Miron Lakomy*

Polityka bezpieczeństwa teleinformatycznego Polski

Wprowadzenie

Jak słusznie zauważył Krzysztof Liedel, współcześnie jedna z podstawowych zmian w obszarze bezpieczeństwa jest związana ze wzrostem znaczenia płaszczyzny informacyjnej, kosztem płaszczyzny fizycznej[1]. Trudno nie zgodzić się z tym stwierdzeniem, obserwując niezwykle silny wpływ rewolucji informatycznej przełomu XX i XXI wieku na funkcjonowanie państw i społeczeństw. Z jednej strony, bezprecedensowy rozwój technologii informatycznych i związanych z nimi urządzeń sprawił, że diametralnie zmieniły one oblicze wielu obszarów ludzkiej działalności. Z drugiej — wiąże się z tym zjawiskiem rosnące uzależnienie od ich wykorzystania, a co za tym idzie, od ich niezawodności. Dynamiczny postęp technologiczny, obserwowany od drugiej połowy XX wieku, przyniósł jednak nieoczekiwane konsekwencje: nie tylko istotne korzyści, lecz także coraz wyraźniejsze zagrożenia[2].

Można wskazać wiele powodów tego stanu rzeczy. Przede wszystkim, przyczyną jest wyścig technologiczny, w wyniku którego na rynku często pojawiają się produkty niedopracowane, posiadające wady konstrukcyjne lub programowe. Po drugie, wiąże się to z otwartą architekturą sieci Inter-

* Doktor, adiunkt w Zakładzie Stosunków Międzynarodowych Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego.

[1] K. Liedel: *Bezpieczeństwo informacyjne państwa*. W: *Transsektorowe obszary bezpieczeństwa narodowego*. Red. K. Liedel. Warszawa 2011, s. 45.

[2] Zob. M. Madej: *Rewolucja informatyczna — istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*. W: *Bezpieczeństwo teleinformatyczne państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009.

net. W momencie powstania Internetu jego twórcy nie myśleli bowiem nad aspektami bezpieczeństwa teleinformatycznego. Wreszcie, wynika to także z rosnącego zainteresowania różnorodnych podmiotów potencjałem szeroko pojętej cyberprzestrzeni[3] jako środowiska realizacji partykularnych interesów. Infrastruktura teleinformatyczna i kierujące nią oprogramowanie mogą stać się instrumentem przestępców, dążących do osiągnięcia rozmaitych korzyści lub celów osobistych. Można także zauważyć, że od lat 80. XX wieku, coraz większą aktywność w tym obszarze wykazują także inni aktorzy: państwa, organizacje terrorystyczne czy grupy politycznie motywowanych hakerów. W tej perspektywie niezwykłe korzyści płynące z procesów komputeryzacji i informatyzacji wiążą się więc paradoksalnie z powstawaniem nowych zagrożeń dla bezpieczeństwa państw[4].

Początkowo, fenomen szkodliwego wykorzystania cyberprzestrzeni był postrzegany głównie przez pryzmat działalności przestępczej. Takie zjawiska jak haking czy haktywizm już w latach 80. i 90. XX wieku zwracały uwagę opinii publicznej[5]. W tym samym okresie pojawiły się pierwsze ostrzeżenia ze strony naukowców, wskazujących, że sieci teleinformatyczne mogą stanowić poważne zagrożenie również dla bezpieczeństwa państw. Początkowo tego typu głosy były lekceważone, a ryzyko zagrożenia traktowano jako sprawę odległej przyszłości. Czas przełomu tysiącleci szybko jednak potwierdził obawy. Tym samym rola cyberprzestrzeni jako nowego wymiaru bezpieczeństwa narodowego i międzynarodowego zaczęła dynamicznie rosnąć[6]. Było to szczególnie widoczne w przypadku Stanów Zjednoczonych, które stały się wówczas jednym z najpopularniejszych obiektów ataków teleinformatycznych, m.in. pochodzenia chińskiego i rosyjskiego. Tylko w ramach afery *Moonlight Maze*, z serwerów amerykańskich wykradziono informacje dotyczące m.in. systemów kierowania rakietami. Te oraz kolejne ataki na USA sprawiły, że w 2003 roku ogłoszono *The National Strategy to Secure Cyberspace*, w której zabezpieczenie cyberprzestrzeni określono

[3] Departament Obrony USA definiuje ją jako „globalną domenę w środowisku informacyjnym, składającą się ze współzależnych sieci infrastruktur teleinformatycznych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów". Zob. *DoD Dictionary of Military Terms*. Joint Staff, Joint Doctrine Division, J-7, Washington D.C., 17.10.2008.

[4] Szerzej: M. Madej: *Rewolucja informatyczna — istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*. W: *Bezpieczeństwo teleinformatyczne państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 17—40; P. Dawidziuk, B. Łącki, M.P. Stolarski: *Sieć Internet — znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*. W: *Bezpieczeństwo teleinformatyczne państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 41—62.

[5] Zob. T. Jordan: *Hakerstwo.* Przeł. T. Płudowski. Warszawa 2011.

[6] Zob. J.A. Lewis: *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies. Washington 2002.

mianem strategicznego wyzwania[7]. Przełomowym momentem w debacie na ten temat stały się jednak dopiero wydarzenia z 2007 roku. W kwietniu rosyjscy specjaliści, na tle sporu politycznego między Estonią a Federacją Rosyjską, dokonali bowiem pierwszego masowego ataku teleinformatycznego w historii przeciwko innemu państwu. Zablokowano wówczas nie tylko witryny internetowe instytucji publicznych, lecz także koncernów medialnych i banków. W rezultacie sparaliżowano wysoce rozwinięty system estońskiej bankowości internetowej[8]. Niedługo później cyberprzestrzeń została wrogo wykorzystana przez Izrael, który w ramach operacji *Orchard*, zainfekował wirusem komputerowym system obrony przeciwlotniczej Syrii. Rok później poważne ataki teleinformatyczne towarzyszyły również wojnie gruzińsko-rosyjskiej. W tym wypadku jednak ich efekty miały przede wszystkim wymiar propagandowy. Skutecznie ograniczono bowiem władzom w Tbilisi możliwość informowania opinii publicznej o stanowisku rządu podczas walk w Osetii Południowej[9]. W kolejnych latach potencjał sieci teleinformatycznych wykorzystano także m.in. do spowolnienia irańskiego programu atomowego (robak *Stuxnet*), ataków na Kirgistan czy Koreę Południową. We wszystkich tych przypadkach odwoływano się do nowej kategorii cyberwojny oraz związanych z nią dylematów dotyczących całej społeczności międzynarodowej[10]. Na tej podstawie należy zgodzić się z Radosławem Banią, według którego „w coraz większym stopniu cyberprzestrzeń staje się ważną areną, na którą przenoszone są różnego rodzaju starcia mające miejsce we współczesnych stosunkach międzynarodowych”[11].

Warto dodać, że w ciągu ostatnich dwudziestu lat doszło także do bezprecedensowego rozpowszechnienia się w Internecie działalności *stricte* kryminalnej. Cyberprzestrzeń na przełomie wieków stała się bowiem dogodnym obszarem nielegalnego osiągania szeroko pojętych korzyści osobistych. Szybko zdano sobie sprawę z faktu, że w dobie rewolucji technologicznej informacja ma coraz większą wartość. Szeroka gama technik i narzędzi, jakimi dysponuje współczesny cyberprzestępca sprawia, że celem ataków są

[7] Za: M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe — International Relations” 2010, nr 3—4, s. 59.

[8] S. Herzog: *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. “Journal of Strategic Security” 2011, nr 2.

[9] K. Saalbach: *Cyber War. Methods and Practice.* ver. 6.0, Universität Osnabrück, LV Internet Policy, 2.01.2013, s. 20; D.J. Smith, K. Mshvidobadze: *Russia, Georgia and the Shape of Cyber Wars to Come*. Cyber Defence Conference. Istanbul 16.05.2011.

[10] Zob. M. Lakomy: *Cyberwojna jako rzeczywistość XXI wieku*. „Stosunki Międzynarodowe — International Relations” 2011, nr 3—4, s. 141—162; K. Liedel, P. Piasecka: *Wojna cybernetyczna — wyzwanie XXI wieku*. „Bezpieczeństwo Narodowe” 2011, nr 1.

[11] R. Bania: *Wojny w cyberprzestrzeni — przypadek Iranu*. W: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Afryki Północnej (MENA) u progu XXI wieku*. Red. R. Bania, K. Zdulski. Łódź 2012, s. 197.

nie tylko pojedynczy użytkownicy i przedsiębiorstwa, lecz także instytucje państwowe, organizacje rządowe i pozarządowe oraz transnarodowe korporacje. Warto przytoczyć dane z *2012 Norton Cybercrime Report*, zgodnie z którymi roczne straty wynikające z tego procederu wynoszą ok. 110 mld USD. Co więcej, każdego dnia ofiarami cyberprzestępców pada ok. 1,5 mln użytkowników Internetu. Dane te świadczą najlepiej o skali współczesnych zagrożeń teleinformatycznych[12].

Nie ulega wątpliwości, że na początku drugiej dekady XXI wieku cyberprzestrzeń zaczęła odgrywać istotną rolę jako nowy wymiar bezpieczeństwa narodowego i międzynarodowego. W tym kontekście, warto zadać pytanie, w jaki sposób do tych zagrożeń podchodzi Rzeczpospolita Polska. Wydaje się, że jest to kwestia o fundamentalnym znaczeniu dla polskiej racji stanu. Sposób przeciwdziałania zagrożeniom pojawiającym się w przestrzeni teleinformatycznej warunkuje współcześnie nie tylko stan bezpieczeństwa państwa, lecz także rozwój gospodarczy, konkurencyjność technologiczną czy pozycję na arenie międzynarodowej.

Główne zagrożenia dla bezpieczeństwa teleinformatycznego państwa

Wydaje się, że na wstępie warto omówić specyfikę najpoważniejszych zagrożeń dla bezpieczeństwa teleinformatycznego Polski. Przede wszystkim, należy zwrócić uwagę na uwarunkowania funkcjonowania samej cyberprzestrzeni, która jest środowiskiem niematerialnym. Wynika z tego szereg wątpliwości co do interpretacji obowiązujących przepisów prawa międzynarodowego czy dotychczas raczej jasno zdefiniowanych kategorii, takich jak suwerenność czy integralność terytorialna. W sieci nie da się bowiem jednoznacznie wyznaczyć granic ani terytorium. Sytuację dodatkowo komplikuje fakt, że mimo swojej niematerialności, jak udowodniły chociażby wydarzenia w Iranie, atak teleinformatyczny może doprowadzić do zniszczeń fizycznych. Co za tym idzie, rodzi to oczywiste zagrożenia dla bezpieczeństwa państwa oraz stymuluje proceder motywowanych politycznie ataków komputerowych. Mimo wieloletniej dyskusji, tak w wymiarze politycznym, prawnym, jak i naukowym, nie do końca wiadomo, jak należy oceniać najpoważniejsze ataki teleinformatyczne i jak na nie reagować, odwołując się chociażby do zapisów Karty Narodów Zjednoczonych[13]. Dzięki swojej nie-

[12] *2012 Norton Cybercrime Report*. Symantec Annual Report, 5.09.2012.

