Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu

Michał Grzelak, Krzysztof Liedel

Ochrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa. Państwa, organizacje międzynarodowe i inni aktorzy niepaństwowi zrozumieli, że stabilność funkcjonowania i rozwój globalnego społeczeństwa informacyjnego jest uzależniony od otwartej, niezawodnej i – przede wszystkim – bezpiecznej cyberprzestrzeni. Podnoszenie świadomości w tym zakresie idzie w parze z gwałtownym wzrostem liczby incydentów komputerowych i nowych rodzajów zagrożeń. Polska również jest obiektem ataków cybernetycznych. Podobnie jak inne państwa stoi przed wyzwaniem, jakim jest wypracowanie zmian prawnych i organizacyjnych, pozwalających na zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli.

Historia internetu – ogólnoświatowej sieci komputerowej, pozbawionej wyróżnionego centralnego punktu – rozpoczęła się na przełomie lat 60. i 70. XX w. w Stanach Zjednoczonych. W latach 90. ubiegłego wieku nastąpiła gwałtowna komercjalizacja i rozwój tego środowiska. Powstały nowe usługi: strony internetowe, poczta elektroniczna, wyszukiwarki, komunikatory, strumieniowe przesyłanie multimediów, sieci społecznościowe, fora, blogi i wiele innych. Wraz z rozwojem fizycznej infrastruktury globalnej sieci ciągle rośnie liczba jej użytkowników. Szacuje się, że liczba internautów wyniosła w grudniu 2011 r. ponad 2,2 mld, czyli około 30 proc. ludzkiej populacji na świecie[1]. W Polsce za początek internetu uznaje się 1991 r., kiedy to nastąpiło pierwsze połączenie z zagranicą przez protokół TCP/IP[2]. Według szacunków, dostęp do internetu ma około 62 proc. mieszkańców kraju, czyli ponad 23 mln Polaków[3].

[1] *World Internet Usage and Population Statistics December 31, 2011*, http://www.internetworldstats.com/stats.htm (dostęp: 24 kwietnia 2012 r.).

[2] NASK Historia, http://www.nask.pl/run/n/Historia (dostęp: 18 czerwca 2012 r.).

[3] *Internet User Statistics & Population for 53 European Countries and Regions*, http://www.internetworldstats.com/stats4.htm (dostęp: 24 kwietnia 2012 r.).

Rozwojowi społeczeństwa informacyjnego, połączonemu z rozszerzaniem zasięgu internetu, towarzyszy przenikanie kolejnych aspektów ludzkiej działalności do cyberprzestrzeni. Ogólnoświatowy zasięg oraz możliwość natychmiastowego dostępu z niemal dowolnego miejsca na Ziemi, w połączeniu z niewielkimi kosztami użytkowania, sprawił, że coraz więcej podmiotów (rządów, instytucji i firm), a także indywidualnych osób decyduje się przenosić różne elementy swojej codziennej aktywności do cyberprzestrzeni. Wielu użytkowników internetu nie wyobraża sobie życia bez szybkiego dostępu do najświeższych informacji i poczty elektronicznej, internetowej bankowości, zakupów *online*, elektronicznej rezerwacji biletów czy kontaktu z rodziną i znajomymi przez portale społecznościowe oraz internetowe komunikatory. 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.

Niestety, w czasie gdy cyberprzestrzeń staje się wirtualnym odzwierciedleniem fizycznej rzeczywistości, przenikają do niej również negatywne formy ludzkiej działalności. Konstrukcja stworzonej z myślą o współpracy naukowej sieci internetowej daje duże poczucie anonimowości, wykorzystywana jest przez przestępców, terrorystów, a także niektóre państwa, do prowadzenia nielegalnej działalności lub agresji wobec innych podmiotów.

Jak wynika z raportu firmy Symantec[4], straty powstałe w wyniku działalności cyberprzestępców na świecie wyniosły w 2011 r. 388 mld dolarów, a 69 proc. dorosłych użytkowników internetu choć raz w swoim życiu było (44 proc. w 2011 r.) ofiarami przestępczości internetowej. W dużej mierze wynika to z faktu, że 41 proc. użytkowników nie posiada aktualnego oprogramowania zabezpieczającego systemy komputerowe. Użytkownicy padali najczęściej ofiarami wirusów i innego szkodliwego oprogramowania, oszustw internetowych oraz *phishingu* (wyłudzenia poufnych informacji). Motywacją do działania większości cyberprzestępców jest zazwyczaj chęć zysku, jednak wiele osób decyduje się łamać prawo również z innych pobudek. Przykładem są tu tzw. haktywiści, którzy w dążeniu do osiągnięcia celów ideowych dopuszczają się np. kradzieży i niszczenia wrażliwych danych bądź utrudniają do nich dostęp.

[4] *Symantec Cybercrime Report 2011*, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf (dostęp: 24 kwietnia 2012 r.).

