Jerzy Zawisza
Społeczna Akademia Nauk w Warszawie
e-mail: jerzyzawisza19@wp.pl

JOURNAL OF MODERN SCIENCE TOM 4/27/2015, S. 403–416

The cyberspace as the threat of the state security

Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa

Abstract

The development of teleinformatic technologies and the Internet causes coming into existence of new threats so as cybercrisises and cyberconflicts, cyberviolence, cberprotesty, whether cyberdemonstrations about destructive character disrupting the accomplishment of significant tasks of the Civil Service with the participation of national and nonnational entities, including threat of triggering the cyberwar. Progress in the teleinformatics caused, that cyberspace, is not only contributing to the development of national entities (non-government) whether individuals, but is also the source of considerable risks for their safety. Operations in the cyberspace constitute the integral part of classical crises and political-military conflicts today (of wars), in frames of their hybrid character. The cyberspace became a field of conflict, on which we are happening to stand up not only with other states, but also with hostile organizations about extremist, terrorist character. With strategic aim in the area of the cybersafety the Republic of Poland, providing safe functioning for the Republic of Poland is in the cyberspace, in it of appropriate security level of national teleinformatic systems – of especially a teleinformatic critical infrastructure of the state – as well as crucial for functioning of the society of private economic operators, in particular of sectors being a member: financial, energy and health cares. One should emphasize that the protection of the cyberspace became one of the subjects most often taken up concerning the safety.

Streszczenie

Rozwój technologii teleinformatycznych oraz Internetu prowadzi do powstawania nowych zagrożeń, takich jak cyberkryzysy i cyberkonflikty, cyberprzemoc, cyberprotesty czy cyberdemonstracje o charakterze destrukcyjnym, zakłócające realizację istotnych zadań administracji państwowej z udziałem podmiotów państwowych i niepaństwowych, w tym także groźba wywołania cyberwojny. Postęp w teleinformatyce sprawił, że cyberprzestrzeń nie tylko przyczynia się do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa. Operacje w cyberprzestrzeni stanowią dziś integralną część klasycznych kryzysów i konfliktów polityczno-militarnych (wojen), w ramach ich hybrydowego charakteru. Cyberprzestrzeń stała się polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami o charakterze ekstremistycznym, terrorystycznym czy zorganizowanymi grupami przestępczymi. Strategicznym celem w obszarze cyberbezpieczeństwa RP jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia. Należy zaznaczyć, że ochrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa.

Keywords: *cyberspace, cyberwar, cybercrisis, cyberconflict, critical infrastructure, chipping, backdoor – santas, cracking, the Trojan Horse, information environment, cyberthreat, nationalization of the cyberspace*

Słowa kluczowe: *cyberprzestrzeń, cyberwojna, cyberkryzys, cyberkonflikt, infrastruktura krytyczna, chipping, backdoor – santas, cracking, koń trojański, środowisko informacyjne, cyberzagrożenie, nacjonalizacja cyberprzestrzeni*

Wprowadzenie

Państwa i organizacje międzynarodowe, a także inni aktorzy niepaństwowi zrozumieli, że stabilność funkcjonowania i rozwój globalnego społeczeństwa informacyjnego są uzależnione od otwartej, niezawodnej i przede wszystkim bezpiecznej cyberprzestrzeni. Ogólnoświatowy zasięg oraz możliwość natychmiastowego dostępu z niemal dowolnego miejsca na Ziemi sprawiły, że coraz więcej podmiotów (rządów, instytucji i firm), a także osób indywidualnych

decyduje się przenosić różne elementy swojej codziennej aktywności do cyberprzestrzeni. Internet stał się jednym z podstawowych mediów, synonimem wolności słowa i nieskrępowanego przepływu informacji, a w pewnych przypadkach z powodzeniem służy jako narzędzie rewolucji i zmian społecznych.