[13] Zob. A. Bufalini: *Les cyber-guerres a la lumière des regles internationales sur l'interdiction du recours à la force*. In: *La gouvernance globale face aux défis de la sécurité collective.* Red. M. Arcari,

materialności oraz otwartej architekturze, sieci teleinformatyczne są również domeną działalności szerokiej gamy podmiotów, do której można zaliczyć m.in. hakerów, haktywistów, przestępców, organizacje terrorystyczne, korporacje, państwa czy organizacje międzynarodowe. Co więcej, jest to także przestrzeń, w której istnieje zasadnicza trudność ustalenia sprawcy ataków. Łatwa do osiągnięcia anonimowość stymuluje ofensywne wykorzystanie Internetu. Jednocześnie obrona przed włamaniami jest znacząco utrudniona, nie tylko przez brak systemu wczesnego ostrzegania czy konwencjonalnego wywiadu, lecz także na skutek wrażliwości systemów teleinformatycznych i wysokie koszty zabezpieczania ich. Wreszcie, warto zwrócić uwagę na aspekt informacyjny. Sieci teleinformatyczne mogą bowiem zostać także skutecznie zastosowane do działalności propagandowej, co udowodnił *casus* wojny gruzińskiej[14].

W literaturze specjalistycznej wyróżnia się kilka form najpoważniejszych zagrożeń dla bezpieczeństwa teleinformatycznego państw. Wymienia się m.in.: haking, haktywizm, cyberterroryzm, cyberszpiegostwo oraz militarne wykorzystanie cyberprzestrzeni. Haking można najogólniej ująć jako zjawisko obejmujące łamanie zabezpieczeń komputerowych oraz uzyskanie nieuprawnionego dostępu do danych w formie elektronicznej. Hakerzy nie posiadają jednak motywacji politycznych, przez co z reguły stanowią marginalne zagrożenie dla bezpieczeństwa narodowego[15]. Haktywizm z kolei można określić jako zastosowanie technik hakingu do ataków motywowanych politycznie. W tym wypadku celem haktywistów są spektakularne akcje, które jednak nie powinny zagrozić np. funkcjonowaniu infrastruktury krytycznej[16]. Zdecydowanie poważniejszą formą szkodliwego wykorzystania cyberprzestrzeni jest natomiast cyberterroryzm. Zdaniem Agnieszki Bógdał-Brzezińskiej i Marcina Floriana Gawryckiego, jest to „politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów". W szerszym rozumieniu, jest to także „wykorzystanie Internetu przez or-

L. Balmond. Napoli 2012; *Tallin Manual on the International Law Applicable to Cyber Warfare*. Ed. M.N. Schmitt. Cambridge 2013.

[14] Zob. F. Schreier: *On Cyberwarfare*. "DCAF Horizon 2015 Working Paper", vol. 7; M. Terlikowski: *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*. W: *Bezpieczeństwo teleinformatyczne państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009; A. Lupovici: *Cyber Warfare and Deterrence: Trends and Challenges in Research*. "Military and Strategic Affairs Journal" 2011, nr 3; T. Rid: *Cyber War Will Not Take Place*. "Journal of Strategic Studies" 2012, nr 1.

[15] M. Terlikowski: *Bezpieczeństwo teleinformatyczne państwa…*, s. 98—99. Szerzej: T. Jordan: *Hakerstwo*. Warszawa 2011.

[16] Zob. np. M.G. Milone: *Hacktivism: Securing the National Infrastructure*. "The Business Lawyer" 2002, no 1 (58), s. 385—386.

ganizacje terrorystyczne do komunikowania się, propagandy i dezinformacji"[17]. Cyberszpiegostwo z kolei polega na pozyskiwaniu niejawnych danych i informacji przy wykorzystaniu sieci teleinformatycznych. W ostatnich latach ta forma zagrożeń, szczególnie pochodzenia chińskiego, staje się coraz powszechniejsza. Wreszcie, zwraca się uwagę na fakt, że cyberprzestrzeń może być wykorzystywana jako piąty teatr działań zbrojnych, co udowodniła wspomniana już izraelska operacja *Orchard* przeciwko Syrii[18]. Do tego należy doliczyć nieco odmienną formę zagrożeń, jaką jest cyberprzestępczość. Jak słusznie jednak zauważył Marcin Terlikowski, przestępcy „nie mają zazwyczaj interesu w bezpośrednim uderzeniu w podmioty państwowe, gdyż mogłoby to zwrócić uwagę władz i w konsekwencji skutkować podjęciem wobec nich działań przez organy ścigania"[19]. Co za tym idzie, z reguły (choć nie zawsze) stanowią oni pośrednie zagrożenie dla bezpieczeństwa państw.

Uwarunkowania bezpieczeństwa teleinformatycznego Polski

Na tle wcześniejszych rozważań, warto podjąć próbę wskazania najistotniejszych czynników wpływających na wzrost cyberprzestrzennych zagrożeń dla bezpieczeństwa RP. Przede wszystkim, należy zwrócić uwagę na dynamicznie rozwijające się od początku lat 90. XX wieku procesy komputeryzacji i informatyzacji, łączące się z coraz powszechniejszym dostępem obywateli do Internetu. W połowie lat 90., liczba komputerów z dostępem do sieci wynosiła w Polsce jedynie ok. 50 tys.[20]. Pod koniec 2012 roku dostęp do Internetu w Polsce miało aż 17,1 mln osób. Tym samym, możliwość połączenia się z siecią dotyczyła 73% wszystkich gospodarstw domowych. Ten rewolucyjny wzrost jest jeszcze bardziej widoczny w przypadku sektora gospodarczego. Według Głównego Urzędu Statystycznego, w 2012 roku z komputerów korzystało aż 95% polskich przedsiębiorstw, a 93% miało dostęp do Internetu. Co więcej, aż 41% ich pracowników korzysta z sieci

[17] A. Bógdał-Brzezińska, M.F. Gawrycki: *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. Warszawa 2003, s. 73.

[18] Zob. *Cyber Espionage. The Harsh Reality of Advanced Security Threats*. Deloitte, Center for Security & Privacy Solutions, 2011; F. Schreier: *On Cyberwarfare*. "DCAF Horizon 2015 Working Paper", vol. 7.

[19] M. Terlikowski: *Bezpieczeństwo teleinformatyczne państwa…*, s. 96.

[20] Zob. *Rozwój Internetu w Polsce*. Zob. http://www.winter.pl/hosts.html [dostęp: 10.04. 2013].

i z urządzeń mobilnych[21]. Można zatem stwierdzić, że polskie społeczeństwo oraz gospodarka w bardzo dużym stopniu opierają się na wykorzystaniu komputerów i Internetu. Z jednej strony, rodzi to oczywiste korzyści, z drugiej jednak sprawia, że Polska jest coraz bardziej wrażliwa na ataki teleinformatyczne.

Po drugie, warto podkreślić znaczenie procesu informatyzacji infrastruktury krytycznej Rzeczpospolitej Polskiej na początku XXI wieku. Zgodnie z definicją zawartą w ustawie o zarządzaniu kryzysowym z 26 kwietnia 2007 roku, przez infrastrukturę krytyczną rozumie się m.in. systemy zaopatrywania w wodę, żywność, surowce energetyczne, energię, systemy łączności, finansowe, transportowe, ratownicze czy sieci teleinformatyczne. Są to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"[22]. Oczywiście, proces informatyzacji infrastruktury jest w zasadniczym stopniu stymulowany przez polskie władze. Już w 2005 roku, w „Strategii kierunkowej rozwoju informatyzacji Polski do roku 2013 oraz perspektywicznej prognozie transformacji społeczeństwa informacyjnego do roku 2020" stwierdzono, że: „o poziomie rozwoju i miejscu Polski w układzie międzynarodowym, zwłaszcza o pozycji Polski w Unii Europejskiej, w coraz większym stopniu będzie decydować skala dostępności informacji i znaczenie wiedzy. Zależeć będzie od tego konkurencyjność polskiej gospodarki, zarówno w wymiarze ekonomicznym, jak i politycznym". Do najważniejszych priorytetów zaliczono m.in. usieciowienie administracji publicznej, wdrożenie systemu identyfikacji obywatela *online* czy zwiększenie dostępu do publicznych i prywatnych usług elektronicznych. W dokumencie wspomniano więc o rozwoju takich usług, jak: *eGovernment*, *eLearning* czy *eTransport*[23]. Założenia strategii w dużej mierze podtrzymano w raporcie z 2009 roku „Polska 2030"[24]. Warto również zwrócić uwagę na „Program Zintegrowanej Informatyzacji Państwa", gdzie podkreślono potrzebę usieciowienia następujących dzie-

[21] *Społeczeństwo informacyjne w Polsce*. Główny Urząd Statystyczny, październik 2012, s. 1—2; M. Lemańska: *Spadła liczba internautów w Polsce*. Zob. http://www.ekonomia24.pl/artykul/963361.html [data publikacji: 20.12.2012; dostęp: 10.04.2013].

[22] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Dz.U. 2007, nr 89, poz. 590.

[23] Zob. Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020. Ministerstwo Nauki i Informatyzacji, 24.06.2005.

[24] Zob. *Polska 2030. Wyzwania rozwojowe*. Zespół Doradców Strategicznych Prezesa Rady Ministrów RP. Warszawa 2009.

dzin: wymiaru sprawiedliwości i sądownictwa, prowadzenia działalności gospodarczej, rolnictwa, obsługi celnej, ubezpieczeń społecznych, ochrony zdrowia, kultury i nauki czy bezpieczeństwa[25]. Należy podkreślić, że w ciągu ostatniej dekady dynamicznym procesom informatyzacji podlegały także inne systemy składające się na infrastrukturę krytyczną RP, w tym np. energetyka (inteligentne sieci elektroenergetyczne) czy system finansowy. O skali przemian w tym ostatnim przypadku może świadczyć fakt, że w 2012 roku z bankowości internetowej korzystało w Polsce aż 10,5 mln klientów indywidualnych[26]. Na tej podstawie można więc stwierdzić, że bez względu na wysokie korzyści wynikające z rewolucji informatycznej, wrażliwość Polski na ataki teleinformatyczne skierowane przeciwko infrastrukturze krytycznej w ostatnich latach zdecydowanie wzrosła. Tym samym kwestia odpowiedniego jej zabezpieczenia w cyberprzestrzeni zyskała fundamentalne znaczenie.

Po trzecie, bezpieczeństwo teleinformatyczne jest bez wątpienia uwarunkowane także sytuacją polityczną kraju, tak w aspekcie wewnętrznym, jak i międzynarodowym. Ważnym przykładem wpływu wewnętrznej sytuacji politycznej na bezpieczeństwo teleinformatyczne była sprawa podpisania umowy ACTA na początku 2012 roku. Decyzja rządu RP spotkała się wówczas z poważnymi protestami społecznymi, a w konsekwencji wywołała reakcję haktywistów. Wydaje się, że w przyszłości tego typu tendencje będą coraz bardziej widoczne[27]. Nie można natomiast zapominać, że najpoważniejsze dotychczas incydenty teleinformatyczne wiązały się z określonymi napięciami, kryzysami lub konfliktami w wymiarze międzynarodowym. Sytuacja Polski w tym względzie wiąże się więc z pewnymi zagrożeniami. Wynika to w pierwszej kolejności z udziału sił zbrojnych RP w misjach pokojowych na całym świecie, w tym przede wszystkim w operacji ISAF w Afganistanie. Sytuacja ta podwyższa ryzyko ataku cyberterrorystycznego, tym bardziej, że w ostatnich latach największe organizacje terrorystyczne coraz częściej wykorzystują przestrzeń teleinformatyczną. Po drugie, rośnie ryzyko ataków cyberszpiegowskich. Mogą mieć one charakter zarówno polityczny, wynikający ze standardowej działalności

[25] Program Zintegrowanej Informatyzacji Państwa. Ministerstwo Administracji i Cyfryzacji. Warszawa 2013.

