FOLIA 292

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 9(4) (2019)
ISSN 2657-8549
DOI 10.24917/26578549.9.4.11

Aneta Waloch
ORCID ID 0000-0003-3820-2110
Lotnicza Akademia Wojskowa

Współczesne zagrożenia dla bezpieczeństwa państwa polskiego w cyberprzestrzeni

Wprowadzenie

W świecie postępującej globalizacji internet jest jednym z głównych kanałów komunikacyjnych na świecie. Komputerowe techniki, które ponad 15 lat temu były tylko wytworem ludzkiej wyobraźni bądź stanowiły wątki filmów *science fiction*, są obecnie wykorzystywane na co dzień. Stosowanie elektronicznych podpisów, korzystanie z portali społecznościowych oraz rozrywkowych, posiadanie kont bankowych w sieci, wizualizacja rzeczywistości czy ogólnoświatowa wymiana informacji nie jest dla nas niczym zaskakującym, ponieważ korzystamy z tego każdego dnia. Niemniej jednak wraz z rozwojem internetu oraz cyfryzacji zaczęło się rozwijać środowisko hakerów oraz szkodliwego oprogramowania. Aby przeciwdziałać ich ingerencji w komputery, firmy zajmujące się oprogramowaniem antywirusowym wydają coraz nowsze i bardziej nowoczesne aktualizacje swoich programów. Ponadto bardzo dobrym działaniem, które ma przyczynić się do wzrostu naszego bezpieczeństwa w sieci, jest informowanie użytkowników internetu przez różnego rodzaju kanały przepływu informacji (portale społecznościowe, telewizję, gazety) o zagrożeniach, na które naraża ludzi korzystanie z internetu. Nie zawsze jednak zdajemy sobie sprawę z tego, jakie zagrożenia niesie nieumiejętne lub nieuważne korzystanie z nowoczesnych technologii. Może ono prowadzić do awarii sprzętu, z którego korzystamy, jak również, w najgorszym przypadku, do utraty wrażliwych danych (m.in. danych bankowych) lub skasowania bądź zainfekowania danych znajdujących się na danym urządzeniu.

Pojęcie cyberprzestrzeni

Termin „cyberprzestrzeń" został użyty po raz pierwszy w 1984 roku przez amerykańskiego pisarza *science fiction*, Williama Gibsona, który opisał ją jako

„wygenerowany świat wirtualnej rzeczywistości utworzonej przez komputer, nazwany inaczej matrycą”[1].

Badanie podstaw prawnych regulujących pojęcie bezpieczeństwa w cyberprzestrzeni należy rozpocząć od najważniejszego aktu prawnego określającego polskie prawo, czyli Konstytucji RP. Wprawdzie w wymienionym akcie ustawodawca nie użył nazwy „cyberprzestrzeń” wprost, jednak takie elementy jak ochrona praw oraz wolności obywatela, zapewnienie niepodległości i nienaruszalności swojego terytorium, zapewnienie wolności i praw człowieka odnosi się również do środowiska cyberprzestrzeni[2].

Dopiero jednak w roku 2014 w Strategii Bezpieczeństwa Narodowego bezpośrednio określony został cel dotyczący bezpieczeństwa państwa polskiego w cyberprzestrzeni[3].

Kolejną definicję przedstawia Ustawa z dnia 30 sierpnia 2011 roku o zmianie ustawy o stanie wojennym i kompetencjach Naczelnego Dowódcy Sił Zbrojnych. W tym akcie prawnym pojęcie jest definiowane jako „przestrzeń przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne”. W *Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej* wyjaśniono z kolei, że cyberprzestrzenią jest „przestrzeń przetwarzania i wymiany informacji tworzona przez system teleinformatyczny wraz z powiązaniami między nimi oraz relacjami z użytkownikami”[4].

Departament Obrony USA definiuje cyberprzestrzeń jako „Globalną domenę środowiska informacyjnego składającą się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery”[5]. Mimo że definicje cyberprzestrzeni różnią się od siebie, można wyróżnić w nich kilka cech wspólnych: zjawiska zachodzące w tej płaszczyźnie cechują się asymetrycznością, mają charakter transgraniczny, przenikają wszystkie sektory gospodarki i mają wpływ na funkcjonowanie państwa i społeczeństwa we wszystkich jego wymiarach, tworząc całość powiązań w sektorze ludzkiej działalności z udziałem technologii informacyjno-komunikacyjnych[6].