Terminologia i istota cyberprzestrzeni

Termin „cyberprzestrzeń" (ang. *cyberspace*) został użyty po raz pierwszy w 1984 roku przez W. Gibsona w powieści *Burning Chrome*. Wygenerowany przez komputer świat wirtualnej rzeczywistości stał się szczególną matrycą (*matrix*), inaczej przestrzenią komunikowania tworzoną przez system powiązań internetowych (Blair, D.C. 2011, s. 2). Cyberprzestrzeń w dzisiejszym rozumieniu to przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie jako synonim Internetu. Według Pierre'a Levy'ego cyberprzestrzeń ma charakter „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny. To nowe środowisko umożliwia współdziałanie poprzez łączenie wszystkich narzędzi tworzenia informacji, rejestrowania, komunikacji i symulacji, przez co stało się głównym kanałem informacyjnym i głównym nośnikiem pamięciowym ludzkości".

Kiedy w połowie lat 80. nad zatoką San Francisco powstawał WALL (*Whole Earth Lectronie Link*), nikt nie przypuszczał, że tak szybko na świecie nastąpi rozwój sieci komputerowych. Stworzyły one cyberprzestrzeń o nieograniczonych możliwościach komunikacyjnych. Rozwój ten w istotny sposób wpłynął na stworzenie środowiska społecznego wywierającego coraz większy wpływ na edukację. Jak nietrudno zauważyć, wokół człowieka wyrósł i rozszerzył się nieznany dotąd świat kultury, nauki, zabawy, komunikacji i społecznych relacji. Zjawiska te powodują istotne zmiany zarówno w procesie edukacji, jak i w postawach jej uczestników (Białoskórski, 2011, s. 15–16). Umiejętność funkcjonowania w przestrzeni rzeczywistej i wirtualnej staje się niezbędna na każdym etapie życia człowieka. Możemy mówić o cyberprzestrzeni jako miejscu publikacji, inwigilacji, kontroli i co ważniejsze – uzależnienia od zniewolenia.

Środowisko cyberprzestrzeni

Cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa, co pociąga za sobą konieczność dokonania licznych zmian zarówno w pragmatyce, jak i w prawnoorganizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa na świecie. Cyberprzestrzeń ukształtowały następujące procesy:

- proces integracji podstawowych form przekazu i prezentacji informacji- (*data* + *texts* + *pictures* + *voices* + *movies*), który przyniósł multimedialność, ucyfrowienie infosfery i ikonosfery,
- proces konwergencji ICT (*Information Communication Technologies*): systemów informatycznych, systemów telekomunikacyjnych i mediów elektronicznych,
- proces integracji technosfery, który ukształtował globalną zintegrowaną platformę teleinformatyczną.

Jak każde niemal zjawisko, wywołane rewolucją technologiczną w drugiej połowie XX wieku, także cyberprzestrzeń ma zarówno swoją jasną, jak i ciemną stronę. Cyberprzestrzeń jest obszarem zarówno kooperacji pozytywnej, jak i kooperacji negatywnej. Ta pierwsza oznacza wzrost możliwości wszechstronnego zaspokojenia potrzeb społecznych, w tym potrzeby samorozwoju (samorealizacji), we wszystkich dziedzinach życia, a mianowicie w sferze:

- edukacji: dzięki zwiększonym i ułatwionym możliwościom korzystania z globalnych zasobów danych, informacji i wiedzy (Europejska Przestrzeń Edukacyjna),
- badań naukowych: dzięki wzrostowi zasobów wiedzy i wspomagania badań (Europejska Przestrzeń Badawcza),
- komunikacji: dzięki rozwojowi sieci komunikacji społecznej w niespotykanej dotąd skali globalnej,
- ekonomii: dzięki rozwojowi różnych form „e-biznesu" i powstaniu tzw. gospodarki opartej na wiedzy,
- kultury: dzięki niemal nieograniczonemu dostępowi do zasobów wirtualnej ikonosfery,
- ludycznej: powstała arena globalnych igrzysk, gier i zabaw,
- bezpieczeństwa: dzięki zwiększonej sprawności służb nastąpił wzros bezpieczeństwa obywateli, jednakże kosztem utraty części wolności.