[26] K. Billewicz: *Inteligentne sieci elektroenergetyczne — zagadnienia bezpieczeństwa cyfrowego*. „Nowe Technologie Energetyczne" 2012, nr 154—155; I. Chojnacki: *Informatyzacja energetyki za 7,5 mld zł*. „Dziennik Internautów". Zob. http://di.com.pl/news/29441,0,Informatyzacja_energetyki_za_75_mld_zl.html [data publikacji: 9.11.2009; dostęp: 17.04.2013]; *E-bankowość w Polsce. Popularność rośnie*. Zob. http://www.money.pl/gospodarka/wiadomosci/artykul/e-bankowosc;w;polsce;popularnosc;rosnie,13,0,1112845.html [data publikacji: 26.06.2012; dostęp: 17.04.2013].

[27] M. Płociński: *To nie był cyberterroryzm*. „Rzeczpospolita" 28.01.2012. Zob. http://www.rp.pl/artykul/799250.html [dostęp: 17.04.2013].

wywiadowczej, jak i gospodarczy, polegający np. na wykradaniu określonych technologii. Wreszcie, warto wziąć pod uwagę, że w najbliższym otoczeniu Polski znajduje się kraj słynący z ofensywnego wykorzystania przestrzeni teleinformatycznej. Z terytorium Federacji Rosyjskiej dokonywano szeregu poważnych cyberataków m.in. na Estonię, Gruzję, Kirgistan czy Stany Zjednoczone. Mając na uwadze niezmiennie trudne relacje dwustronne, można założyć znaczne prawdopodobieństwo wykorzystania przez Kreml przestrzeni teleinformatycznej jako instrumentu nacisku na polskie władze[28].

Po czwarte, charakteryzując najpoważniejsze uwarunkowania dla bezpieczeństwa teleinformatycznego Polski, należy wziąć pod uwagę proces coraz widoczniejszej militaryzacji Internetu — coraz więcej państw tworzy specjalne jednostki wojskowe, przygotowane do działania wyłącznie w środowisku teleinformatycznym. Tendencje te wynikają w dużej mierze z zauważonej już w latach 90. XX wieku przez RAND Corporation możliwości prowadzenia „strategicznej wojny w cyberprzestrzeni"[29]. W 2009 roku Stany Zjednoczone jako pierwsze utworzyły odrębne dowództwo sił zbrojnych dla przestrzeni teleinformatycznej — United States Cyber Command (USCYBERCOM). Działania w tym kierunku podjęły także Wielka Brytania oraz Francja[30]. W 2012 roku amerykańska korporacja Madiant opublikowała raport, który ujawnił istnienie chińskiej „cyber-jednostki" nr 61398 z siedzibą w Szanghaju, funkcjonującej w ramach sił zbrojnych Chińskiej Republiki Ludowej[31]. Wreszcie, warto pamiętać, że o przydatności cyberprzestrzeni jako piątego teatru wojny świadczyła, wspomniana już, izraelska operacja *Orchard* przeciwko Syrii w 2007 roku. Należy zatem zauważyć, że procesy te rodzą kolejne wyzwania dla bezpieczeństwa teleinformatycznego Rzeczpospolitej Polskiej. Sprawiają bowiem, że zagrożenia w cyberprzestrzeni mogą dotknąć nie tylko infrastruktury krytycznej, lecz także szeroko pojętego sys-

[28] Zob. M. Łapczyński: *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*. „Komentarz Międzynarodowy Pułaskiego" 3.05.2009; M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe — International Relations" 2010, nr 3—4, s. 66; P. Harris: *White House warns of cyber threat from 'aggressive' China and Russia*. "Guardian" 21.02.2013. Zob. http://www.guardian.co.uk/technology/2013/feb/21/white-house-cyber-threat-russia-china [dostęp: 17.04.2013].

[29] *Strategic War in… Cyberspace*. "Rand Research Brief" I 1996. Zob. również: A. Bautzmann: *Le cyberespace, nouveau champ de bataille?*. "Diplomatie. Affaires Stratégiques et Relations Internationales" I—II 2012, s. 80—81; A. Bufalini: *Les cyber-guerres a la lumière…*, s. 92.

[30] *Vers une cyber-armée française*. Zob. http://www.franceculture.fr/emission-le-choix-de-la-redaction-vers-une-cyber-armee-francaise%C2%A0-2013-01-29 [data publikacji: 29.01.2013; dostęp: 17.04.2013]; *UK beefs up cyber warfare plans*. Zob. http://www.bbc.co.uk/news/technology-13599916 [data publikacji: 31.05.2011; dostęp: 17.04.2013].

[31] Exposing One of China's Cyber Espionage Units. Mandiant Report 2012.

temu obronnego[32]. Tym samym, wymusza to dostosowanie polskiej armii do wymogów współczesnego pola walki.

Po piąte wreszcie, na wrażliwość polskiej cyberprzestrzeni na ataki wpływa również pat w międzynarodowej dyskusji na temat bezpieczeństwa teleinformatycznego. Mimo wieloletniej debaty w ramach Organizacji Narodów Zjednoczonych, nadal nie udało się bowiem osiągnąć porozumienia w sprawie międzynarodowego traktatu regulującego te kwestie. Co za tym idzie, Konwencja Rady Europy o Cyberprzestępczości, podpisana w Budapeszcie w 2001 roku, pozostaje jednym z nielicznych dokumentów w tej dziedzinie[33]. Z drugiej jednak strony, na początku XXI wieku problematyką cyberbezpieczeństwa zainteresowało się NATO oraz Unia Europejska. Obie organizacje zajęły się odmiennymi jego aspektami, wypracowując w ciągu kilku lat interesujące metody współpracy w zakresie zwalczania zagrożeń teleinformatycznych. Nie zaproponowano jednak skutecznych rozwiązań wielu wymienionych wcześniej dylematów natury politycznej, prawnej lub wojskowej. Przykładowo, członkowie Sojuszu Północnoatlantyckiego nadal nie wiedzą, w jaki sposób interpretować zapisy traktatu waszyngtońskiego, a w szczególności jego artykułu 5[34]. Można stwierdzić, że dynamika międzynarodowej debaty oraz kooperacji w zakresie cyberbezpieczeństwa wywiera zasadniczy wpływ na stan bezpieczeństwa teleinformatycznego RP.

Incydenty teleinformatyczne w Polsce

Analiza wskazanych uwarunkowań pozwala stwierdzić, że Polska jest w dużym stopniu narażona na ataki komputerowe, które mogą mieć poważne konsekwencje dla bezpieczeństwa narodowego. Warto więc omówić charakter i skutki najpoważniejszych dotychczas ataków teleinformatycznych przeciwko instytucjom RP. Przede wszystkim, należy mieć na uwadze, że znaczna część zagrożeń wiąże się z globalnym charakterem sieci. Jest to szczególnie widoczne na przykładzie proliferacji wirusów komputerowych. Już w latach 90. XX wieku, mimo niewielkiego stopnia komputeryzacji i in-

[32] Zgodnie z rozumieniem tego terminu zawartym w Strategii Obronności Rzeczpospolitej Polskiej z 2009 roku. Zob. Strategia Obronności Rzeczpospolitej Polskiej. Ministerstwo Obrony Narodowej. Warszawa 2009.

[33] Konwencja Rady Europy o Cyberprzestępczości. Rada Europy. Budapeszt 23.11.2001.

[34] J. Healey, L. van Bochoven: *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. "Atlantic Council Issue Brief" 27.02.2012; A. Bendiek: *European Cyber Security Policy*. "SWP Research Paper" 2012, RP 13.

formatyzacji, w Polsce rozprzestrzeniały się najbardziej niebezpieczne wersje szkodliwego oprogramowania, w tym np. *Michelangelo*, *Boza* czy *Marburg*. Podobna sytuacja zachodzi również współcześnie[35]. Nieco inaczej wygląda sprawa ataków teleinformatycznych. Należy bowiem zauważyć, że Polska nie była dotychczas priorytetowym celem włamań komputerowych. Pierwsze poważniejsze incydenty hakerskie odnotowano jeszcze w latach 90. XX wieku, lecz nie miały one bezpośredniego związku z funkcjonowaniem instytucji państwowych. Przełom nastąpił dopiero w drugiej połowie pierwszej dekady XXI wieku, po atakach na Estonię. Doszło wówczas do szeregu poważnych włamań do komputerów i sieci rządowych. Wśród nich można wymienić m.in.:

— włamanie na stronę internetową Dowództwa Operacyjnego Wojska Polskiego (III 2007);
— włamanie na strony internetowe Kancelarii Prezydenta RP oraz Ministerstwa Pracy i Polityki Społecznej (IV i VIII 2008);
— włamanie dokonane na stronę Ministerstwa Obrony Narodowej (I 2009)[36];
— udaremniony przez Agencję Bezpieczeństwa Wewnętrznego cyberatak na serwery instytucji państwowych, przeprowadzony prawdopodobnie z terytorium Rosji, w okresie wizyty Władimira Putina na Westerplatte oraz podjęcia uchwały przez Sejm RP dotyczącej 17 września oraz zbrodni katyńskiej (IX 2009);
— paraliż serwerów Ministerstwa Spraw Zagranicznych RP (IV 2010);
— włamanie na kilkaset stron internetowych prowadzonych przez polskie samorządy (IX 2011);
— seria udanych ataków haktywistów na witryny internetowe polskich instytucji rządowych. Włamano się m.in. na stronę Kancelarii Prezesa Rady Ministrów, Kancelarii Prezydenta, sejmu oraz Ministerstwa Obrony Narodowej (I 2012);
— włamanie do Centrum Usług Wspólnych przy Kancelarii Prezesa Rady Ministrów, przeprowadzone przez hakera ukrywającego się pod pseudonimem Alladyn2 (VII 2012);
— włamanie do systemu informatycznego Kancelarii Prezesa Rady Ministrów oraz prawdopodobnie również kilku ministerstw. Celem ataków były m.in. skrzynki e-mailowe części wysokich rangą urzędników pań-

[35] T. Grudziecki: *Cyberataki wczoraj, dziś i jutro*. CERT Polska/NASK. Zob. http://www.nask.pl/files/p/Cyberataki_wczoraj_dzis_i_jutro.pdf [dostęp: 17.04.2013].