W dokumentach strategicznych przyjętych w Polsce obszar cyberprzestrzeni definiowany jest jako „cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki

---

[1] W. Gibson, *Neuromancer*, Książnica, Katowice 2009, s. 59.

[2] Konstytucja RP z dnia 2 kwietnia 1977 roku, Dz.U. z 1997, nr 78, poz. 483 z. późn. zm.

[3] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014, s. 14.

[4] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s. 7.

[5] G.A. Crowther, *The Cyber Defense Review*, Vol. 2, No. 3, Army Cyber Institute 2017, s. 63.

[6] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003, s. 19.

dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)"[7].

Szeroki zakres definicyjny cyberprzestrzeni w polskich dokumentach strategicznych powoduje wiele niejasności prawno-instytucjonalnych. Takie uchybienia mogą powodować zagrożenia zarówno dla państwa, jak i społeczeństwa, związane ze strefą cywilną oraz militarną; może to wpływać na funkcjonowanie sektora bankowego, sektora teleinformatycznego, na kwestie związane z ochroną praw obywatela i protekcją infrastruktury krytycznej[8].

Zagrożenia w cyberprzestrzeni stanowiące wyzwanie dla państwa polskiego

Tabela 1. Rodzaje zagrożeń i ich odbiorcy

Zagrożenie dla państwa polskiego w cyberprzestrzeni	Zagrożenie dla obywateli państwa polskiego w cyberprzestrzeni
• Cyberprzestępczość • Cyberdemonstracje • Cyberszpiegostwo	• Cyberprzemoc • Cyberdemonstracje • Kradzież danych • Kradzież tożsamości

Źródło: opracowanie własne.

Wraz ze wzrostem znaczenia cyberprzestrzeni w czasach współczesnych, zarówno dla państwa, jak i dla obywateli, coraz istotniejszy staje się problem jej bezpieczeństwa[9].

Od wielu lat bezpieczeństwo definiowane jest w kontekście zagrożeń i wyzwań dla danego podmiotu. Zagrożenie bezpieczeństwa tym różni się od wyzwania bezpieczeństwa, że jest ono sytuacją, w której istnieje możliwość pojawienia się stanu niebezpiecznego dla otoczenia. Odznacza się ono wysokim ryzykiem powstania konfliktu, a nawet zachodzi bezpośrednie prawdopodobieństwo jego zaistnienia. W przypadku wyzwań bezpieczeństwa mówimy jedynie o przesłankach powstania konfliktu. Wyzwanie bezpieczeństwa może być pierwszym krokiem do powstania zagrożeń dla bezpieczeństwa. Współczesne wyzwania i zagrożenia bezpieczeństwa stanowią ważną treść założeń strategii bezpieczeństwa organizacji międzynarodowych i państw demokratycznych, w tym również państwa polskiego[10].

Jednym z pierwszych zagrożeń dla państwa polskiego jest cyberprzestępczość. Cyberprzestępczość to „motywowane finansowo lub materialnie akcje

[7] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*..., op. cit., s. 7.

[8] J. Świątkowska, *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014, *passim*.

[9] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, s. 12.

[10] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, R. Zięba (red.), Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 25.

w cyberprzestrzeni lub ich zamiar prowadzone przez pojedyncze osoby lub ugrupowania przestępcze, skierowane przeciwko różnorodnym podmiotom państwowym lub niepaństwowym, które w sposób bezpośredni lub pośredni prowadzą lub mogą prowadzić do ich określonych strat finansowych lub materialnych"[11].

Drugim zagrożeniem dla państwa polskiego są cyberdemonstracje. Są to publiczne zbiorowe zgromadzenia mające na celu wyrażenie zdania protestujących osób przeciw danej sprawie w internecie. Przykładem cyberdemonstracji, która miała miejsce w Polsce, była akcja w sprawie przyjęcia zapisów ACTA. Była to pierwsza cyberdemonstracja w Polsce na tak dużą skalę. Początkowo polegała ona na masowym blokowaniu stron internetowych należących do administracji państwowej. Następnie doszło do ataków na serwery rządowe. Z uwagi na to, że tego typu wydarzenia miały miejsce po raz pierwszy, Polska nie była w odpowiedni sposób przygotowana do neutralizacji tego typu zagrożeń, co w przyszłości powinno stać się początkiem dyskusji odnoszącej się do sposobów radzenia sobie z tego typu zjawiskiem.