Niestety, „ciemna strona" oznacza, że cyberprzestrzeń stała się niebezpieczna, okazując się źródłem zagrożeń dla bezpieczeństwa zewnętrznego (międzynarodowego) i wewnętrznego (narodowego). Możemy mieć do czynienia z następującymi zjawiskami:

- cyberprzestępstwa, czyli wykorzystania cyberprzestrzeni do celów kryminalnych, zarówno przestępstw pospolitych, jak i zorganizowanych,
- cyberinwigilacji, czyli wykorzystania cyberprzestrzeni w celach kontroli społecznej (np. identyfikacja lokalizacji, częstości korzystania z ICT, treści przekazów itd.),
- cyberterroryzmu, czyli działań terrorystycznych w cyberprzestrzeni,
- cyberszpiegostwa, to jest działań wywiadowczych polegających na zbieraniu informacji stanowiących tajemnicę i przekazywaniu ich organom wywiadowczym,
- cyberwojny, czyli wykorzystania cyberprzestrzeni w działaniach wojennych lub w operacjach innych niż wojna (Sienkiewicz, Świeboda, 2010, s. 29–30).

Coraz szersze zagospodarowanie cyberprzestrzeni może stwarzać ryzyko braku akceptacji społecznej dla racjonalnego określenia granicy między wolnością osobistą i ochroną praw jednostki w świecie wirtualnym a stosowaniem środków służących zapewnieniu akceptowalnego poziomu bezpieczeństwa, co może powodować trudności we wprowadzaniu nowych, efektywnych systemów bezpieczeństwa w cyberprzestrzeni.

Ochrona cyberprzestrzeni

Rządowy obowiązujący program ochrony cyberprzestrzeni RP na lata 2009–2011 definiuje pojęcie cyberprzestrzeni państwa jako „(…) przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest też mianem cyberprzestrzeni RP. Cyberprzestrzeń RP obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu,

łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne" (Sienkiewicz, 2010, s. 28). Rządowy program ochrony cyberprzestrzeni na lata 2011–2016 jest obecnie w trakcie uzgodnień resortowych (ROOCRP). W tym kontekście szczególnie istotne jest zrozumienie dynamiki zmian tego środowiska. Ochrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa. Państwa, organizacje międzynarodowe i inni aktorzy niepaństwowi zrozumieli, że stabilność funkcjonowania i rozwój globalnego społeczeństwa informacyjnego są uzależnione od otwartej, niezawodnej i przede wszystkim – bezpiecznej cyberprzestrzeni. Podnoszenie świadomości w tym zakresie idzie w parze z gwałtownym wzrostem liczby incydentów komputerowych i nowych rodzajów zagrożeń. Polska również jest obiektem ataków cybernetycznych. Podobnie jak inne państwa, stoi przed wyzwaniem, jakim jest wypracowanie zmian prawnych i organizacyjnych, pozwalających na zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli. Rozwojowi społeczeństwa informacyjnego, połączonemu z rozszerzaniem zasięgu Internetu, towarzyszy przenikanie kolejnych aspektów ludzkiej działalności do cyberprzestrzeni. Ogólnoświatowy zasięg oraz możliwość natychmiastowego dostępu z niemal dowolnego miejsca na Ziemi, w połączeniu z niewielkimi kosztami użytkowania, sprawiły, że coraz więcej podmiotów (rządów, instytucji i firm), a także indywidualnych osób decyduje się przenosić różne elementy swojej codziennej aktywności do cyberprzestrzeni. Wielu użytkowników Internetu nie wyobraża sobie życia bez szybkiego dostępu do najświeższych informacji i poczty elektronicznej, internetowej bankowości, zakupów online, elektronicznej rezerwacji biletów czy kontaktu z rodziną i znajomymi przez portale społecznościowe oraz internetowe komunikatory. Dostępny za pomocą komputerów, telefonów komórkowych, tabletów Internet stał się jednym z podstawowych mediów, synonimem wolności słowa i nieskrępowanego przepływu informacji, a w pewnych przypadkach z powodzeniem służy jako narzędzie rewolucji i zmian społecznych. Niestety, w czasie gdy cyberprzestrzeń staje się wirtualnym odzwierciedleniem fizycznej