[36] Za M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe — International Relations" 2010, nr 3—4, s. 66; *Stanęły serwery naszej armii*. Zob. http://wiadomosci.dziennik.pl/wydarzenia/artykuly/135711,stanely-serwery-naszej-armii.html [data publikacji: 14.01.2009; dostęp: 17.04.2013].

stwowych. Do włamania przyznał się polski haker o pseudonimie Alladyn2, motywując swoje działanie chęcią podniesienia poziomu zabezpieczeń urzędów RP (II—III 2013)[37];

Oprócz tego, zespoły CERT Polska i CERT.GOV.PL obsługują każdego roku setki innych incydentów teleinformatycznych. Przykładowo, na początku 2012 roku aktywność CERT Polska obejmowała obsługę m.in. podmiany treści stron internetowych w domenach sdn.gov.pl, mil.pl, edu.pl czy prób włamań na skrzynki e-mailowe Sejmu RP[38]. Natomiast zespół CERT.GOV.PL tylko w pierwszym kwartale 2012 roku zarejestrował aż 156 incydentów teleinformatycznych[39].

Warto dodać, że zdecydowanie częściej ataki wymierzane są w sektor prywatny. Stosunkowo często ich celem padają np. internetowe serwisy aukcyjne oraz banki. Znakiem tego typu aktywności była poważna awaria serwisów Allegro oraz mBanku na początku kwietnia 2013 roku. Według informacji medialnych, haker Inifinity, który wykorzystał metodę DDoS[40], został wynajęty za równowartość ok. 1000 zł[41]. Skalę szeroko pojętej cyberprzestępczości w Polsce ujawniły m.in. raporty CERT Polska oraz *Norton Cybercrime Report*. Według pierwszego z nich, w 2011 roku zespół otrzymał 21,2 mln zgłoszeń incydentów komputerowych. Oznaczało to wzrost o 75% w stosunku do roku 2010. Do najpopularniejszych form zagrożeń zaliczono: wykorzystanie sieci *botnet* (niemal 10 mln incydentów), skanowanie portów (5,7 mln), spam (4,68 mln), otwarte serwery DNS (0,58 mln) oraz złośliwe adresy internetowe (0,18 mln). Sam zespół obsłużył jedynie

[37] T. Pietryga: *Wrześniowy cyberatak na Polskę*. „Rzeczpospolita" 11.10.2009. Zob. http://prawo.rp.pl/artykul/375962.html [dostęp: 17.04.2013]; *Rosyjski cyberatak na Polskę. Jakie zdobyli informacje?*. Zob. http://wiadomosci.wp.pl/kat,38200,title,Rosyjski-cyberatak-na-Polske-Jakie-zdobyli-informacje,wid,14213018,wiadomosc.html [data publikacji: 31.01.2012; dostęp: 17.04.2013]; *Atak na portale samorządowe.* CERT Polska, http://www.cert.gov.pl/portal/cer/9/478/Atak_na_portale_samorzadowe.html [dostęp: 17.04.2013]; *Atak na strony rządowe w odwecie za ACTA?*. Zob. http://www.polskieradio.pl/5/3/Artykul/521918,Atak-na-strony-rzadowe-w-odwecie-za-ACTA [data publikacji: 22.01.2012; dostęp: 17.04.2013]; *Włamanie do sieci kancelarii premiera? Atakujący miał uzyskać dostęp do poczty pracowników KPRM.* Zob. http://niebezpiecznik.pl/post/wlamanie-do-sieci-kancelarii-premiera-atakujacy-mial-uzyskac-dostep-do-poczty-pracownikow-kprm/ [data publikacji: 6.03.2013; dostęp: 19.04.2013].

[38] Za K. Liedel, M. Grzelak: *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski — zarys problemu*. „Bezpieczeństwo Narodowe" 2012, nr 2, s. 135.

[39] Warto dodać, że zdaniem CERT.GOV.PL, jedynie ok. 7% portali rządowych ma wystarczający poziom zabezpieczeń teleinformatycznych. Zob. Raport kwartalny CERT.GOV.PL styczeń—marzec 2012. Warszawa 2012.

[40] Ang. *Distributed Denial of Service*.

[41] P. Rybicki: *Atak na Allegro i mBank to dzieło jednej osoby?*. Zob. http://www.hotmoney.pl/Atak-na-Allegro-i-mBank-to-dzielo-jednej-osoby-a30048 [data publikacji: 5.04.2013; dostęp: 19.04.2013].

605 najpoważniejszych incydentów[42]. Według raportu CERT Polska za rok 2012, odnotowano jedynie 10,59 mln zgłoszeń naruszeń bezpieczeństwa teleinformatycznego. Jak jednak zauważyli autorzy, „jedną z przyczyn mniejszej liczby zgłoszeń są zmiany w liczbie źródeł oraz rodzaju danych z nich pochodzących […]. Inną przyczyną jest zmiana sposobu zliczania niektórych zgłoszeń, pośrednio wynikająca także z faktu zmiany źródeł. Z powodów opisanych powyżej porównywanie liczb bezwzględnych pomiędzy kolejnymi latami nie jest miarodajne ani dla łącznej liczby zgłoszeń, ani dla poszczególnych kategorii". Po raz pierwszy od kilku lat wzrosła, aż o 80%, liczba najpoważniejszych incydentów obsługiwanych przez CERT Polska — do pułapu 1 082. W raporcie zawarto również ciekawe informacje na temat źródeł ataku. Najczęściej pochodziły one z terytorium Chin, Stanów Zjednoczonych, Zjednoczonych Emiratów Arabskich, Rosji, Niemiec oraz Indii[43]. Według *Norton Cybercrime Report*, codziennie ofiarą cyberprzestępców pada ok. 22 tys. Polaków. W 2011 roku straty z tego tytułu, w ocenie Symantec, wyniosły niemal 1 mld USD[44]. Przytoczone dane udowadniają, że zagrożenia dla bezpieczeństwa teleinformatycznego Polski w ostatnich latach dynamicznie się rozwijają. Na szczęście nie osiągnęły one jeszcze poziomu tych, z którymi muszą się mierzyć najbardziej rozwinięte kraje na świecie. Dla porównania, w 2011 roku tylko instytucje rządowe Stanów Zjednoczonych każdego miesiąca były atakowane w cyberprzestrzeni 1,8 mld razy[45]. Statystyki te uświadamiają, z jaką skalą zagrożeń mogą mieć do czynienia w przyszłości polskie służby, np. w przypadku kolejnego kryzysu politycznego na linii Warszawa—Moskwa.

Zagrożenia teleinformatyczne w dokumentach państwowych RP

Mając na uwadze dynamiczny wzrost cyberzagrożeń dla bezpieczeństwa RP w XXI wieku, warto zadać pytanie, w jaki sposób polskie władze odnoszą się do tych problemów? Na wstępie należałoby omówić podstawowe akty prawne w tej materii. Podstawą prawną walki z cyberprzestępczością w Polsce jest Ustawa z dnia 6 czerwca 1997 r. Kodeks karny. W KK znajduje się

[42] Raport CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011. CERT Polska — NASK. Warszawa 2012, s. 10—11.

[43] Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne. CERT Polska — NASK. Warszawa 2013, s. 6, 9, 58.

[44] Zob. *Norton Cybercrime Report.* Symantec 2011.

[45] S. Collins: *How to Make Internet More Secure*. "Politico" 7.03.2011.

14 podstawowych artykułów, które dotyczą tego procederu. Należy wymienić m.in.: art. 267 §1 o nieuprawnionym uzyskaniu informacji (hakingu), art. 267 §2 o podsłuchu komputerowym, czy art. 269 §1 i 2 o sabotażu komputerowym. Ustawami pomocniczymi są m.in.:

— Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych;
— Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego;
— Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
— Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych;
— Ustawia z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym;
— Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[46].

Nieco inaczej wygląda natomiast kwestia percepcji zagrożeń teleinformatycznych z perspektywy bezpieczeństwa narodowego. Po raz pierwszy kwestie te poruszono w większym stopniu w Strategii Bezpieczeństwa Narodowego RP z 2003 roku. Stwierdzono m.in.: „Zwalczanie zagrożeń dla rządowych systemów i sieci teleinformatycznych należy do kompetencji wyspecjalizowanych komórek cywilnych i wojskowych służb państwowych. Ich zadaniem jest zwalczanie przestępczości komputerowej wymierzonej w rządową i samorządową infrastrukturę telekomunikacyjną, w tym przeciwdziałanie atakom na jej elementy. Do zapewnienia należytej ochrony tej infrastruktury niezbędny jest rozwój i utrzymanie zdolności do zapobiegania wszelkim zakłóceniom, jakie mogą wystąpić w tej sferze, a także zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury teleinformatycznej”[47]. Stopień ogólności tych zapisów dowodził, że władze postrzegały wyzwania w cyberprzestrzeni jako problem o marginalnym znaczeniu dla bezpieczeństwa państwa. Świadczył o tym zresztą fakt, że problematykę tę zaliczono jedynie do wewnętrznych aspektów bezpieczeństwa.

Po raz drugi kwestie te, tym razem nieco szerzej, omówiono w Strategii Bezpieczeństwa Narodowego RP z 2007 roku. W podrozdziale pod

[46] Za: *Zwalczaj cyberprzestępczość*. Zob. http://www.policja.pl/portal/pol/1350/83643/Zwalczaj_cyberprzestepczosc.html [dostęp: 19.04.2013]. Zob. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny. Dz.U. Nr 88, poz. 553 z późn. zm.; Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.; Dz.U. Nr 43, poz. 296 z późn. zm.; Dz.U. z 2003 r. Nr 153, poz. 1503 z późn. zm.; Dz.U. Nr 128, poz. 1402, z późn. zm.; Dz.U. Nr 126, poz. 1068 z późn. zm.; Dz.U. Nr 144, poz. 1204 z późn. zm.

[47] Strategia Bezpieczeństwa Narodowego RP. Ministerstwo Spraw Zagranicznych RP. Warszawa 22.07.2003.

tytułem: „Bezpieczeństwo informacyjne i telekomunikacyjne", omówiono jednak tylko niektóre aspekty zagrożeń teleinformatycznych. Podkreślono co prawda znaczenie ochrony m.in. systemu bankowego czy telekomunikacyjnego, lecz bardzo mało miejsca poświęcono możliwości wykorzystania cyberprzestrzeni przez inne państwa bądź organizacje terrorystyczne. Z drugiej strony, należy pozytywnie ocenić zaakcentowanie znaczenia systemu łączności instytucji państwowych i wojska. Stwierdzono bowiem, że: „Krytycznym dla bezpieczeństwa państwa jest zapewnienie systemu łączności dla administracji rządowej, sił zbrojnych i innych kluczowych instytucji państwowych, opartego na najnowocześniejszych technologiach telekomunikacyjnych i najwyższych standardach bezpieczeństwa. Państwo polskie powinno jak najszybciej zbudować własny system łączności satelitarnej, wykorzystując w tym celu przyznane geostacjonarne pozycje orbitalne"[48].