Cyberprzestrzeń jest wykorzystywana również przez terrorystów jako narzędzie prowadzenia motywowanej politycznie działalności. Z uwagi na kontrowersje i problemy z jasnym zdefiniowaniem pojęcia cyberterroryzmu, trudno jednoznacznie zakwalifikować konkretne przykłady ataków jako efekt działalności terrorystów w cyberprzestrzeni. Wiele incydentów przypisywanych terrorystom może być formą wandalizmu, działaniem niejawnie sponsorowanym lub prowadzonym przy cichej akceptacji państwa, co jednak jest trudne do udowodnienia. Klasycznym przykładem są zmasowane cyberataki na infrastrukturę teleinformatyczną Estonii w 2007 r. Doprowadziły one do paraliżu państwa, blokując dostęp m.in. do systemu bankowego i sieci komórkowych. O przeprowadzenie ataków oskarżono Rosję, jednak nie udało się zebrać dowodów pozwalających stwierdzić, że władze tego kraju były za nie formalnie odpowiedzialne[5]. Z uwagi na duże koszty i potencjalne trudności zorganizowania skutecznego, spektakularnego cyberataku na dobrze zabezpieczone cele jest mało prawdopodobne, aby jakaś grupa terrorystyczna była w stanie podjąć działanie tego typu bez wsparcia ze strony władz państwowych[6]. Internet jest wykorzystywany przez terrorystów również jako narzędzie komunikacji. Używają oni globalnej sieci do koordynowania swoich działań, propagandy, dezinformacji, gromadzenia środków finansowych oraz werbowania członków. Ponadto za jej pośrednictwem udostępniane są materiały o charakterze typowo instruktażowym[7].

Jedną z podstawowych funkcji internetu jest uzyskiwanie informacji. Dlatego nie jest zaskoczeniem, że powszechnie stosowaną praktyką jest użycie cyberprzestrzeni do celów wywiadowczych. Jak napisano w raporcie opracowanym przez służby kontrwywiadowcze Stanów Zjednoczonych[8], wybrane państwa (raport wymienia m.in. Chiny i Rosję) na szeroką skalę wykorzystują cyberprzestrzeń do zbierania danych wywiadowczych, szczególnie danych gospodarczych dotyczących nowoczesnych technologii, przemysłu obronnego, farmaceutycznego itp. Z uwagi na niskie koszty i łatwość uniknięcia wykrycia, cyberszpiegostwo jest niezwykle efektywną

[5] *Estonia Has no Evidence of Kremlin Involvement in Cyber Attacks*, RIA Novosti, 6 września 2007 r., http://en.rian.ru/world/20070906/76959190.html (dostęp: 24 kwietnia 2012 r.).

[6] T. Rid, P. McBurney, *Cyber-Weapons,* The Royal United Services Institute, luty 2012 r., http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354 (dostęp: 24 kwietnia 2012 r.).

[7] Zob. więcej w: M. Adamczuk, *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, „Bezpieczeństwo Narodowe", nr 19, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 211–214.

[8] *Foreign Spies Stealing US Economic Secrets in Cyberspace*, październik 2011 r., http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20 maja 2012 r.).

formą prowadzenia działalności wywiadowczej. „Pozytywnym skutkiem" tej formy działań jest fakt, że tak długo jak internet będzie źródłem przydatnych informacji o konkurentach i przeciwnikach, jest mało prawdopodobne, aby któraś z globalnych potęg zdecydowała się na jego uszkodzenie lub zniszczenie.

Wiele mówi się także o działaniach militarnych w cyberprzestrzeni, nazywanej kolejnym po lądzie, morzu, przestrzeni powietrznej i przestrzeni kosmicznej środowiskiem prowadzenia walki[9]. Zarówno organizacje międzynarodowe, jak i państwa przyznają konieczność rozwijania zdolności obronnych w cyberprzestrzeni. Nie jest jednak tajemnicą, że niektóre kraje zdecydowały się również na rozwój zdolności ofensywnych – tworzą odpowiednie struktury w siłach zbrojnych i prowadzą badania nad nowymi rodzajami „cyberbroni", budując w ten sposób własne zasoby odstraszania potencjalnych adwersarzy. Poza specjalnie wydzielonymi jednostkami działającymi w strukturach sił zbrojnych wybrane państwa korzystają również z usług płatnych ekspertów, którzy jako najemnicy lub członkowie „cybermilicji" realizują ofensywne i defensywne zadania w cyberprzestrzeni[10]. Militaryzacja cyberprzestrzeni obejmuje również rozwój narzędzi służących walce w tym środowisku. Dotychczas wykorzystywano raczej „cywilne" środki, jednak podnoszenie zdolności obronnych doprowadziło do znacznego uodpornienia na konwencjonalne cyberataki i spowodowało wzrost nakładów na tworzenie „cyberbroni"[11] wykorzystywanych przez państwa do prowadzenia kierunkowych ataków[12]. W kwestii walki w cyberprzestrzeni jest jeszcze wiele niejasności, m.in. natury prawnej. Kolejne państwa tworzą strategie dotyczące obrony, a także otwarcie mówią o możliwości ofensywy lub ataków odwetowych w cyberprzestrzeni. W tym kontekście należy wspomnieć o amerykańskim projekcie „Olympic Games", którego celem, zgodnie z doniesieniami medialnymi, było powstrzymanie irańskiego programu

[9] *US Department of Defense Strategy for Operating in Cyberspace*, Departament Obrony USA, lipiec 2011 r., http://www.defense.gov/news/d20110714cyber.pdf (dostęp: 22 czerwca 2012 r.).