rzeczywistości, przenikają do niej również negatywne formy ludzkiej działalności. Konstrukcja stworzonej z myślą o współpracy naukowej sieci internetowej daje duże poczucie anonimowości, wykorzystywana jest przez przestępców, terrorystów, a także niektóre państwa do prowadzenia nielegalnej działalności lub agresji wobec innych podmiotów. W dużej mierze wynika to z faktu, że ponad połowa użytkowników nie posiada aktualnego oprogramowania zabezpieczającego systemy komputerowe. Motywacją do działania większości cyberprzestępców jest zazwyczaj chęć zysku, przykładem są tu tzw. haktywiści, którzy w dążeniu do osiągnięcia celów ideowych dopuszczają się np. kradzieży i niszczenia wrażliwych danych bądź utrudniają do nich dostęp (Domański, 2013, s. 69–71). Cyberprzestrzeń jest wykorzystywana również przez terrorystów jako narzędzie prowadzenia motywowanej politycznie działalności. Z uwagi na kontrowersje i problemy z jasnym zdefiniowaniem pojęcia cyberterroryzmu trudno jednoznacznie zakwalifikować konkretne przykłady ataków jako efekt działalności terrorystów w cyberprzestrzeni. Wiele incydentów przypisywanych terrorystom może być formą wandalizmu, działaniem niejawnie sponsorowanym lub prowadzonym przy cichej akceptacji państwa, co jednak jest trudne do udowodnienia. Klasycznym przykładem są zmasowane cyberataki na infrastrukturę teleinformatyczną wielu państw czy instytucji, czego przykładem może być Estonia, gdzie w 2007 roku cyberataki doprowadziły do paraliżu państwa (Grzelak, Liedel, 2012, s. 127). Internet jest wykorzystywany przez terrorystów również jako narzędzie komunikacji, prowadzenia motywowanej politycznie działalności, w ich rękach jest także narzędziem koordynowania swoich działań, propagandy, dezinformacji, gromadzenia środków finansowych oraz werbowania członków. Używają oni globalnej sieci do koordynowania swoich działań, propagandy, dezinformacji, gromadzenia środków finansowych oraz werbowania członków. Ponadto za jej pośrednictwem udostępniane są materiały o charakterze typowo instruktażowym. Jedną z podstawowych funkcji Internetu jest uzyskiwanie informacji. Dlatego nie jest zaskoczeniem, że powszechnie stosowaną praktyką jest użycie cyberprzestrzeni do celów wywiadowczych, gdzie służby niektórych państw na szeroką skalę wykorzystują cyberprzestrzeń do zbierania danych wywiadowczych, szczególnie danych gospodarczych dotyczących nowoczesnych technologii, przemysłu obronnego, farmaceutycznego itp. Wiele mówi