Jak stwierdzono wcześniej, do zasadniczego przełomu w działaniach władz RP w dziedzinie bezpieczeństwa teleinformatycznego doszło dopiero w latach 2007—2008, w wyniku doświadczeń estońskich i gruzińskich[49]. W reakcji na te wydarzenia Agencja Bezpieczeństwa Wewnętrznego w 2008 roku podjęła się sprawdzenia stanu zabezpieczeń witryn internetowych instytucji państwowych. W tym samym roku, w maju, Departament Transformacji Ministerstwa Obrony Narodowej wydał dokument Wizja Sił Zbrojnych RP 2030, który częściowo dotyczył również bezpieczeństwa teleinformatycznego. Zawarto w nim niezwykle istotne stwierdzenie: „Systematycznie rosnący poziom uzależnienia społeczeństwa od systemów teleinformatycznych spowoduje, że realnym zagrożeniem dla bezpieczeństwa państwa stanie się cyberterroryzm. Jego istotą będzie atak i zniszczenie zasobów informacyjnych systemu obronnego państwa oraz zasadniczych elementów systemu informatycznego (infosfery) zarządzającego m.in. energetyką, gospodarką oraz finansami państwa. Wzrośnie również poziom zagrożeń dla bezpieczeństwa energetycznego Polski". Co ważne, zauważono, że cyberprzestrzeń staje się kolejnym teatrem działań zbrojnych. Stwierdzono bowiem, że cechuje ją rosnący potencjał w takich dziedzinach, jak: wsparcie działań bojowych, łączność, rozpoznanie, dowodzenie, transmisja danych czy kierowanie systemami uzbrojenia oraz walka psychologiczna. Rozróżniono przy tym przestrzeń cybernetyczną i sferę informacyjną. W tym kontekście zapowiedziano rozwój komponentu Sił Zbrojnych RP odpowiedzialnego za

[48] Strategia Bezpieczeństwa Narodowego RP. Biuro Bezpieczeństwa Narodowego RP. Warszawa 2007, s. 20—21.

[49] Zob. E. Licnocki: *Bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczpospolitej Polskiej w dobie zagrożeń cybernetycznych.* Centrum Symulacji i Komputerowych Gier Wojennych. Warszawa 2009.

działania w przestrzeni teleinformatycznej[50]. Omawiany dokument trafnie wyznaczał priorytety rozwoju polskiej polityki cyberbezpieczeństwa.

We wrześniu 2008 roku rozpoczęto natomiast prace nad pierwszym rządowym dokumentem w pełni poświęconym bezpieczeństwu teleinformatycznemu. Pierwszy projekt Rządowego programu ochrony cyberprzestrzeni RP na lata 2008—2011 trafił do konsultacji w listopadzie 2008 roku[51]. We wstępie zawarto szereg definicji niezbędnych do prawidłowego zrozumienia tego dokumentu. Cyberterroryzm określono jako: „terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym". Uznano go za kluczową i „stale rosnącą postać ataków terrorystycznych". Cyberprzestrzeń zdefiniowano natomiast jako: „przestrzeń komunikacyjną tworzoną przez systemy powiązań internetowych". W tym rozumieniu cyberprzestrzeń RP objęła, według autorów, „systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne"[52]. Należy przy tym zauważyć, że przyjęte definicje cyberprzestrzeni oraz cyberprzestrzeni RP posiadały poważne wady. Jak zauważył Krzysztof Liderman, obie, nie dość, że nie mogły być podstawą „sensownych działań technicznych", to nie były ze sobą spójne[53]. Tak rozumiana cyberprzestrzeń nie obejmowałaby bowiem m.in. odrębnych od Internetu sieci — tzw. intranetów. Cyberprzestrzeń RP utożsamiano także, co wydaje się błędne, z infrastrukturą krytyczną państwa. Co ważne, autorzy mieli jednak świadomość słabości tych definicji, bowiem w rozdziale 2: „Działania organizacyjno-prawne", uznano, że istnieje potrzeba „prawnego zdefiniowania pojęć dotyczących cyberprzestrzeni i cyberterroryzmu"[54].

W dokumencie wymieniono szereg priorytetowych zadań programu:

— zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa;

---

[50] Wizja Sił Zbrojnych RP 2030. Departament Transformacji Ministerstwa Obrony Narodowej, maj 2008, s. 10, 13—15.

[51] W konsultacjach: Rządowy program ochrony cyberprzestrzeni RP. Vagla.pl, 11.11.2008. Zob. http://prawo.vagla.pl/node/8211 [dostęp: 19.04.2013]; M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku.* „Stosunki Międzynarodowe — International Relations" 2010, nr 3—4, s. 67.

[52] Rządowy program ochrony cyberprzestrzeni RP na lata 2008—2011. Wersja 1.0, październik 2008, s. 3.

[53] K. Liderman: *Bezpieczeństwo informacyjne.* Warszawa 2012, s. 64.

[54] Rządowy program ochrony cyberprzestrzeni RP na lata 2008—2011…, s. 7.

— stworzenie i realizacja spójnej polityki dotyczącej bezpieczeństwa w cyberprzestrzeni;
— obniżenie skuteczności ataków cyberterrorystycznych;
— stworzenie systemu koordynacji i wymiany informacji między sektorem publicznym i prywatnym;
— zwiększenie kompetencji podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa odnośnie do bezpieczeństwa cyberprzestrzeni;
— zwiększenie świadomości użytkowników systemów elektronicznych i sieci teleinformatycznych w zakresie metod i środków bezpieczeństwa.

Dokument został zaadresowany do Ministerstwa Spraw Wewnętrznych i Administracji, Agencji Bezpieczeństwa Wewnętrznego, Ministerstwa Obrony Narodowej, Służby Kontrwywiadu Wojskowego, podmiotów prywatnych oraz innych organów administracji publicznej. Cele programu miały być realizowane na trzy sposoby. Przede wszystkim, dzięki „stworzeniu systemu koordynacji zwalczania, przeciwdziałania oraz reagowania na zagrożenia i ataki w cyberprzestrzeni państwa". Po drugie, przez wdrożenie na dużą skalę „mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń teleinformatycznych". Po trzecie wreszcie, dzięki edukacji społecznej i specjalistycznej w tym zakresie[55]. W tym kontekście warto zwrócić uwagę, że ta wstępna wersja przywołanego rządowego programu pominęła niestety szereg istotnych kwestii. Nadmiernie akcentując znaczenie cyberterroryzmu, potraktowała marginalnie kilka innych form zagrożeń teleinformatycznych, w tym np. cyberwojnę czy cyberszpiegostwo. Nie był to więc projekt kompletny i spójny pod względem przedstawionej wizji. Nie ulega jednak wątpliwości, że zestaw pomysłów i środków zawartych w programie i tak był niezwykle potrzebny. Zdecydowana większość zaproponowanych działań była niezbędna dla zabezpieczenia państwa przed szkodliwą działalnością w cyberprzestrzeni. Warto podkreślić szczególnie trzy sprawy. Po pierwsze, zauważono wreszcie fundamentalne znaczenie infrastruktury krytycznej. Po drugie, doceniono znaczenie współpracy międzynarodowej w tym zakresie. Dano tym samym wyraz zrozumienia, że problemy dotyczące bezpieczeństwa teleinformatycznego mają zasięg globalny. Wreszcie, zwrócono uwagę na istotne znaczenie działalności edukacyjnej i szkoleniowej. Ten kierunek działań udowadniał, że autorzy zdawali sobie sprawę z faktu, że nawet najlepsze systemy zabezpieczeń nie będą skuteczne, kiedy zawodzić będzie „czynnik ludzki".

Twórczym rozwinięciem tego dokumentu był Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011—2016, którego projekt został przygotowany w czerwcu 2010 roku. Już we wstępie trafnie

[55] Ibidem, s. 3—5.

stwierdzono, że: „W obliczu globalizacji, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa […]. Obecnie w cyberprzestrzeni granica między pokojem a wojną staje się coraz bardziej umowna […]. W dodatku obiektem cyberwojny są elementy infrastruktury cywilnej. Należy w związku z tym dopracować mechanizmy komunikacji w obszarze cywilnym, uregulować prawnie, wprowadzając dotkliwe sankcje karne za ich łamanie — z jednej strony — a z drugiej intuicyjnie istnieje konieczność ustanowienia kanałów wymiany informacji w obie strony. Uważa się, iż w przypadku cyberataku, zaatakowane zostaną zarówno struktury wojskowe, jak i cywilne, które powinny mieć zdolność współpracy, która bez sprawnych kanałów wymiany informacji skaże Państwo na porażkę". Co ważne, program nie obejmował sieci niejawnych, które posiadają odrębne mechanizmy obronne oraz regulacje prawne. Wydaje się, że jednym z najistotniejszych elementów tego dokumentu był punkt 1.1 zawierający definicje stosowanych terminów. Cyberprzestrzeń uznano za „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Cyberprzestępstwem nazwano czyn zabroniony, „popełniony w obszarze cyberprzestrzeni". Cyberterroryzm to „cyberprzestępstwo o charakterze terrorystycznym". Cyberatak natomiast to „celowe zakłócanie prawidłowego funkcjonowania cyberprzestrzeni, bez konieczności angażowania personelu lub innych użytkowników. Umożliwia ominięcie lub osłabienie sprzętowych i programowych mechanizmów kontroli dostępu". Wreszcie, krytyczną infrastrukturę informatyczną zdefiniowano jako „infrastrukturę krytyczną wyodrębnioną w systemie łączności i sieciach teleinformatycznych", na podstawie art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym. Za cel strategiczny program uznał stworzenie podstawowych ram instytucjonalno-prawnych oraz systemu koordynacji i wymiany informacji między administracją publiczną a innymi podmiotami i użytkownikami cyberprzestrzeni Polski. Do celów szczegółowych zaliczono natomiast:

— zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym infrastruktury krytycznej RP;
— minimalizację skutków incydentów komputerowych;
— zdefiniowanie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo RP;
— stworzenie i realizację spójnego systemu zarządzania cyberbezpieczeństwem dla podmiotów administracji publicznej;
— stworzenie systemu koordynacji i wymiany informacji między podmiotami czuwającymi nad bezpieczeństwem teleinformatycznym RP;
— zwiększenie świadomości użytkowników w zakresie zagrożeń teleinformatycznych i sposobów przeciwdziałania im.

Działania te miały zostać zrealizowane za pomocą szerokiej gamy środków, wśród których wymieniono m.in. ustalenie hierarchii priorytetów, w tym działania legislacyjne polegające na przeglądzie istniejących przepisów i ich aktualizacji. Co więcej, postulowano wprowadzenie programów ochrony, obejmujących np. precyzyjne zdefiniowanie pojęć z zakresu bezpieczeństwa teleinformatycznego, podział obowiązków w zakresie ochrony cyberprzestrzeni RP pomiędzy poszczególne instytucje czy powołanie Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP. Bardzo duży nacisk położono na edukację i szkolenia, tak dzieci i młodzieży, jak i urzędników państwowych. Podkreślono także znaczenie badań naukowych oraz racjonalizacji programów kształcenia w tej dziedzinie. Wreszcie, warto zauważyć, że w dokumencie wymieniono bardzo liczną grupę organów państwowych odpowiedzialnych za realizację programu. Zaliczono do nich m.in.: Prezesa Rady Ministrów, Ministra Edukacji Narodowej, Ministra Nauki i Szkolnictwa Wyższego, Ministra Obrony Narodowej, Ministra Spraw Wewnętrznych i Administracji, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Służby Kontrwywiadu Wojskowego, Dyrektora Rządowego Centrum Bezpieczeństwa, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Państwowej Straży Pożarnej. Natomiast za instytucję odpowiedzialną za ochronę cyberprzestrzeni RP uznano Prezesa Rady Ministrów, który miał wykonywać swoje obowiązki przez: Ministra Spraw Wewnętrznych i Administracji, Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego oraz Szefa Służby Kontrwywiadu Wojskowego[56]. W tym kontekście, należy stwierdzić, że w programie, z jednej strony, niestety pozostała część błędów z wcześniejszej wersji — szczególnie w kwestii przyjętych definicji niektórych pojęć bądź pominięcia szeregu istotnych zagrożeń teleinformatycznych. Z drugiej strony, nie ulega jednak wątpliwości, że projekt był niezwykle potrzebny. Zawierał bowiem bogaty zbiór środków i rozwiązań, które są niezbędne dla zabezpieczenia krytycznej infrastruktury teleinformatycznej RP.