[10] *Chinese Military Mobilises Cybermilitias*, „The Financial Times", http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html (dostęp: 20 maja 2012 r.).

[11] Podobnie jak w przypadku innych pojęć dotyczących cyberbezpieczeństwa nie ma zgody co do jednolitej definicji cyberbroni. Odnosząc się do analogii konwencjonalnej broni, jako narzędzia użytego lub zaprojektowanego do użycia w celu wyrządzenia szkody (systemom, strukturom bądź istotom żywym), można przyjąć, że cyberbroń to kod komputerowy użyty lub zaprojektowany do użycia w celu wyrządzenia podobnych szkód. *Cyber-Weapons, op. cit.*

[12] *Pentagon Creating New-Generation Cyberweapon*, 20 marca 2012 r., http://rt.com/usa/news/cyberweapon-us-report-920/ (dostęp: 23 maja 2012 r.).

nuklearnego, m.in. za pomocą specjalnie opracowanego robaka Stuxnet[13]. Jest niemal pewne, że również inne rodzaje wykrytych w ostatnim czasie cyberbroni – programy Duqu i Flame – są owocem prac dobrze zorganizowanych i finansowanych zespołów specjalistów działających na zlecenie państwa (lub państw). Na tym polu wciąż nie doszło jednak do otwartej konfrontacji między krajami. Nie wiadomo, jak dokładnie mógłby wyglądać przebieg takiego konfliktu. Nie jest jasne, czy atak w cyberprzestrzeni pociągnie za sobą konwencjonalne, tzn. militarne działania odwetowe, a także, jak środowisko międzynarodowe zareaguje w takiej sytuacji. Wiele mówi się o współpracy i kolektywnej obronie. Kwestia obrony cyberprzestrzeni została ujęta w dwóch ostatnich deklaracjach przyjętych po szczytach NATO w 2010[14] i 2012 r.[15]. Trudno jednak przewidzieć, czy np. atak cybernetyczny na jednego z członków sojuszu faktycznie uruchomi wszystkie mechanizmy związane z art. 5 traktatu waszyngtońskiego i jaka będzie skala ewentualnych działań w tym zakresie.

Wyzwania i zagrożenia występujące w cyberprzestrzeni

Jedną z największych przeszkód stojących na drodze formalno-prawnego uregulowania kwestii bezpieczeństwa cyberprzestrzeni, zarówno na poziomie państwowym, jak i międzynarodowym, są trudności ze spójnym zdefiniowaniem terminów dotyczących tego zagadnienia. Problem stanowi nawet uzgodnienie definicji pojęcia samej cyberprzestrzeni. W jednej ze swoich publikacji Centrum Doskonalenia Cyberobrony NATO w estońskim Tallinie (NATO Cooperative Cyber Defence Centre of Excellence, CCDCoE) proponuje definicję mówiącą, że cyberprzestrzeń jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami"[16]. CCDCoE zwraca uwagę na mnogość funkcjonujących definicji, które często jednak opisują wyłącznie sprzętowe komponenty cy-

[13] *Obama Order Sped Up Wave of Cyberattacks Against Iran*, „The New York Times", 1 czerwca 2012 r., http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (dostęp: 6 czerwca 2012 r.).

[14] *Lisbon Summit Declaration*, 20 listopada 2010 r., http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease (dostęp: 22 czerwca 2012 r.).

[15] *Chicago Summit Declaration*, 20 maja 2012 r., http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease (dostęp: 23 maja 2012 r.).

[16] *Cyberspace: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf (dostęp: 20 maja 2012 r.).

berprzestrzeni (*hardware*) z ewentualnym uwzględnieniem oprogramowania (*software*), ignorując przy tym człowieka, jako użytkownika wchodzącego w interakcję z cyberprzestrzenią, stającego się w ten sposób jej częścią. Przykładem są definicje stosowane przez Departament Obrony USA oraz Komisję Europejską, krótko opisujące cyberprzestrzeń jako globalną sferę wymiany informacji.