się także o działaniach militarnych w cyberprzestrzeni, nazywanej kolejnym po lądzie, morzu, przestrzeni powietrznej i przestrzeni kosmicznej środowiskiem prowadzenia walki. Zarówno organizacje międzynarodowe, jak i państwa przyznają, iż konieczne jest rozwijanie zdolności obronnych w cyberprzestrzeni (Białoskórski, 2011, s. 47–48). Nie jest jednak tajemnicą, że niektóre kraje zdecydowały się również na rozwój zdolności ofensywnych, tworząc odpowiednie struktury w siłach zbrojnych, i prowadzą badania nad nowymi rodzajami „cyberbroni", budując w ten sposób własne zasoby odstraszania potencjalnych adwersarzy. Poza specjalnie wydzielonymi jednostkami działającymi w strukturach sił zbrojnych wybrane państwa korzystają również z usług płatnych ekspertów, którzy jako najemnicy lub członkowie „cybermilicji" realizują ofensywne i defensywne zadania w cyberprzestrzeni. Militaryzacja cyberprzestrzeni obejmuje również rozwój narzędzi służących walce w tym środowisku. Podnoszenie zdolności obronnych doprowadziło do znacznego uodpornienia na konwencjonalne cyberataki i spowodowało wzrost nakładów na tworzenie „cyberbroni" wykorzystywanych przez państwa do prowadzenia kierunkowych ataków.

Niejasności walki w cyberprzestrzeni

W kwestii walki w cyberprzestrzeni jest jeszcze wiele niejasności, m.in. natury prawnej. Kolejne państwa tworzą strategie dotyczące obrony, a także otwarcie mówią o możliwości ofensywy lub ataków odwetowych w cyberprzestrzeni, tylko nie wiadomo, jak dokładnie mógłby wyglądać przebieg takiego konfliktu. Nie jest jasne, czy atak w cyberprzestrzeni pociągnie za sobą konwencjonalne, tzn. militarne, działania odwetowe, a także jak środowisko międzynarodowe zareaguje w takiej sytuacji. Wiele mówi się o współpracy i kolektywnej obronie (Sienkiewicz, Świeboda, 2010, s. 75–77).

Kwestia obrony cyberprzestrzeni została ujęta w dwóch ostatnich deklaracjach przyjętych po szczytach NATO w 2010 i 2012 roku. Trudno jednak przewidzieć, czy np. atak cybernetyczny na jednego z członków sojuszu faktycznie uruchomi wszystkie mechanizmy związane z art. 5 traktatu waszyngtońskiego i jaka będzie skala ewentualnych działań w tym zakresie. Jedną z największych przeszkód stojących na drodze formalnoprawnego uregulowania kwestii bezpieczeństwa cyberprzestrzeni, zarówno na poziomie państwowym, jak i mię-

dzynarodowym, są trudności ze spójnym zdefiniowaniem terminów dotyczących tego zagadnienia. Problem stanowi nawet uzgodnienie definicji pojęcia samej cyberprzestrzeni. Centrum Doskonalenia Cyberobrony NATO w Tallinie (NATO *Cooperative Cyber Defence Centre of Excellence*, CCDCoE) proponuje definicję mówiącą, że cyberprzestrzeń jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami". Wspomniana instytucja zwraca uwagę na wielość definicji w tym obszarze. Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (*European Network and Information Security Agency,* ENISA) do jej realizowanych zadań zalicza:

- doradzanie Komisji i państwom członkowskim w zakresie bezpieczeństwa informacji oraz pomaganie im, w porozumieniu z odpowiednim sektorem, w rozwiązywaniu problemów z zakresu bezpieczeństwa sprzętu komputerowego i oprogramowania,
- gromadzenie i analizę danych dotyczących przypadków naruszania w Europie bezpieczeństwa w tych dziedzinach oraz analizę ryzyka, jakie w związku z tym powstaje,
- promowanie metod analizy oceny ryzyka oraz zarządzania ryzykiem w celu doprowadzenia do sprawniejszego reagowania na zagrożenia w dziedzinie bezpieczeństwa informacji,
- wymianę najlepszych bieżących praktyk w zakresie podnoszenia wiadomości i współpracy z równymi podmiotami działającymi w dziedzinie bezpieczeństwa informacji, w szczególności poprzez tworzenie partnerstw publiczno-prywatnych z udziałem przedsiębiorstw z tej branży,
- monitorowanie procesu opracowywania norm dla produktów i usług z dziedziny bezpieczeństwa sieci i informacji.