Mimo wysokiego stadium zaawansowania prac, dokument ten niestety nie wszedł w życie. Jak informowała „Rzeczpospolita" w styczniu 2012 roku, prace zatrzymały się bowiem na etapie konsultacji międzyresortowych, a nowe propozycje MSWiA z 2011 roku nie zostały uwzględnione. Ten stan rzeczy potwierdził Biuletyn Informacji Publicznej Ministerstwa Spraw Wewnętrznych RP, w którym Rządowy program ochrony cyberprzestrzeni RP na lata 2011—2016 nadal posiada status skierowanego do uzgodnień

[56] Za: Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011—2016. Departament Ewidencji Państwowych i Teleinformatyki MSWiA, wersja 1.1, Warszawa, czerwiec 2010.

międzyresortowych[57]. W dużej mierze wynikało to z faktu, że kompetencje w zakresie polityki bezpieczeństwa teleinformatycznego przejęło Ministerstwo Administracji i Cyfryzacji, utworzone w listopadzie 2011 roku.

Bardzo ważnym efektem prac MAiC oraz Agencji Bezpieczeństwa Wewnętrznego był projekt Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, opublikowany i przesłany do konsultacji resortowych we wrześniu 2012 roku. W jego zmodyfikowanej wersji zawarto wiele niezwykle cennych rozwiązań z zakresu bezpieczeństwa teleinformatycznego RP. Bazując w dużej mierze na omówionych wcześniej projektach Rządowego programu ochrony cyberprzestrzeni RP, nowy dokument z pewnością ujął zagadnienia bardziej przejrzyście i usystematyzował. Przede wszystkim, poszerzono, w porównaniu z RPOC, zakres celów polityki cyberbezpieczeństwa o: zwiększenie zdolności do zwalczania i zapobiegania zagrożeniom teleinformatycznym, przy czym na zmianę stosowano zwroty „bezpieczeństwo teleinformatyczne" i „bezpieczeństwo cyberprzestrzeni", co mogło być dość mylące. W odróżnieniu od wcześniejszych projektów, stwierdzono jednoznacznie, że podmiotem odpowiedzialnym za koordynację tej polityki jest Ministerstwo Administracji i Cyfryzacji („minister właściwy ds. informatyzacji"). Bardziej kompleksowo autorzy podeszli również do kwestii działań podejmowanych w ramach POCRP. W ich obrębie wymieniono m.in.:

— szacowanie ryzyka związanego z funkcjonowaniem cyberprzestrzeni, za co odpowiedzialny ma być Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL);
— zapewnienie bezpieczeństwa portali administracji rządowej, pozostające również w gestii CERT.GOV.PL;
— inicjowanie przez MAiC działań legislacyjnych, pozwalających na realizację Polityki Ochrony Cyberprzestrzeni RP;
— działania proceduralno-organizacyjne, obejmujące m.in. wdrożenie mechanizmów zarządzania bezpieczeństwem cyberprzestrzeni RP — wprowadzono przy tym jasny podział na organy odpowiedzialne za bezpieczeństwo sieci cywilnych i administracji publicznej (CERT.GOV.PL) i wojskowych (Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych);
— działania w zakresie kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa teleinformatycznego, obejmujące m.in. szkolenia pełnomocników ds. bezpieczeństwa cyberprzestrzeni, kampanie społeczne czy kształcenie na poziomie studiów wyższych;

[57] W. Wybranowski: *Cyberochrona Polski padła*. „Rzeczpospolita" 24.01.2012. Zob. http://www.rp.pl/artykul/797348.html?print=tak&p=0 [dostęp: 26.04.2013]; Rządowy program ochrony cyberprzestrzeni RP na lata 2011—2016. Biuletyn Informacji Publicznej Ministerstwa Spraw Wewnętrznych. Zob. http://bip.msw.gov.pl/portal/bip/6/19057/Rzadowy_Program_Ochrony_Cyberprzestrzeni_RP_na_lata_20112016.html [dostęp: 26.04.2013].

— działania techniczne obejmujące prace badawcze, rozbudowę zespołów CERT, rozbudowę systemu wczesnego ostrzegania czy testowanie stanu zabezpieczeń teleinformatycznych.

Realizacji mają służyć m.in.: powołanie Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP, wprowadzenie mechanizmów wymiany informacji, współpraca z sektorem prywatnym oraz współpraca międzynarodowa[58]. Dokument ten można oceniać z dwóch perspektyw. Z jednej strony, jest on niezbędny dla zapewnienia bezpieczeństwa teleinformatycznego RP. Rosnąca skala wyzwań w cyberprzestrzeni sprawia, że stworzenie spójnego systemu reagowania na incydenty komputerowe ma dla państwa strategiczne znaczenie. W tym kontekście należy pozytywnie ocenić zdecydowaną większość proponowanych rozwiązań. Z drugiej strony, warto zwrócić uwagę na trzy wątpliwości. Po pierwsze, POCRP w dużej mierze powtórzyła aparat pojęciowy zawarty we wcześniejszych projektach RPOC. Jak wskazano, część stosowanych pojęć, w tym np. pojęcie cyberterroryzmu, została sformułowana mało precyzyjnie, co może być niekorzystne dla skuteczności dokumentu. Po drugie, dość ogólnikowo potraktowano zagadnienie kosztów wdrożenia projektu. Jest to dość problematyczne, ponieważ, jak wskazują doświadczenia państw zachodnich, zabezpieczenie krytycznej infrastruktury teleinformatycznej wiąże się z reguły ze znacznymi nakładami finansowymi. Po trzecie wreszcie, POCRP cechowało zbyt niskie tempo prac koncepcyjnych w tej dziedzinie — dokument przyjęto dopiero w czerwcu 2013 roku, czyli sześć lat po tzw. pierwszej cyberwojnie.

Obok strategii ochrony cyberprzestrzeni, w ostatnich latach instytucje państwowe RP przygotowały wiele innych dokumentów, obejmujących tematykę bezpieczeństwa teleinformatycznego. Przede wszystkim, część zagrożeń na tym obszarze omówiono w Strategicznym Przeglądzie Bezpieczeństwa Narodowego z 2012 roku. W rozdziale pierwszym pod tytułem „Diagnoza Polski jako podmiotu bezpieczeństwa. Interesy narodowe i cele" zauważono, że RP stoi przed szeregiem istotnych wyzwań, jeśli chodzi o potencjał ochronny. Zaliczono do nich m.in. cyberterroryzm. Również w rozdziale drugim: „Ocena i prognoza środowiska bezpieczeństwa. Scenariusze kształtowania się warunków bezpieczeństwa", autorzy dostrzegli proces przenoszenia się zjawiska terroryzmu w wymiar cyberprzestrzenny[59]. Sugestie SPBN zostały później rozwinięte w opracowaniach m.in. Departamentu Zwierzchnictwa nad Siłami Zbrojnymi, Departamentu Prawa i Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego oraz, co najważniejsze, w Białej Księdze Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej. W pierw-

[58] Zob. Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej. Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, czerwiec 2013.

[59] Strategiczny Przegląd Bezpieczeństwa Narodowego. Główne wnioski i rekomendacje. Biuro Bezpieczeństwa Narodowego. Warszawa 2012.

szym z nich: „Aspekty bezpieczeństwa militarnego w ujęciu Strategicznego Przeglądu Bezpieczeństwa Narodowego" zauważono m.in. rosnącą podatność informatycznych systemów państwowych na zagrożenia cybernetyczne. Słusznie dostrzeżono także proces zmniejszającej się wagi klasycznych zagrożeń militarnych na rzecz wyzwań asymetrycznych i cybernetycznych. Podkreślono przy tym znaczenie informatyzacji systemów walki oraz działań w cyberprzestrzeni. Było to stwierdzenie niezwykle istotne, wskazywało bowiem na potrzebę dogonienia światowej czołówki w zakresie zdolności do walki teleinformatycznej[60]. Zagadnienia te poruszono również w drugim opracowaniu: „Bezpieczeństwo pozamilitarne Polski w świetle rezultatów SPBN". Omawiając asymetryczne zagrożenia dla bezpieczeństwa państwa, zwrócono uwagę na wyzwania pojawiające się w cyberprzestrzeni, w tym: cyberprzestępczość, cyberszpiegostwo oraz haking. Co bardzo ważne, zaakcentowano także znaczenie zjawiska wojny informacyjnej. Stwierdzono przy tym, że „może przybierać postać działalności o charakterze agresji cybernetycznej mającej bardzo różną motywację — od politycznej, przez religijną po biznesową — po którą sięgać mogą zarówno władze i służby państw wrogich, jak i organizacje o charakterze pozarządowym i ponadnarodowym oraz organizacje przestępcze"[61]. Wreszcie, najważniejszym rezultatem SPBN było przygotowanie Białej Księgi Bezpieczeństwa Narodowego RP, opublikowanej w maju 2013 roku. Wielokrotnie podkreślono w niej rosnące znaczenie zagrożeń dla bezpieczeństwa teleinformatycznego, w różnych wymiarach. Na problem ten zwrócił nawet uwagę w przedmowie prezydent Bronisław Komorowski. Na tej podstawie trafnie stwierdzono, że cyberprzestrzeń staje się stopniowo sferą nie tylko działalności przestępców i terrorystów, lecz także rywalizujących ze sobą państw. W tym kontekście szkodliwą działalność w przestrzeni teleinformatycznej uznano za jedno z głównych wyzwań o charakterze transnarodowym i asymetrycznym. Wydaje się, że najistotniejsze ustalenia zawarto jednak w rozdziale trzecim: „Koncepcja Działań Strategicznych". Wyróżniono w nim bowiem szereg zadań stojących przed państwową polityką bezpieczeństwa teleinformatycznego. Zaliczono do nich: „ochronę systemów informacyjnych państwa, rozwój współpracy i koordynację działań ochronnych z podmiotami sektora prywatnego […] szczególnie w sferze dostępu do informacji o dokonywanych atakach i ich rodzajach, prowadzenie działań o charakterze prewencyjnym i profilaktycznym w zakresie ochrony obywateli przed zagrożeniami płynącymi z cyberprzestrzeni, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie ofensywnej i defensywnej walki

[60] Aspekty bezpieczeństwa militarnego w ujęciu Strategicznego Przeglądu Bezpieczeństwa Narodowego. „Bezpieczeństwo Narodowe" 2012, nr 3—4, s. 42, 44, 45, 48.