Na brak jednolitej definicji cyberprzestrzeni zwraca uwagę także Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency, ENISA). W rekomendacjach zawartych w publikacji poświęconej przeglądowi narodowych strategii cyberbezpieczeństwa (*national cyber security strategy*, NCSS) przyjętych przez państwa Unii Europejskiej[17] (od 2008 r. NCSS przyjęło 10 państw UE; wśród nich nie ma Polski), ENISA podkreśla m.in. wagę międzynarodowej współpracy w zakresie cyberbezpieczeństwa. Zaleca uzgodnienie jednolitych definicji pojęć z zakresu bezpieczeństwa cyberprzestrzeni, wokół których kraje Unii będą tworzyły narodowe strategie, wspomagając w ten sposób utrzymanie bezpieczeństwa cyberprzestrzeni na globalnym poziomie.

Problem braku spójnych rozwiązań systemowych i prawnych ogranicza te państwa, instytucje oraz inne podmioty, których celem jest zapewnienie bezpiecznego działania globalnej sieci. Przestępcy, nieskrępowani ograniczeniami nakładanymi przez prawo, sprawnie wymyślają coraz to nowe formy wykorzystania cyberprzestrzeni do prowadzenia nielegalnej działalności. Ułatwia to dynamika zmian w tym środowisku, prowadząca do niekończącego się „wyścigu zbrojeń" między przestępcami a środowiskami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni.

Brak międzynarodowych regulacji stanowi problem nie tylko w obszarze cyberprzestępczości, ale też relacji między państwami. Działania programów takich jak Stuxnet, Duqu oraz Flame (i być może innych, jeszcze niewykrytych) pokazują, że rywalizacja państw w cyberprzestrzeni stała się faktem. Jest też bardzo prawdopodobne, że problem ten będzie narastał, co może doprowadzić do międzypaństwowego „wyścigu zbrojeń" w cyberprzestrzeni. Obecnie kwestia ta pozostaje prawnie nieuregulowana, co budzi uzasadniony niepokój. Pojawiają się głosy wzywające do ściślejszej współpracy państw w tym obszarze bezpieczeństwa. Eksperci nawołują do formalnego uregulowania

[17] *National Cyber Security Strategies*, European Network and Information Security Agency, maj 2012 r., http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport (dostęp: 23 maja 2012 r.).

zasad walki i konfliktów zbrojnych w cyberprzestrzeni[18], tak jak to uczyniono w odniesieniu do konwencjonalnych konfliktów, lub całkowitej demilitaryzacji cyberprzestrzeni (podobnie jak przestrzeni kosmicznej).

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- ataki z użyciem szkodliwego oprogramowania (*malware*, wirusy, robaki itp.);
- kradzieże tożsamości;
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych;
- blokowanie dostępu do usług (*mail bomb*, DoS oraz DDoS[19]);
- spam (niechciane lub niepotrzebne wiadomości elektroniczne);
- ataki socjotechniczne (np. *phishing*, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Coraz większym wyzwaniem stają się ataki typu APT (*advanced persistent threat*). Łączą one narzędzia różnego typu (socjotechniczne, programistyczne itp.). Przygotowania do ataku APT mogą trwać wiele tygodni, a nawet miesięcy. Przeprowadzają je zazwyczaj zorganizowane grupy dysponujące znacznymi budżetami oraz czasem pozwalającym na zinfiltrowanie konkretnego celu – firmy bądź instytucji – a następnie precyzyjnego przeprowadzenia ataku, którego celem może być kradzież wrażliwych danych lub uszkodzenie/zniszczenie systemu komputerowego. Przykładem APT jest użycie robaka Stuxnet, czego efektem było m.in. opóźnienie irańskiego programu nuklearnego[20]. Udowadnia to, że ataki tego typu mogą być wykorzystane w „słusznej sprawie", pomagając rozwiązać problemy, które do tej pory wymagały użycia konwencjonalnych sił i stanowiły zagrożenie dla życia ludzi.

Polska a zagrożenia w cyberprzestrzeni

Mimo że problem bezpieczeństwa sieci komputerowych i obiegu informacji pozostaje przedmiotem zainteresowania organów ochrony prawnej

[18] *Flame: UN Urges Co-operation to Prevent Global Cyberwar*, BBC News, 7 czerwca 2012 r., http://www.bbc.com/news/technology-18351995 (dostęp: 11 czerwca 2012 r.).

[19] Atak *denial of service* (DoS) oraz jego odmiana *distributed denial of service* (DDoS) polegają na blokowaniu dostępu do usługi przez zajęcie jej wszystkich wolnych zasobów (np. zalanie nadmiarową ilością danych lub zapytań), co prowadzi do przeciążenia i zawieszenia systemu.

[20] *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, „The New York Times", 15 stycznia 2011 r., http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all (dostęp: 23 maja 2012 r.).

już od kilku lat, to do niedawna w polskim ustawodawstwie brak było definicji przekładającej pojęcie przestrzeni wirtualnej – jako obszaru potencjalnych zagrożeń – na język prawny.