Wspomniana Agencja zaleca uzgodnienie jednolitych definicji pojęć z zakresu bezpieczeństwa cyberprzestrzeni, wokół których kraje Unii będą tworzyły narodowe strategie, wspomagając w ten sposób utrzymanie bezpieczeństwa cyberprzestrzeni na lokalnym i globalnym poziomie.

Kwestia cyberbezpieczeństwa, czyli bezpieczeństwa EPC, została podjęta na forum G8, a także przez Radę Europy w międzynarodowej konwencji dotyczącej przestępczości informatycznej w dniu 8 listopada 2001 r.

Do najważniejszych postanowień Konwencji Rady Europy należy zaliczyć:

- harmonizację narodowych systemów prawnych dotyczących zdefiniowania cyberprzestępstw,
- wypracowanie standardów prowadzenia postępowania karnego oraz procedur sądowych dostosowanych do zasad działania globalnej sieci teleinformatycznej,
- utworzenie szybkiego i skutecznego systemu współpracy międzynarodowej w zakresie bezpieczeństwa EPC (Sienkiewicz, Świeboda, 2010, s. 33).

Bezpieczeństwo cyberprzestrzeni w wymiarze instytucjonalnym

Ochrona sieci formacji zmilitaryzowanych

W Polsce nie dopracowano się w pełni skutecznego systemu reagowania na incydenty komputerowe. Należy stwierdzić, iż główną funkcję pełni w nim rząd, który za pomocą właściwych ministerstw, takich jak Ministerstwo Administracji i Cyfryzacji (MAiC), Ministerstwo Spraw Wewnętrznych (MSW), Ministerstwo Obrony Narodowej (MON), oraz służb, takich jak Agencja Bezpieczeństwa Wewnętrznego (ABW), Służba Kontrwywiadu Wojskowego (SKW), Służba Wywiadu Wojskowego (SWW), stara się przeciwdziałać zagrożeniom pojawiającym się w cyberprzestrzeni (Sulowski, Brzeziński, 2014, s. 258). Ministerstwa odgrywają zasadniczą rolę, jeśli chodzi o wypracowywanie odpowiednich rozwiązań koncepcyjnych, legislacyjnych czy politycznych. Tymczasem odpowiedzialność za praktyczne reagowanie na incydenty ciąży na wspomnianych służbach i strukturach, mających charakter zarówno cywilny, jak i wojskowy.

W 2008 roku powołano w Resorcie Obrony Narodowej System Reagowania na Incydenty Komputerowe, w ramach którego działają: Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi oraz Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Oprócz nich można wymienić także: Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe Departamentu Informatyki i Telekomunikacji MON, Departament Ochrony Informacji Niejawnych, Komendę Główną Żandarmerii Wojskowej oraz Zarząd Planowania Systemów Dowodzenia i Łączności Sztabu Generalnego WP (Sulowski, Brzeziński, 2014, s. 253).

Ochrona sieci cywilnych

W ochronie sieci cywilnych zasadniczą rolę odgrywają dwie struktury. Z jednej strony sieci administracji publicznej zabezpiecza Agencja Bezpieczeństwa Wewnętrznego (ABW), w ramach której funkcjonuje, utworzony 1 lutego 2008 r., Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Do jego zadań zalicza się zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Ponadto realizuje on jednocześnie zadania narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP. Z kolei strukturą odpowiedzialną za ochronę polskich sieci cywilnych jest funkcjonujący od 1996 roku CERT Polska, który działa w ramach Naukowej i Akademickiej Sieci Komputerowej, z którą CERT.GOV.PL utrzymuje ścisłe kontakty. Do kompetencji CERT Polska należy m.in.: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci, reagowanie na bezpośrednie zagrożenia dla użytkowników, udział w krajowych i międzynarodowych projektach związanych z bezpieczeństwem teleinformatycznym oraz działania informacyjno-edukacyjne. Warto dodać, że CERT Polska utrzymuje ożywione kontakty międzynarodowe, od 2000 roku należy do TERENA TFCSIRT (TERENA – *Trans-European Research and Education Networking Association*), a od 2010 roku do *Anti-Phishing Working Group* (Czornik, Łakomy, 2014, s. 428–433).

