenses and misdemeanours. *Ipso facto*, network is now an area that requires measures to ensure safety of its users. Although a cybercrime is currently a subject of the work on complementary legal solutions on both national and international levels, we can wonder if thanks to them the Internet will become a safe place one day.

Nota o autorze

Mateusz Karatysz [mateuszkaratysz@onet.eu] – doktorant w Zakładzie Marketingu Politycznego i Socjotechniki WNPiD UAM. Zainteresowania badawcze koncentruje w obrębie technik perswazyjnych w komunikacji wizualnej.