Nawet przepisy Kodeksu karnego, znowelizowanego w 2004 r. w celu wprowadzenia na grunt polskiego prawa zapisów Konwencji Rady Europy o cyberprzestępczości (tzw. budapeszteńskiej), podpisanej przez Polskę w 2001 r.[21], poza objęciem penalizacją przestępstw komputerowych oraz przestępstw godzących w bezpieczeństwo systemów informatycznych[22], nie zawierają w tej materii określeń definicyjnych.

Problem bezpieczeństwa w cyberprzestrzeni wychodzi przy tym poza ramy tradycyjnie pojmowanego czynu o charakterze przestępczym, w rozumieniu Kodeksu karnego. W skrajnych przypadkach może on bowiem przybrać postać, która w świetle konstytucji stanowi podstawę do wprowadzenia jednego ze stanów nadzwyczajnych.

27 września 2011 r. prezydent RP Bronisław Komorowski podpisał nowelizację ustawy o stanie wojennym[23]. Zmiany legislacyjne dotyczyły także ustaw o stanie wyjątkowym i o stanie klęski żywiołowej. Przygotowany w Biurze Bezpieczeństwa Narodowego projekt nowelizacji wprowadził do polskiego prawa pojęcie „cyberprzestrzeni". Przyjęta w ustawie definicja mówi, że cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". W tym brzmieniu definicja jest podobna do tej proponowanej przez CCDCoE, uwzględniając zarówno techniczny, jak i ludzki komponent cyberprzestrzeni.

Prezydencka inicjatywa w założeniu nie miała stanowić kompletnego rozwiązania dla problemów cyberbezpieczeństwa w Polsce, ale miała „zaszczepić" pojęcie cyberprzestrzeni w polskim systemie prawnym i stanowić

[21] *Convention on Cybercrime, CETS No.: 185*, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=29/05/2012&CL=ENG (dostęp: 29 maja 2012 r.).

[22] Po incydentach związanych z protestami przeciw podpisaniu przez Polskę dokumentu ACTA (omówione w dalszej części artykułu) wszczęto śledztwo, którego podstawą jest art. 269a. Kodeksu karnego stanowiący, że „kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5", http://www.tvn24.pl/1,1737163,druk.html (dostęp: 29 maja 2012 r.).

[23] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz.U. 2011 Nr 222, poz. 1323.

impuls do dalszych prac legislacyjnych. Wprowadzenie tej definicji stało się szczególnie ważne dla instytucji i organów odpowiadających za szeroko rozumiane bezpieczeństwo, umożliwiając stworzenie odpowiedniego instrumentarium kompetencyjnego, niezbędnego do wykonywania zadań przez te podmioty w zgodzie z konstytucyjną zasadą legalizmu. Przyjęte rozwiązania są zgodne z obowiązującą Koncepcją Strategiczną NATO i stanowią zarazem uzupełnienie do przygotowywanego przez Radę Ministrów Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016.

Opublikowany 17 kwietnia 2012 r. przez CERT Polska[24] raport roczny[25] za 2011 r. stanowi analizę zagrożeń w polskich sieciach komputerowych, opartą m.in. na przeszło 21 mln zgłoszeń incydentów pochodzących z systemów automatycznych, wykrytych w owym roku. Prezentując główne wnioski, raport CERT Polska zwraca uwagę m.in., że:

- w 2011 r. pojawiły się nowe źródła informacji, co przyczyniło się do poprawy wykrywalności incydentów komputerowych (wzrost o około 76 proc. w stosunku do 2010 r.);
- coraz powszechniejsze stają się ataki na telefony komórkowe (*smartphone*). Pojawił się m.in. nowy wariant popularnego trojana Zeus, który poza komputerami atakuje także telefony komórkowe;
- w dalszym ciągu celem ataków jest bankowość elektroniczna (systemy finansowe) i związane z nią poufne informacje;
- znaczna część incydentów obsłużonych nieautomatycznie w 2011 r. przez CERT Polska dotyczyła *phishingu* (wzrost o 1/3 w stosunku do 2010 r.);
- do zespołu CERT Polska dotarło w 2011 r. stosunkowo niewiele zgłoszeń dotyczących ataków DDoS. Wiąże się to jednak trudnością wykrycia tego typu ataków przez stronę trzecią oraz oporem poszkodowanych przed zgłaszaniem takich incydentów;

[24] CERT Polska jest zespołem reagowania na incydenty komputerowe działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), instytutu zajmującego się m.in. rejestracją domen .pl oraz działalnością naukową. Jest pierwszym tego typu zespołem w Polsce; działa od 1996 r. Do jego zadań należy m.in. wykrywanie i reagowanie na zdarzenia naruszające bezpieczeństwo sieci. Zespół pełni też funkcję koordynacyjną, przyjmując zgłoszenia od innych podmiotów zajmujących się bezpieczeństwem w internecie i przekazując je właściwym operatorom.

[25] *Raport CERT Polska 2011*, CERT Polska, http://www.cert.pl/PDF/Raport_CERT_Polska_2011.pdf (dostęp: 15 maja 2012 r.).