Co budzi lęk i obawy?

Po pierwsze – to, że świat ma problemy z jasnym zdefiniowaniem pojęcia cyberterroryzmu, wiele incydentów może być formą wandalizmu, prowadzone działania niejawnie sponsorowane lub prowadzone przy cichej akceptacji państwa są trudne do udowodnienia. Nie jest jednak tajemnicą, że niektóre kraje zdecydowały się na rozwój swoich zdolności ofensywnych – tworząc odpowiednie struktury w siłach zbrojnych i prowadząc badania nad nowymi rodzajami „cyberbroni", budują w ten sposób własne zasoby odstraszania potencjalnych przeciwników. Dla przykładu MON USA ustaliło, że „podejmowany przez inne państwo sabotaż komputerowy może stanowić akt wojny, co otwiera USA drogę do zareagowania na cyberatak

użyciem swoich Sił Zbrojnych". Stąd też kwestia obrony cyberprzestrzeni została ujęta w dwóch ostatnich deklaracjach przyjętych po szczytach NATO w 2010 i 2012 roku.

Po drugie – największą przeszkodą stojącą na drodze formalnoprawnego uregulowania kwestii bezpieczeństwa cyberprzestrzeni są trudności ze spójnym zdefiniowaniem terminów dotyczących tego zagadnienia. Troska i odpowiedzialność za utrzymanie bezpieczeństwa w cyberprzestrzeni nie mogą spoczywać wyłącznie na władzach, które część zobowiązań w tym zakresie powinny przenieść na barki społeczeństwa, sektora prywatnego i organizacji pozarządowych.

Po trzecie – bezpieczeństwo cyberprzestrzeni nie będzie możliwe bez rozbudowy systemów wczesnego ostrzegania przed atakami. Wdrożenie dodatkowych rozwiązań prewencyjnych i szczególnej ochrony kluczowych systemów teleinformatycznych, połączonych z ćwiczeniami, pozwoli uodpornić tę infrastrukturę na ataki cybernetyczne. Zapewnienie bezpieczeństwa cyberprzestrzeni nie będzie możliwe bez zaangażowania jak najszerszego grona użytkowników globalnej sieci, którzy świadomi niebezpieczeństw będą mogli przyczyniać się do ochrony tego środowiska (Sulowski, Brzeziński, 2014, s. 268).

Podsumowanie

Polska, jak inne państwa, stoi przed wyzwaniem, jakim jest wypracowanie zmian prawnych i organizacyjnych, pozwalających na zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli. Konieczne jest ciągłe kształcenie specjalistów od bezpieczeństwa teleinformatycznego i kadry urzędniczej. Należy racjonalizować programy kształcenia na wyższych uczelniach. Równolegle do wymienionych przedsięwzięć konieczne jest prowadzenie kampanii społecznej o charakterze edukacyjno-prewencyjnym, której celem będzie podnoszenie świadomości użytkowników w zakresie zagrożeń czyhających na nich w cyberprzestrzeni. Nie można zapominać, że choć zagrożenia w cyberprzestrzeni stanowią odmienną kategorię wyzwań legislacyjno-organizacyjnych, to problemy, które stwarzają, powinny wymuszać na strukturach państwowych ewolucję w stronę rozwiązań mniej hierarchicznych, a bardziej elastycznych zarówno w wymiarze społecznym, jak

i technologicznym, wraz z jej wszystkimi konsekwencjami. Należy z jednej strony zauważyć, że powszechny i wygodny dostęp do informacji i zapewnienie odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni są problemem, który nie da się rozwiązać *ad hoc*. Z drugiej strony zbyt restrykcyjne podejście do tego problemu może przynieść nieoczekiwane skutki od wcześniej założonych, uznanych za wartość szczególnej troski. W tym miejscu należy zadać pytanie – czy nadmierne działania prowadzące do ograniczania dostępu do informacji, rozbudowa cenzury czy nadmierna inwigilacja Internetu są celowe i przyniosą określony skutek? Warto też dodać, iż zagrożenia bezpieczeństwa cyberprzestrzeni mają charakter asymetryczny, zatem rozwijanie ofensywnego potencjału do walki w cyberprzestrzeni jest zasadne w trosce o żywotne interesy każdego państwa.