Jako kolejne zagrożenie wyróżnia się cyberszpiegostwo. Jest to zdobywanie istotnych informacji i materiałów w cyberprzestrzeni przez służby wywiadowcze za pomocą różnych technik i metod, w szczególności metod cybernetycznych. W ciągu minionych lat w Polsce nie odnotowano aktów cyberszpiegostwa ze strony innych państw, co nie oznacza, że te akty można wykluczyć. Zagrożenie to jest coraz częściej spotykane w innych państwach i szerzy się na skalę globalną[12].

Niestety, podczas gdy cyberprzestrzeń stała się odzwierciedleniem rzeczywistości, pojawiły się w niej zagrożenia, czyli negatywne formy ludzkiej działalności. Przestrzeń internetowa ze względu na możliwość bycia anonimowym okazała się miejscem idealnym dla przestępców takich jak hakerzy, pedofile czy wyłudzacze. Jest również enigmatycznym miejscem komunikowania się terrorystów na całym świecie. Z impersonalnego charakteru internetu korzystają również państwa prowadzące działania wywiadowcze oraz te kierujące agresję w stronę innych państw, co prowadzi do tzw. cyberwojny. Najczęściej występującym zagrożeniem jest zainfekowanie urządzenia wirusem lub innym szkodliwym oprogramowaniem oraz wyłudzanie poufnych informacji. Dla cyberprzestępców największą motywacją do działania jest chęć zysku, jednak wyróżniamy jeszcze kilka innych pobudek. Przykładem są tzw. haktywiści – pojęcie to powstało od połączenia słów *hacking* i *activism*[13]. Osoby zajmujące się haktywizmem za pomocą komputerów i sieci promują cele społeczne i polityczne, np. takie jak wolność słowa, prawa człowieka. Działania takie bardzo często prowadzą do powstawania protestów, obywatelskiego nieposłuszeństwa lub aktywizmu politycznego i społecznego, czyli do cyberdemonstracji.

---

[11] D. Tennant, *The fog of (cyber) war*, „Computerworld", 27.04.2009, https://www.computerworld.com/article/2523545/the-fog-of--cyber--war.html, [dostęp: 3.04.2019].

[12] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki,* Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, s. 71.

[13] P. Krapp. *Terror and Play, or What was Hacktivism*, „Grey Room" 2015, No. 27, s. 72.

Często dochodzi również do kradzieży i przechwycenia wrażliwych danych osób, które są stanowczo przeciwne takim działaniom i pokazują to w sposób otwarty[14]. Cyberprzestrzeń bardzo często jest wykorzystywana przez terrorystów jako doskonałe narzędzie działalności o charakterze politycznym mającej podłoże cyberszpiegostwa. Wiele incydentów w cyberprzestrzeni przybierających formę wandalizmu, działań prowadzonych przy cichej akceptacji państwa lub niejawnie sponsorowanej, przypisywana jest terrorystom, lecz nie została prawnie i jednoznacznie udowodniona. Za jeden z największych cyberataków na świecie uważa się atak z 12 maja 2017 roku obejmujący 99 państwa i 75 000 zarażonych komputerów. Według specjalistów Kaspersky Lab i Avast Software państwami najbardziej dotkniętymi przez atak były Rosja, Ukraina, Indie, Tajwan, Wielka Brytania, Stany Zjednoczone, Chiny i Włochy. Atak na tak bezprecedensową skalę doprowadził do całkowitego paraliżu państw, zablokował dostępy do sieci komórkowych, systemów bankowych, systemów zdrowia[15]. Przeprowadzenie ataku nie zostało nikomu udowodnione ze względu na brak dowodów. Najczęściej stosowanym przez terrorystów narzędziem komunikacyjnym jest właśnie internet, za jego pomocą są w stanie koordynować działania propagandowe, stosować dezinformację, werbować nowych członków i pozyskiwać środki finansowe[16]. Przydatny jest również do rozpowszechniania informacji instruktażowych o charakterze terrorystycznym.

Internet służy nam głównie do pozyskiwania informacji, nie jest więc tajemnicą, że cyberprzestrzeni używa się w działaniach wywiadowczych.