- przez przestępców coraz częściej wykorzystywane są serwisy internetowe oferujące darmowe *aliasy*, wykorzystywane w przypadkach *phishingu* w domenie .pl;
- zaobserwowano aż 5,5 mln botów[26]. Najczęściej występujący w polskich sieciach był bot Conficker (2,1 mln automatycznych zgłoszeń).

W 2011 r. zespół CERT Polska obsłużył 605 incydentów naruszających bezpieczeństwo teleinformatyczne, zgłoszonych przez różne podmioty. Najczęściej zgłaszanym typem incydentu były oszustwa komputerowe (o 1/3 więcej niż w 2010 r.). Na kolejnych pozycjach znalazły się incydenty dotyczące obraźliwych i nielegalnych treści, a także gromadzenia informacji oraz złośliwego oprogramowania. Zespół CERT Polska zwraca uwagę, że już po raz kolejny zanotowano mniejszą liczbę incydentów. Są one przy tym bardziej skomplikowane, a proces ich obsługi znacznie się wydłużył.

W raporcie kwartalnym[27] (styczeń–kwiecień 2012 r.) opublikowanym przez zespół CERT.GOV.PL[28] autorzy zwracają szczególną uwagę na działalność haktywistów, głównie w kontekście styczniowych ataków związanych z protestami przeciw dokumentowi ACTA. Ze wstępnej oceny zgromadzonego materiału wynika, że tylko około 7 proc. stron internetowych w domenie .gov.pl ma akceptowalny poziom bezpieczeństwa, a 18 proc. to strony cechujące się nieakceptowalnie niskim poziomem bezpieczeństwa. CERT.GOV.PL zauważa również, że coraz częściej występują nietypowe incydenty, niewykrywane przez standardowe systemy bezpieczeństwa. Zdaniem autorów, wiąże się to z globalną tendencją stosowania ataków w cyberprzestrzeni do nielegalnego zdobywania informacji z systemów należących do konkretnych instytucji.

Poza atakami typu DDoS w pierwszym kwartale 2012 r. zespół CERT.GOV.PL obsłużył incydenty dotyczące m.in.:

[26] Bot to pojedynczy element (komputer) tzw. botnetu – grupy komputerów zainfekowanych złośliwym oprogramowaniem, pozwalającym na zdalną kontrolę nad wszystkimi komputerami należącymi do botnetu. Boty mogą być wykorzystywane np. do rozsyłania spamu lub prowadzenia ataków DDoS.

[27] *Raport z działalności zespołu CERT.GOV.PL za I kwartał 2012*, CERT.GOV.PL, http://cert.gov.pl/download/3/136/Raport_CERT_GOV_PL_za_I_kwartal_2012.pdf (dostęp: 12 czerwca 2012 r.).

[28] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL został powołany 1 lutego 2008 r. Zadaniem zespołu jest ochrona jednostek organizacyjnych administracji publicznej RP przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków na systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska, spowodować poważne straty materialne albo zakłócić funkcjonowanie państwa.

- podmiany treści stron internetowych w domenach sdn.gov.pl, so.gov.pl, mil.pl, edu.pl, oip.pl (należących do schronisk dla nieletnich, sądów okręgowych, sił zbrojnych, okręgowych inspektoratów pracy i instytucji związanych z edukacją);
- ataków na usługi serwerowe Sejmu RP, których celem było przejęcie skrzynek e-mail;
- przesyłania zainfekowanych załączników użytkownikom poczty elektronicznej instytucji centralnej administracji publicznej;
- komputerów zombie należących do botnetu Kelihos.B.

W styczniu 2012 r. miała miejsce wspomniana wcześniej seria powiązanych incydentów dotyczących bezpieczeństwa systemów teleinformatycznych należących do polskich instytucji państwowych. Ataki, które trwały od 21 do 25 stycznia 2012 r., były formą haktywizmu – zorganizowanego w cyberprzestrzeni protestu przeciw podpisaniu przez władze Polski dokumentu ACTA (*Anti-Counterfeiting Trade Agreement*), mającego ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej. Był to element szerszej, globalnej kampanii przeciw zmianom prawnym, które – zdaniem protestujących – mogłyby ograniczać wolność słowa w internecie. W przypadku Polski punktem zapalnym był atak przeprowadzony przez profesjonalnych hakerów, polegający na zablokowaniu dostępu do stron internetowych (głównie ataków typu DDoS) należących do instytucji administracji publicznej. Następnie do akcji przyłączyli się tzw. *script kiddies* – niedoświadczeni użytkownicy, stosujący gotowe oprogramowanie i skrypty działania, dostarczone przez innych, bardziej zaawansowanych użytkowników. Zablokowano m.in. strony internetowe sejm.gov.pl, prezydent.gov.pl, premier.gov.pl, abw.gov.pl, cert.gov.pl, ms.gov.pl, msz.gov.pl, mkidn.gov.pl, bor.gov.pl, cbs.policja.pl, policja.pl, a także strony internetowe polityków i partii politycznych oraz portale informacyjne. Do koordynowania swoich działań, a także wymiany informacji o kolejnych celach oraz metodach ataków, wykorzystywano serwisy społecznościowe i fora internetowe. Z analiz przeprowadzonych przez zespół CERT.GOV.PL[29] wynika, że źródłem 81 proc. ataków były adresy IP komputerów znajdujących się na terenie Polski. Geolokalizacji adresów IP nie można jednak łączyć z faktycznym miejscem, z którego przeprowadzono atak, gdyż dla ukrycia swojej tożsamości atakujący mogli używać serwerów pośredniczących (*proxy*) lub komputerów,