Literatura

Bączek, P. (2006). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*. Toruń, Wyd. Adam Marszałek. ISBN 8374413476.

BBN. (2013). *Biała Księga Bezpieczeństwa Narodowego RP*. Warszawa, BBN. ISBN 9788360846179.

Białoskórski, R. (2011). *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku, zarys problematyki*. Warszawa, Wydawnictwo Wyższej Szkoły Cła i Logistyki. ISBN 9788389226853.

Blair, D.C. (2011). *Annual Treat Assessment of the Intelligence Community for the Senate Select Committe on Intelligece*. Montreal, International Centre for the Prevention of Crime. ISBN 9782921916691.

Bógdał-Brzezińska, A., Gawrycki, M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego w świecie*. Warszawa, Wydawnictwo ASPRA-JR. ISBN 8388766597.

Castells, M. (2010). *Społeczeństwo w sieci*. Warszawa, PWN. ISBN 9788301162948.

Czornik, K., Lakomy, M. (2014). *Dylematy polityki bezpieczeństwa na początku drugiej dekady XXI wieku*. Katowice, Wydawnictwo UŚ. ISBN 9788393876020.

Domański, Z. (2013). *Zagrożenia w cyberprzestrzeni*. W: M. Such-Pyrgiel (red.), *Bezpieczeństwo społeczne w XXI wieku w ujęciu socjologicznym, pedagogicznym, prawnym i nauk o zarządzaniu*. Józefów, WSGE. ISBN 9788362753376.

Grzelak, M., Liedel, K. (2014). *Bezpieczeństwo w cyberprzestrzeni, zagrożenia i wyzwania dla Polski – zarys problemu*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego". Kraków, Wydawnictwo UE. Nr 2(926).

Kucharski, M. (2012). *Bezpieczeństwo dyscypliny w obszarze nauk społecznych*. Warszawa – Łódź, Wydawnictwo SAN. ISBN 9788362916528.

Liedel, K., Piasecka, P., Aleksandrowicz, T.R. (2014). *Sieciocentryczne bezpieczeństwo: wojna, pokój i terroryzm w epoce informacji*. Warszawa, Difin. ISBN 9788379302710.

Madej, M. (2009). *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw systemu międzynarodowego*. Warszawa, PISM. ISBN 9788389607713.

MAiC. (2014). *Polityka ochrony cyberprzestrzeni RP*. Warszawa. ISBN 9788362723058.

Pokruszyński, W. (2012). *Bezpieczeństwo, teoria i praktyka*. Józefów, WSGE. ISBN 9788362753154.

Rydlewski, G. (2011). *Decydowanie publiczne*. Warszawa, DW ELIPSA. ISBN 9788371510496.

Sienkiewicz, P. (2004). *Wizje i modele wojny informacyjnej*. Kraków. AGH. ISBN 8389388324.

Skrzypczak, J. (2014). *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2084–6991. R. 4, nr 7.

Sulowski, S., Brzeziński, M. (2014). *Trzy wymiary współczesnego bezpieczeństwa*. Warszawa, DW ELIPSA. ISBN 9788380170315.

Zawisza, J. (2015). *The Organization and Functioning of the Polish Security System for Cross – Border Crisis. Słupsk, ProPomerania*. ISBN 9788363680329.

Zięba, R. (2004). *Instytucjonalizacja bezpieczeństwa europejskiego*. Warszawa, WN. SCHOLAR. ISBN 8373830758.