Służby specjalne krajów skandynawskich w corocznych publikacjach wskazują, że rosyjskie służby specjalne takie jak Służba Wywiadu Zagranicznego i Główny Zarząd Wywiadowczy stosują agresywne rozpoznanie zarówno cywilnych, jak i wojskowych elementów infrastruktury krytycznej. Zbieżne informacje w stosunku do służb skandynawskich podają służby krajów bałtyckich oraz Europy Środkowej. Głównymi zaletami wykorzystywania cyberprzestrzeni w działaniach wywiadowczych są niskie koszty oraz anonimowość[17].

Rozwiązania regulacyjne dotyczące ochrony cyberprzestrzeni

Bardzo ważną rolę w dziedzinie zapewnienia bezpieczeństwa odgrywa Prezydent RP, którego zadaniem jest zagwarantowanie „suwerenności i bezpieczeństwa

[14] M. Milone, *Hactivism: Securing the National Infrastrucutre* [w:] *Technology and Terrorism*, D. Clarke (red.), Transaction Publishers, Piscataway 2004, s. 84–85.

[15] R. Muczyński, *Największy cyberatak w historii*, http://www.nowastrategia.org.pl/najwiekszy-cyberatak-w-historii, [dostęp: 3.04.2019].

[16] B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Akademia Obrony Narodowej, Warszawa 2013, s. 85.

[17] K. Liedel *Bezpieczeństwo informacyjne w sobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 20005, s. 19.

państwa oraz nienaruszalności i niepodzielności jego terytorium"[18]. Rada Bezpieczeństwa Narodowego wspomaga działania prezydenta zarówno w zakresie bezpieczeństwa zewnętrznego, jak i wewnętrznego państwa[19]. W sytuacji zagrożenia państwa w cyberprzestrzeni z zewnątrz na wniosek Rady Ministrów Prezydent RP może wprowadzić stan wojenny[20]. Z kolei stan wyjątkowy może zostać wprowadzony w podobny sposób, jeśli wystąpi „zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego"[21]. Wszelkie zadania Prezydenta RP w zakresie obronności oraz bezpieczeństwa są wykonywane z udziałem Biura Bezpieczeństwa Narodowego, które stworzyło *Doktrynę Cyberbezpieczeństwa Rzeczypospolitej Polskiej*[22]. Jej celem jest wyznaczenie strategicznych kierunków w dziedzinie należytego poziomu bezpieczeństwa w Polsce[23].

Prezes Rady Ministrów wraz z Radą Ministrów są podmiotami odpowiedzialnymi za koordynację strategii w zakresie ochrony państwa[24]. Prezes Rady Ministrów powierza zadania podległym mu ministerstwom, wśród których w kwestii cyberbezpieczeństwa ważną rolę odgrywa Ministerstwo Cyfryzacji. Niektóre zadania związane z zapewnieniem bezpieczeństwa są wykonywane także przez Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, czy Szefa ABW. Wszystkie te jednostki tworzą wspólnie z Ministerstwem Finansów oraz Ministerstwem Sprawiedliwości wymiar strategiczny mający zapewnić bezpieczeństwo państwa polskiego w cyberprzestrzeni.

Ministerstwo Spraw Wewnętrznych ma zapewniać ochronę porządku publicznego, a co za tym idzie działania dotyczące organów mu podległych będą związane także ze zwalczaniem przestępczości w środowisku cyberprzestrzeni. Od 16 listopada 2015 roku obowiązek realizacji tematu bezpieczeństwa w cyberprzestrzeni należy do Ministerstwa Cyfryzacji, co czyni go kluczową instytucją w procesie zagwarantowania protekcji w cyberprzestrzeni. Minister Cyfryzacji ma zarówno wprowadzać i koordynować Politykę Ochrony Cyberprzestrzeni RP (POC), jak również edukować społeczeństwo w dziedzinie informatyki[25]. Celem Polityki Ochrony Cyberprzestrzeni RP jest „osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni

---

[18] Konstytucja Rzeczypospolitej Polskiej…, op. cit., art. 126, pkt 2.

[19] Ibidem, art. 135.

[20] Ibidem, art. 229.

[21] Ibidem, art. 230.

[22] Ustawa z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz.U. 2004, Nr 241, poz. 2416 z późn. zm.