[29] Wyciąg z ogólnej analizy ataków na witryny administracji państwowej RP w okresie 21–25 stycznia 2012 r., CERT.GOV.PL, http://cert.gov.pl/download/3/135/ANALIZA.pdf (dostęp: 21 maja 2012 r.).

nad którymi wcześniej przejęto kontrolę. Do blokowania stron przyczyniły się również próby wejścia na witryny przez zwykłych użytkowników internetu, którzy chcieli sprawdzić czy blokowane strony faktycznie nie działają.

Przebieg i skutki ataków wskazują na niewystarczające zabezpieczenia stron internetowych w domenie .gov.pl, które często są utrzymywane na serwerach zewnętrznych firm, niedostatecznie przygotowanych do odpierania zmasowanych ataków DDoS. Konieczne wydaje się więc wprowadzenie stosownych rozwiązań prawnych i organizacyjnych, wymuszających na jednostkach administracji publicznej działania w zakresie szeroko pojętego cyberbezpieczeństwa (nie tylko zabezpieczenia stron internetowych) oraz raportowania wykrytych incydentów.

Po incydentach ze stycznia 2012 r. powołany został zespół zadaniowy do spraw ochrony portali rządowych. Opracował on Wytyczne ministra administracji i cyfryzacji w zakresie ochrony portali informacyjnych administracji publicznej[30] zawierające rekomendacje mające na celu podniesienie poziomu bezpieczeństwa stron internetowych oraz poczty elektronicznej, należących do instytucji publicznych. Dotyczą one m.in. zapisów w umowach z zewnętrznymi dostawcami usług prowadzenia stron internetowych w zakresie zabezpieczeń witryn i reagowania na incydenty.

Propozycje zmian systemowych dla poprawy cyberbezpieczeństwa RP

Analizując omówione zagrożenia, łatwo dostrzec, że zasoby informacyjne i elementy infrastruktury teleinformatycznej Polski podlegają tym samym trendom, co cyberprzestrzeń na poziomie globalnym. Wraz z postępującą informatyzacją państwa, konieczne jest tworzenie skutecznych rozwiązań profilaktycznych, technicznych i organizacyjno-prawnych, pozwalających chronić jego obywateli. Troska i odpowiedzialność za utrzymanie bezpieczeństwa i rozwój cyberprzestrzeni nie mogą przy tym spoczywać wyłącznie na władzach, które część zobowiązań w tym zakresie powinny przenieść na barki społeczeństwa, sektora prywatnego i organizacji pozarządowych.

Do podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa cyberprzestrzeni w Polsce zalicza się Ministerstwo Spraw Wewnętrznych,

[30] Wytyczne Ministra Administracji i Cyfryzacji w zakresie ochrony portali informacyjnych administracji publicznej, http://cert.gov.pl/download.php?s=3&id=129 (dostęp: 23 maja 2012 r.).

Ministerstwo Administracji i Cyfryzacji, Ministerstwo Obrony Narodowej, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego oraz podmioty sektora prywatnego. Ich wspólnym celem powinno być:

- zabezpieczenie krytycznej infrastruktury teleinformatycznej państwa przed zagrożeniami płynącymi z cyberprzestrzeni;
- stworzenie na poziomie krajowym spójnej polityki bezpieczeństwa cyberprzestrzeni dla podmiotów sektora publicznego i prywatnego;
- stworzenie efektywnego systemu koordynacji umożliwiającego współpracę między podmiotami sektora publicznego i prywatnego w obszarze bezpieczeństwa cyberprzestrzeni;
- opanowywanie skutków incydentów komputerowych w celu minimalizowania ich kosztów;
- zwiększanie świadomości społecznej w zakresie bezpieczeństwa cyberprzestrzeni.