[61] Bezpieczeństwo pozamilitarne Polski w świetle rezultatów SPBN. „Bezpieczeństwo Narodowe" 2012, nr 3—4, s. 64—69, 73—75.

informacyjnej w cyberprzestrzeni, a także koordynację działań z innymi podmiotami systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej". Wreszcie, zauważono potrzebę stworzenia „narodowego systemu obrony cybernetycznej", zintegrowanego z systemami innych państw NATO[62]. Białą Księgę Bezpieczeństwa Narodowego RP należy więc uznać za bardzo istotny dokument, w którym zawarto główne wytyczne dalszych prac nad polityką ochrony cyberprzestrzeni Polski.

Drugim istotnym efektem prac w tej dziedzinie była nowelizacja w 2011 roku ustawy o stanie wojennym. Stanowiła ona w rzeczywistości realizację części założeń omówionych wcześniej programów ochrony cyberprzestrzeni RP. Dokument ten po raz pierwszy w historii wprowadził bowiem do porządku prawnego Polski definicję cyberprzestrzeni. Ustawa uznała ją za „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w 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.1), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[63]. W ustawie tej system teleinformatyczny uznano za „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego"[64]. Jak zauważyli Krzysztof Liedel i Michał Grzelak, definicja ta współgrała z rozumieniem tego pojęcia zaproponowanym przez Centrum Doskonalenia Cyberobrony (CCD COE), łącząc komponent techniczny z ludzkim[65]. Co jednak najważniejsze, poza ostatecznym zdefiniowaniem cyberprzestrzeni, w nowelizacji dostrzeżono skalę zagrożeń dla bezpieczeństwa teleinformatycznego państwa. W art. 2 stwierdzono bowiem, że w wyniku działań w cyberprzestrzeni, prezydent RP na wniosek Rady Ministrów może wprowadzić stan wojenny na części lub na całym terytorium państwa[66].

---

[62] Biała Księga Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej. Biuro Bezpieczeństwa Narodowego, Warszawa 2013, s. 12, 116, 117, 172, 205.

[63] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczpospolitej Polskiej. Dz.U. 2002, Nr 156, poz. 1301; 2003, Nr 228, poz. 2261; 2004, Nr 107, poz. 1135; 2011, Nr 222, poz. 1323.

[64] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005, Nr 64, poz. 565; Dz.U. 2006, Nr 12, poz. 65; Nr 73, poz. 501; Dz.U. 2008, Nr 127, poz. 817; Dz.U.2009, Nr 157, poz. 1241; Dz.U. 2010, Nr 40, poz. 230; Nr 167, poz. 1131; Nr 182, poz. 1228; Dz.U. 2011, Nr 112, poz. 654; Nr 185, poz. 1092; Nr 204, poz. 1195, Dz.U. 2012, poz. 1407.

[65] M. Grzelak, K. Liedel: *Bezpieczeństwo w cyberprzestrzeni…*, s. 132.

[66] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczpospolitej

Wreszcie, warto również omówić Narodowy Program Ochrony Infrastruktury Krytycznej przyjęty 26 marca 2013 roku przez Radę Ministrów. Stał się on odpowiedzią na coraz częściej wskazywane przez ekspertów nowe zagrożenia dla jej prawidłowego funkcjonowania, a co za tym idzie, dla bezpieczeństwa narodowego. W tym kontekście zaproponowano szereg działań ochronnych. Obok ochrony fizycznej czy technicznej, podkreślono także znaczenie ochrony teleinformatycznej. Rozumiano przez to: „zespół przedsięwzięć, procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych. Oznacza to również ochronę przed cyberatakami, cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom". W dokumencie zawarto także definicje tych pojęć, które były w zasadzie tożsame z zaproponowanymi przez Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011—2016[67].

System reagowania na incydenty teleinformatyczne RP

Za ochronę cyberprzestrzeni Rzeczpospolitej Polskiej odpowiedzialny jest rząd. Główna odpowiedzialność koordynacyjna ciąży na ministrze właściwym ds. informatyzacji. Rząd realizuje swoje kompetencje za pomocą kilku instytucji, do których należą: Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych, Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego. Należy jednak rozróżnić dwa aspekty działania służb publicznych. Prezes Rady Ministrów oraz podległe mu ministerstwa są odpowiedzialne przede wszystkim za działania o charakterze koncepcyjnym (opracowywanie strategii), legislacyjnym (aktualizacja i przygotowanie ustawodawstwa), administracyjnym (koordynacyjnym) czy politycznym. Praktycznym przeciwdziałaniem incydentom teleinformatycznym zajmują się jednak wyznaczone do tego podległe im służby i inne organy. Można je podzielić na struktury zajmujące się ochroną sieci cywilnych, w tym administracji publicznej, oraz sieci wojskowych.

System regulujący ochronę sieci wojskowych RP ma w dużej mierze charakter niejawny, przez co jego omówienie nastręcza sporych trudności. Na podstawie dostępnych materiałów, można jednak wskazać jego najważ-

Polskiej. Dz.U. 2002, Nr 156, poz. 1301; Dz.U. 2003, Nr 228, poz. 2261; Dz.U. 2004, Nr 107, poz. 1135; Dz.U. 2011, Nr 222, poz. 1323.

[67] Narodowy Program Ochrony Infrastruktury Krytycznej. Rządowe Centrum Bezpieczeństwa, 26.03.2013.

niejsze cechy i elementy. Przede wszystkim, istotną rolę odgrywają w nim służby wywiadowcze i kontrwywiadowcze: SKW i SWW. Służba Kontrwywiadu Wojskowego zajmuje się m.in. udzielaniem akredytacji bezpieczeństwa teleinformatycznego, szkoleniami specjalistycznymi lub certyfikacją środków ochrony elektromagnetycznej[68]. Natomiast Służba Wywiadu Wojskowego prowadzi wywiad elektroniczny na rzecz Sił Zbrojnych RP[69]. Odpowiednie komórki zajmujące się bezpieczeństwem teleinformatycznym znajdują się również w Ministerstwie Obrony Narodowej RP. W ramach powołanego na mocy decyzji z lipca 2008 roku Systemu Reagowania na Incydenty Komputerowe w Resorcie Obrony Narodowej, funkcjonują dwie niezwykle istotne struktury w praktyce odpowiedzialne za zapewnienie bezpieczeństwa teleinformatycznego w sieciach wojskowych. Są to: Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi oraz Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Oprócz nich, w ramach SRnIK działają także: wspomniana już Służba Kontrwywiadu Wojskowego, Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Departamentu Informatyki i Telekomunikacji MON, Departament Ochrony Informacji Niejawnych, Komenda Główna Żandarmerii Wojskowej czy Zarząd Planowania Systemów Dowodzenia i Łączności (P6), działający w ramach Sztabu Generalnego. Należy podkreślić, że między tymi organami istnieje podział obowiązków na obronę cybernetyczną oraz na dowodzenie i kierowanie w cyberprzestrzeni. Co więcej, mimo wojskowego charakteru tych struktur, współpracują one ściśle z ich odpowiednikami cywilnymi, tak na poziomie narodowym, jak i międzynarodowym. Ponadto, w ramach 9. Batalionu Łączności funkcjonuje również utworzone w 2010 roku w Białobrzegach Centrum Bezpieczeństwa Cybernetycznego. Do jego zadań należy ochrona polskich dowództw wojskowych przed atakami teleinformatycznymi. Szczegóły dotyczące jego funkcjonowania pozostają jednak tajne[70]. W tym kontekście, warto również przytoczyć opinię dyrektora Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe MON Romualda Hoffmana, według którego obszar sieci wojskowych, w odróżnieniu od obszaru administracji publicznej, posiada nie tylko procedury, zasoby i struktury, lecz także niezbędne regulacje[71].

---

[68] Bezpieczeństwo teleinformatyczne. Służba Kontrwywiadu Wojskowego. Zob. http://www.skw.gov.pl/ZBIN/bezp_it.htm?lev1=2&lev2=1 [dostęp: 27.04.2013].

[69] Zadania. Służba Wywiadu Wojskowego. Zob. http://www.sww.gov.pl/pl/11.html [dostęp: 27.04.2013].

[70] Zob. W. Lorenz: *Polska na cyberfroncie*. „Rzeczpospolita" 1.12.2010. Zob. http://www.rp.pl/artykul/572005.html [dostęp: 28.04.2013].

[71] R. Hoffman: Prezentacja: *Doświadczenia z zakresu ochrony cyberprzestrzeni Ministerstwa Obrony Narodowej.* Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputero-

Nieco inaczej wygląda sprawa ochrony sieci cywilnych. W tym przypadku, ze względu na wspomniany już długoletni brak dokumentu wyznaczającego priorytety ochrony cyberprzestrzeni RP, kwestie te są usystematyzowane w sposób nieco mniej kompleksowy. Główną służbą zajmującą się ochroną administracji publicznej jest Agencja Bezpieczeństwa Wewnętrznego. Realizuje ona ustawowe kompetencje w zakresie bezpieczeństwa systemów teleinformatycznych, przeznaczonych do przetwarzania informacji niejawnych. Bezpośrednią odpowiedzialność przyjął Departament Bezpieczeństwa Teleinformatycznego ABW, w ramach którego funkcjonuje przywołany wcześniej Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[72]. Został on utworzony 1 lutego 2008 roku. Do jego zadań należy: „koordynacja reagowania na incydenty, publikacja alertów i ostrzeżeń, obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych), publikacja powiadomień (biuletynów zabezpieczeń), koordynacja reagowania na luki w zabezpieczeniach obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV oraz przeprowadzanie testów bezpieczeństwa. W praktyce to ten zespół jest więc odpowiedzialny za wszystkie ataki teleinformatyczne przeciwko sieciom i komputerom administracji państwowej”[73]. Mimo innego zakresu obowiązków, współpracuje on z omówionym już Systemem Reagowania na Incydenty Komputerowe w Resorcie Obrony Narodowej oraz Ministerstwem Spraw Wewnętrznych. Co więcej, utrzymuje on także ścisłe kontakty z CERT Polska oraz zespołami zagranicznymi: US-CERT czy CERT Coordination Center.

Ochroną cyberprzestrzeni RP zajmuje się również utworzony w 1996 roku zespół CERT Polska, działający w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK). Do jego zadań należy: obsługa zdarzeń naruszających bezpieczeństwo sieci, alarmowanie użytkowników o zagrożeniach, współpraca z innymi zespołami Incidents Response Team, działania na rzecz podnoszenia świadomości użytkowników, prowadzenie badań i przygotowywanie raportów, testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego oraz tworzenie wzorców obsługi i rejestracji incydentów oraz ich odpowiedniej klasyfikacji. W praktyce CERT Polska zajmuje się m.in. walką z kradzieżą tożsamości w polskim Internecie, analizą najpoważniejszych incydentów teleinformatycznych czy zwalczaniem

---

we Departamentu Informatyki i Telekomunikacji MON. Zob. www.automatyzacja.itwl.pl/files/Referat_P22_.ppsx [dostęp: 27.04.2013].

[72] Bezpieczeństwo teleinformatyczne. Agencja Bezpieczeństwa Wewnętrznego. Zob. http://www.bip.abw.gov.pl/portal/bip/79/154/BEZPIECZENSTWO_TELEINFORMATYCZNE.html [dostęp: 27.04.2013].

[73] *O nas.* CERT.GOV.PL. Zob. http://www.cert.gov.pl/portal/cer/27/15/O_nas.html [dostęp: 28.04.2013].

szkodliwego oprogramowania (m.in. *ransomware*). Istotnym osiągnięciem technicznym zespołu CERT Polska jest system ARAKIS, który jest wykorzystywany w wersji ARAKIS-GOV przez zespół CERT.GOV.PL[74].