[23] A. Trubalski, J. Trubalska, *Bezpieczeństwo Polski w cyberprzestrzeni* [w:] *Bezpieczeństwo państwa w cyberprzestrzeni*, J. Trubalska, Ł. Wojciechowski (red.), Innovatio Press – Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji, Lublin 2017, s. 25.

[24] Konstytucja Rzeczypospolitej Polskiej…, op. cit., art. 146, pkt 4.

[25] Ustawa z dnia 17 lutego 2005 roku o informatyzacji podmiotów realizujących zadania publiczne związane z informatyzacją administracji publicznej, Dz.U. 2017, poz. 570.

Państwa"[26]. Wymieniony cel został również zapisany w *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020* oraz w *Rządowym programie ochrony cyberprzestrzeni RP na lata 2011–2016*[27].

Niektóre kompetencje w zakresie zagwarantowania bezpieczeństwa w cyberprzestrzeni zostały nadane Ministrowi Gospodarki. Jego obowiązkiem jest koordynowanie i wdrażanie Rozporządzenia Rady (UE) i Europejskiego Parlamentu nr 910/2014, którego celem jest m.in. ujednolicenie aspektów prawnych okazywania usług zaufania, zapewnienie uznawania działań mówiących o transakcjach elektronicznych czy też uwierzytelnianie stron internetowych[28].

Ministerstwo Sprawiedliwości także odgrywa kluczową rolę w aparacie systemu bezpieczeństwa, ponieważ spoczywa na nim obowiązek stwarzania oraz kodyfikacji prawa odnoszącego się do cyberprzestępczości oraz bezpieczeństwa w środowisku cyberprzestrzeni. Z kolei rolą Ministerstwa Finansów jest dbanie o finanse publiczne, co przekłada się na kształt zarówno bezpieczeństwa w szerokim jego rozumieniu, jak i w rozumieniu bezpieczeństwa w cyberprzestrzeni. Instytucje sektorowe takie jak Komisja Nadzoru Finansowego, Urząd Komunikacji Elektronicznej, Generalny Inspektor Danych Osobowych, czy Rządowe Centrum Bezpieczeństwa również są odpowiedzialne za stwarzanie ram regulacyjnych w zakresie cyberprzestrzeni. Urząd Komunikacji Elektronicznej pełni funkcję regulatora w dziedzinie telekomunikacji, będąc odpowiedzialnym za implementację ustawy o prawie telekomunikacyjnym[29]. Zadaniem Rządowego Centrum Bezpieczeństwa jest utworzenie Narodowego Programu Ochrony Infrastruktury Krytycznej, a także „odpowiadanie za koordynacje działań w zakresie ochrony teleinformatycznej infrastruktury krytycznej"[30]. Do zadań Generalnego Inspektora Ochrony Danych Osobowych należy z kolei zapewnienie bezpieczeństwa danych osobowych oraz scalenie polskiego prawa z prawem unijnym. Komisja Nadzoru Finansowego jest zaś odpowiedzialna za sferę sektora bankowego w momencie, gdy zaistniałe zagrożenie spowoduje negatywne skutki finansowe dla tego sektora[31].

---

[26] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*…, op. cit., s. 8.

[27] *Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016*, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, s. 7; *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020*, Ministerstwo Cyfryzacji, Warszawa 2016, s. 4.

[28] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE Dz. Urz. UE L 257, art. 1 z dnia 28.08.2014.

[29] Ustawa z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne, Dz.U. 2017, poz. 936.

[30] *Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016…*, op. cit., s. 7; *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020*, op. cit., s. 8.

[31] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 132.

Wnioski

Mimo zalet, które wynikają z rozwoju cyberprzestrzeni, można też wyodrębnić szereg wad z nim związanych. Rozwijające się środowisko cyberprzestrzeni jest idealnym miejscem dla hakerów oraz przestępców internetowych, którzy wraz z rozwojem technologii są coraz bardziej efektywni i posiadają dostęp do coraz pilniej strzeżonych danych. Cyberprzestrzeń jest również źródłem wielu zagrożeń dla bezpieczeństwa zewnętrznego i wewnętrznego państwa. Ze względu na ich istotę przeciwdziałanie takim zagrożeniom jest priorytetem.