Aby osiągnąć te cele, konieczne jest podjęcie wielopoziomowych działań wymagających współpracy wszystkich zainteresowanych stron. Przede wszystkim należy zapewnić odpowiednie normy prawne, pozwalające na skuteczne działanie państwa i jego instytucji w zakresie bezpieczeństwa cyberprzestrzeni. Początkiem tego procesu była inicjatywa prezydenta RP, dotycząca wprowadzenia pojęcia „cyberprzestrzeni" do polskiego systemu prawnego. Konieczne jest także prawne uregulowanie zasad ochrony oraz ustalenie obszarów odpowiedzialności za ochronę „polskiej cyberprzestrzeni" i krytycznej infrastruktury teleinformatycznej. Ponieważ wybrane elementy infrastruktury teleinformatycznej państwa są własnością różnych jednostek administracji publicznej, konieczne jest przy tym zapewnienie spójnej polityki bezpieczeństwa tych elementów. Znaczna część krytycznej infrastruktury teleinformatycznej znajduje się jednak w rękach podmiotów prywatnych, wraz z którymi państwo powinno ustalić metody i zakres współpracy. Wypracowanie mechanizmów kooperacji w zakresie ochrony cyberprzestrzeni dotyczy również współdziałania polskiego państwa z innymi krajami, a także organizacjami międzynarodowymi.

Kolejnym obszarem wymagającym działania są kwestie techniczne. Zapewnienie bezpieczeństwa cyberprzestrzeni nie będzie możliwe bez rozbudowy systemów wczesnego ostrzegania przed atakami, wdrożenia dodatkowych rozwiązań prewencyjnych i szczególnej ochrony kluczowych systemów teleinformatycznych, połączonej z ćwiczeniami pozwalającymi ocenić odporność tej infrastruktury na ataki cybernetyczne. Należy również dążyć

do konsolidacji dostępu do usług publicznych oraz rozbudować Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL). Aby przeciwdziałać skutkom potencjalnych incydentów, konieczne jest opracowanie planu wykorzystania systemu powszechnej komunikacji w sytuacji kryzysowej oraz tworzenie zapasowych rozwiązań pozwalających na przejęcie zadań infrastruktury krytycznej w przypadku niedostępności podstawowych systemów.

Zapewnienie bezpieczeństwa cyberprzestrzeni nie będzie możliwe bez zaangażowania jak najszerszego grona użytkowników globalnej sieci, którzy świadomi niebezpieczeństw będą mogli przyczyniać się do ochrony tego środowiska. Konieczne jest ciągłe kształcenie specjalistów od bezpieczeństwa teleinformatycznego i kadry urzędniczej. Należy także racjonalizować programy kształcenia na uczelniach wyższych. Powinny temu towarzyszyć działania konsultacyjne i doradcze oraz współpraca z firmami sektora teleinformatycznego. Równolegle do wymienionych przedsięwzięć konieczne jest prowadzenie kampanii społecznej o charakterze edukacyjno-prewencyjnym, której celem będzie podnoszenie świadomości użytkowników w zakresie zagrożeń czyhających na nich w cyberprzestrzeni.

Podsumowanie

Cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa, co pociąga za sobą konieczność dokonania licznych zmian, zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa na świecie. W tym kontekście szczególnie istotne jest zrozumienie dynamiki zmian tego środowiska.

Budowa systemu prawnego, stanowiącego odpowiedź państwa na szanse i wyzwania związane z jego obecnością w cyberprzestrzeni, jest zadaniem niezwykle złożonym. Wynika to nie tylko z tempa zmian technologicznych, ale także ze szczególnego charakteru środowiska Web 2.0 i jego „interaktywnej" natury. Trendy w prawie międzynarodowym, występujące od zakończenia zimnej wojny, zmierzające do traktowania jednostki jako jednego z równoprawnych aktorów w stosunkach międzynarodowych, zyskują szczególne znaczenie w warunkach społeczeństwa Sieci. Małe, często trudne do zdefiniowania grupy – zarówno pod kątem tożsamości indywidualnych uczestników, jak i ich „zbiorowej" tożsamości – mogą stanowić

zagrożenie dla funkcjonowania nie tylko podmiotów pozapaństwowych, ale także samych państw.

Kształtując normy prawne na poziomie krajowym, przepisy regulujące współpracę międzynarodową oraz strategie i polityki bezpieczeństwa należy zatem uwzględniać te dwa podstawowe wyzwania. Konieczność z jednej strony szybkiego reagowania, a z drugiej – reagowania na zagrożenia ze strony małych, mobilnych grup stanowią nową jakość w obszarze formułowania przepisów regulujących funkcjonowanie państwa w sferze bezpieczeństwa.

Nie można zapominać, że choć zagrożenia w cyberprzestrzeni stanowią odmienną kategorię wyzwań legislacyjno-organizacyjnych, to problemy, które stwarzają, w znacznej mierze przypominają te, generowane przez inne zagrożenia asymetryczne, jak np. terroryzm. Ich wspólną cechą jest zmuszanie struktur państwowych do ewolucji w stronę rozwiązań mniej hierarchicznych, a bardziej elastycznych. Sieciowość, zarówno w wymiarze społecznym, jak i technologicznym, wraz z jej wszystkimi konsekwencjami, zdaje się stanowić jedno z najważniejszych pojęć nowego paradygmatu bezpieczeństwa na poziomie krajowym i międzynarodowym.