Warto dodać, że bezpieczeństwo teleinformatyczne RP wzmacnia dodatkowo członkostwo w Sojuszu Północnoatlantyckim. Od 2011 roku Polska uczestniczy w pracach, mającego siedzibę w Tallinie, Centrum Doskonalenia Cyberobrony (CCD COE). Jest to instytucja zajmująca się przede wszystkim prowadzeniem badań, analiz oraz organizacją szkoleń ekspertów państw członkowskich. Ponadto, w przypadku poważnych incydentów teleinformatycznych, Warszawa może liczyć na pomoc ze strony Zespołów Szybkiego Reagowania NATO (*Rapid Response Teams*)[75].

Na podstawie przytoczonych danych można stwierdzić, że przygotowanie polskich służb do reagowania na incydenty komputerowe w ostatnich latach zdecydowanie się poprawiło. Jest to szczególnie widoczne w obrębie sieci wojskowych, gdzie funkcjonuje złożony system walki z zagrożeniami teleinformatycznymi. Cechują go nie tylko rosnący potencjał, lecz także niezbędne procedury i regulacje prawno-administracyjne. Jeśli chodzi zaś o ochronę sieci administracji publicznej, mimo znacznej efektywności zespołów CERT.GOV.PL i CERT Polska, nie ulega wątpliwości, że nadal brakuje w tym zakresie wielu odpowiednich rozwiązań, tak w wymiarze technicznym, politycznym, prawnym, jak i administracyjnym.

Dylematy polskiej polityki bezpieczeństwa teleinformatycznego

Można wskazać kilka zasadniczych dylematów polskiej polityki bezpieczeństwa teleinformatycznego na początku drugiej dekady XXI wieku. Przede wszystkim, należy zwrócić uwagę na bardzo niskie tempo prac nad pierwszym dokumentem, który uregulował politykę ochrony cyberprzestrzeni RP.

---

[74] *O nas.* CERT Polska. Zob. http://www.cert.pl/o-nas [dostęp: 28.04.2013]; *Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne.* CERT Polska — NASK. Warszawa 2013.

[75] *NATO Rapid Reaction Team to fight cyber attack.* North Atlantic Treaty Organization News. Zob. http://www.nato.int/cps/en/natolive/news_85161.htm [data publikacji: 13.03.2012; dostęp: 28.04.2013]; *NATO opens new center of excellence on cyber defence.* North Atlantic Treaty Organization News. Zob. http://www.nato.int/docu/update/2008/05-may/e0514a.html [data publikacji: 14.05.2008; dostęp: 28.04.2013]; *Przyjęcie Polski do Centrum Cyberobrony NATO w Tallinie.* Ministerstwo Obrony Narodowej RP. Zob. http://mon.gov.pl/pl/artykul/12117 [data publikacji: 17.11.2011; dostęp: 28.04.2013].

Trwały one 6 lat, co jest zdecydowanie zbyt długim okresem. Przeciąganie się dyskusji na ten temat okazało się szkodliwe dla bezpieczeństwa narodowego nie tylko ze względu na dynamikę wyzwań pojawiających się w cyberprzestrzeni, lecz także rosnący poziom zaawansowania innych podmiotów międzynarodowych[76]. Utrzymywanie się sytuacji, w której Polska nie posiadała strategii wyznaczającej priorytety polityki cyberbezpieczeństwa sprawiło, że wysiłki w tej dziedzinie były mało skoordynowane i zapóźnione w stosunku do państw zachodnich. Jest to tym bardziej istotne, że potencjał oraz zdolność rządów do działania w cyberprzestrzeni w przyszłości będą wpływać w coraz większym stopniu na ich pozycję na arenie międzynarodowej.

Po drugie, warto szerzej omówić sygnalizowane wcześniej wątpliwości związane z treścią Polityki Ochrony Cyberprzestrzeni RP. Dotyczą one głównie przyjętych definicji podstawowych terminów z zakresu bezpieczeństwa teleinformatycznego, które mają stanowić fundament dalszych prac legislacyjnych w tej dziedzinie. Jest to szczególnie widoczne w przypadku cyberterroryzmu, który uznano za „przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni". Tymczasem, jak słusznie wskazywali m.in. Agnieszka Bógdał-Brzezińska, Marcin Florian Gawrycki czy Ernest Lichocki, cyberterroryzm obejmuje także aspekty komunikacji, rekrutacji, propagandy lub dezinformacji[77]. Spore wątpliwości może budzić również fakt, że w projekcie POCRP znalazły się definicje cyberterroryzmu, cyberataku czy cyberprzestępstwa, natomiast pominięto inne istotne formy zagrożeń teleinformatycznych, w tym np.: haking, haktywizm, cyberszpiegostwo czy wykorzystanie cyberprzestrzeni do działań zbrojnych. Wydaje się więc, że katalog wyzwań powinien zostać zdecydowanie poszerzony, szczególnie w kontekście coraz powszechniejszego zjawiska cyberwojny[78]. Jest to kwestia o fundamentalnym znaczeniu dla bezpieczeństwa narodowego, o czym świadczy fakt, że najbardziej zaawansowane państwa w tej dziedzinie, w tym m.in. Stany Zjednoczone, już od kilku lat wypracowują mechanizmy interpretacji tego typu incydentów oraz reagowania na nie.

Po trzecie, warto zauważyć, że cyberprzestrzeń w coraz większym stopniu stanowi obszar, gdzie różnorodne podmioty stosunków międzynarodowych starają się realizować określone cele i interesy za pomocą cyberataków. W przypadku polskich rozwiązań, zdecydowany nacisk położono jedynie

---

[76] K. Giles: *Russia's Public Stance on Cyberspace Issues*. In: *2012 4th International Conference on Cyber Conflict*. Ed. C. Czosseck, R. Ottis, K. Ziolkowski. Tallin 2012, s. 63—75; M. Lakomy: *Cyberzagrożenia na początku XXI wieku*. „Przegląd Zachodni" 2012, nr 4, s. 205—224.

[77] A. Bógdał-Brzezińska, M.F. Gawrycki: *Cyberterroryzm i problemy bezpieczeństwa…*, s. 73; E. Lichocki: *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*. W: *Transsektorowe obszary bezpieczeństwa narodowego*. Red. K. Liedel. Warszawa 2011, s. 71.

[78] A. Bautzmann: *Le cyberespace, nouveau champ de bataille…*, s. 80—81.

na wykorzystanie środków defensywnych. Pojawia się więc pytanie, czy nie należałoby w tych pracach, szczególnie w wymiarze wojskowym, uwzględnić również instrumentalnego potencjału rozmaitych narzędzi teleinformatycznych, wzorem np. Stanów Zjednoczonych[79]?

Wreszcie, pewne wątpliwości może budzić także wymiar finansowy wysiłków RP w tej dziedzinie. W POCRP w sposób niezwykle oszczędny autorzy podeszli do kwestii kosztów rozwoju potencjału teleinformatycznego. Wydaje się, że takie podejście jest dalece niewystarczające. Jak bowiem udowadniają doświadczenia państw zachodnich, ofensywne wykorzystanie cyberprzestrzeni wiąże się ze stosunkowo niewielkimi kosztami. Tymczasem zabezpieczenie komputerów i sieci przed cyberatakami jest zdecydowanie bardziej wymagające[80]. Tym samym, zagwarantowanie stałego poziomu finansowania rozwoju potencjału w tej dziedzinie wydaje się warunkiem *sine qua non* wysokiej skuteczności zabezpieczeń w cyberprzestrzeni RP.

Zakończenie

Z pewnością zasadniczym powodem zainicjowania przez polskie władze poważnych prac w dziedzinie bezpieczeństwa teleinformatycznego była „pierwsza cyberwojna" w Estonii oraz następujące po niej wydarzenia w Syrii oraz Gruzji. Wówczas polscy decydenci w stopniu zdecydowanie większym niż wcześniej zainteresowali się skutkami szkodliwego wykorzystania cyberprzestrzeni. Dzięki temu, w ciągu kilku lat udało się wypracować szereg interesujących rozwiązań i mechanizmów. Na pozytywną ocenę zasługują wysiłki w zakresie ochrony polskich sieci wojskowych, które wykazują wysoki stopień zaawansowania oraz skuteczności. Ich pełna ocena jest jednak niemożliwa ze względu na znaczny stopień tajności rozwiązań na tym obszarze. Nieco inaczej należy natomiast postrzegać rozwiązania przyjęte w zakresie ochrony systemów i sieci cywilnych, w tym przede wszystkim administracji publicznej. W tym wypadku, mimo silnego zaawansowania technicznego zabezpieczeń, w ostatnich latach doszło do szeregu zakończonych sukcesem cyberataków.

Na tej podstawie można zauważyć pewien dysonans w pracach na rzecz ochrony cyberprzestrzeni RP. W ciągu ostatnich lat wypracowano bowiem zestaw rozwiązań i mechanizmów, które w praktyce powinny chronić państwo przed różnorodnymi formami zagrożeń teleinformatycznych. Przedsięwzięcia podejmowano jednak nieregularnie, w odpowiedzi na konkretne,

[79] Zob. *Strategy for Operating in Cyberspace*. U.S. Department of Defense, July 2011.
[80] F. Schreier: *On Cyberwarfare*…, s. 12.

bieżące potrzeby państwa, a nie na drodze realizacji założonego wcześniej spójnego planu działań. Wydaje się, że to jest obecnie największy problem, przed którymi stoi polityka cyberbezpieczeństwa Polski. Dopiero po 6 latach dyskusji udało się opracować podstawę koncepcyjną dla rozwoju systemu interpretacji, reagowania oraz przeciwdziałania wyzwaniom pojawiającym się na tym obszarze. W tym kontekście, można zauważyć również pewien rozdźwięk pomiędzy bardzo ciekawymi rozwiązaniami i spostrzeżeniami zawartymi m.in. w raportach i analizach Biura Bezpieczeństwa Narodowego (w tym przede wszystkim Białej Księdze Bezpieczeństwa Narodowego RP) a treścią Polityki Ochrony Cyberprzestrzeni RP (wcześniej RPOC). Doceniając jej priorytety, w tym nacisk na badania naukowe, szkolenia, współpracę z sektorem prywatnym oraz współpracę międzynarodową, należy stwierdzić, że pominięto w niej szereg istotnych kwestii, m.in. sprawę militaryzacji cyberprzestrzeni, wykorzystania jej jako obszaru realizacji określonych interesów i celów przez inne państwa, cyberszpiegostwa czy dylematów związanych z interpretacją prawa międzynarodowego. Twórcy przyszłej, rozwiniętej strategii walki z zagrożeniami teleinformatycznymi RP powinni ustosunkować się do wszystkich tych problemów, co jest kwestią fundamentalną z punktu widzenia polskiej racji stanu. Tylko kompleksowe podejście pozwoli bowiem skutecznie przeciwdziałać różnorodnym i stale ewoluującym zagrożeniom bezpieczeństwa teleinformatycznego Polski. Jest to tym bardziej istotne, że sposób reagowania na te wyzwania może być w przyszłości jednym z determinantów międzynarodowej pozycji RP.