W celu zwiększenia bezpieczeństwa w cyberprzestrzeni państwo polskie powinno zwiększyć nacisk na profilaktykę korzystania z internetu oraz stale uświadamiać społeczeństwo w kwestii zagrożeń w sieci, na które jesteśmy narażeni. Z uwagi na ciągły rozwój technologii niezbędne jest szkolenie większej liczby specjalistów zajmujących się bezpieczeństwem teleinformatycznym, którzy będą w stanie na bieżąco rozpoznawać nowe rodzaje zagrożeń i reagować na nie. Należy również zadbać o ochronę najważniejszych systemów teleinformatycznych państwa polskiego oraz wykonywać ćwiczenia sprawdzające odporność infrastruktury na ataki cybernetyczne.

Z uwagi na globalny charakter internetu niezbędne jest stworzenie dokumentu regulującego aspekty prawne cyberbezpieczeństwa na całym świecie, który ujednoliciłby sposoby przeciwdziałania, szybkiego reagowania i wiele innych kwestii związanych z zagrożeniami w cyberprzestrzeni, tak aby wszystkie kraje respektujące taki dokument były w stanie współpracować i przeciwdziałać tego typu zagrożeniom w przyszłości.

Działania, które mają na celu zapewnienie bezpieczeństwa w cyberprzestrzeni, muszą być stale aktualizowane, tak aby państwo zawsze było w stanie zapobiec zagrożeniom lub w razie ich wystąpienia przeciwdziałać im.

Bibliografia

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016.

Bezpieczeństwo międzynarodowe po zimnej wojnie, R. Zięba (red.), Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

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

Crowther G.A., *The Cyber Defense Review*, Vol. 2, No. 3, Army Cyber Institute 2017.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

Gibson W., *Neuromancer*, Książnica, Katowice 2009.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Liedel K., *Bezpieczeństwo informacyjne w sobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego,* Wydawnictwo Adam Marszałek, Toruń 2005.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz.U. 1997, nr 78.

Krapp P., *Terror and Play, or What was Hacktivism,* „Grey Room" 2015, No. 27.

Milone M., *Hactivism: Securing the National Infrastrucutre* [w:] *Technology and Terrorism*, D. Clarke (red.), Transaction Publishers, Piscataway 2004.

Muczyński R., *Największy cyberatak w historii,* http://www.nowastrategia.org.pl/najwiekszy-cyberatak-w-historii, [dostęp: 3.04.2019].

Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Akademia Obrony Narodowej, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Dz. Urz. UE L 257, art. 1 z dnia 28.08.2014.

Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2014.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020, Ministerstwo Cyfryzacji, Warszawa 2016.

Świątkowska J., *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Instytut Kościuszki, Kraków 2014.

Trubalski A., Trubalska J., *Bezpieczeństwo Polski w cyberprzestrzeni* [w:] *Bezpieczeństwo państwa w cyberprzestrzeni*, Trubalska J., Wojciechowski Ł. (red.), Innovatio Press – Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji, Lublin 2017.

Ustawa z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne, Dz.U. 2017, poz. 936.

Ustawa z dnia 17 lutego 2005 roku o informatyzacji podmiotów realizujących zadania publiczne związane z informatyzacją administracji publicznej, Dz.U. 2017, poz. 570.

Ustawa z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz.U. 2004, Nr 241, poz. 2416 z późn. zm.

Modern risks in the cyberspace for the security of polish country

Abstract

Technology development is a fact, that all the people are dealing with nowadays. When the new spare of activity of the cyberspace came up, the new risks shows up, and people have to deal with it, even if we don't know about it. By becoming the new users of cyberspace people are expose to the dangers like hackers attacks, virtual frauds and many more. Prevention of activities like entering the dangerous websites, or downloading suspicious programs, without using antivirus. The best example of how strong are hackers, we had in 12 of May 2017, when almost 75,000 computers were hacked that day by unknown hackers. Poland has to manage with the preventing problems of risks in cyberspace, but also claiming the appropriate level of security by steady improving the legal foundations and activities in the cybersecurity zone.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, bezpieczeństwo, zagrożenia

Key words: cybersecurity, cyberspace, safety, risks

Aneta Waloch

Studentka Lotniczej Akademii Wojskowej w Dęblinie na kierunku bezpieczeństwo narodowe. Obszary zainteresowań naukowych: bezpieczeństwo państwa, bezpieczeństwo międzynarodowe. Czynna działaczka Koła Naukowego Studentów Bezpieczeństwa Narodowego. E-mail: aneta.waloch@o2.pl