Kultura Bezpieczeństwa
Nr 5/2016

Piotr Michałkiewicz

Cyberprzestrzeń a bezpieczeństwo narodowe

Cyberspace and national security

Streszczenie

Rozwój technologii informacyjno-komunikacyjnych doprowadził do powstania globalnej sieci informatycznej i utworzenia społeczeństwa informacyjnego. Spowodował powstanie tzw. cyberprzestrzeni. Mimo że pojęcie cyberprzestrzeni przeniknęło do wielu dziedzin życia, problem jego uregulowania w obszarze bezpieczeństwa narodowego stanowi niemałe wyzwanie. W artykule przedstawiono podstawowe zagadnienia dotyczące cyberprzestrzeni, przykłady zagrożeń z nią związanych i jej wpływ na regulacje dotyczące bezpieczeństwa narodowego.

Celem artykułu nie jest przedstawienie historii rozwoju regulacji dotyczących bezpieczeństwa narodowego, ale poprzez analizę tych regulacji pokazanie dojrzewania polskiej myśli strategicznej oraz podejścia do problematyki bezpieczeństwa narodowego z uwzględnieniem cyberprzestrzeni i związanych z nią zagrożeń.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, bezpieczeństwo narodowe

Abstract

The development of ICT has led to the emergence of a global information network and the creation of an information society. It gave rise to the so-called cyberspace. Although the concept of cyberspace has infiltrated into many areas of life, the problem of its regulation in the area of national security has been a considerable challenge. The paper pre-

sents the basic concept of cyberspace, examples of threats associated with it and its impact on regulations concerning national security.

The aim of the article is not to present the history of the development of regulations concerning national security, but to show the maturing Polish strategic thinking and approach to issues of national security with regard to cyberspace and the associated risks through the prism of the analysis of these regulations.

Keywords: cyberspace, cyber security, national security

Definicja cyberprzestrzeni

Co to jest cyberprzestrzeń? Jeszcze do niedawna pojęcie to było kojarzone z literaturą science-fiction. W 1982 r. William Gibson wprowadził ten termin do powszechnego obiegu, a jego definicję[1] według swojej wizji podał w 1984 r. Szybki rozwój technologii spowodował jednak przeniesienie tego terminu do „realnej" rzeczywistości i utożsamienie go przez społeczeństwo przede wszystkim z siecią globalną – Internet. Można powiedzieć, że powstanie Internetu, globalnej sieci informatycznej, doprowadziło do powstania globalnej wioski[2]. Przestały istnieć techniczne bariery komunikacyjne, a dostęp do informacji stał się powszechny. Szeroko pojęta globalizacja doprowadziła do zatarcia się granic państwowych w wielu obszarach życia, poczynając od obszaru gospodarczego, w szczególności finansowego, kończąc na społecznym. Termin cyberprzestrzeń zaczął funkcjonować w powszechnym użyciu,

[1] „To jest cyberprzestrzeń. Konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność…", William Gibson, *Neuromancer*, Wydawnictwo Zysk i S-ka, Warszawa 2001, s. 43.

[2] Globalna wioska – termin wprowadzony w 1962 przez Herberta Marshalla McLuhana w jego książce *The Gutenberg Galaxy (Galaktyka Gutenberga)*, opisujący trend, w którym masowe media elektroniczne obalają bariery czasowe i przestrzenne, umożliwiając ludziom komunikację na masową skalę. W tym sensie glob staje się wioską za sprawą elektronicznych mediów, 15.06.2016, https://pl.wikipedia.org/wiki/Globalna_wioska, [dostęp 02.03.2017 r.].

a cyberprzestrzeń zaczęła być postrzegana jako nowy obszar aktywności społecznej.

Należy jednak pamiętać, że z technologicznego punktu widzenia cyberprzestrzeń to nie tylko Internet. Można stwierdzić, że stanowi on system nerwowy cyberprzestrzeni – poza nim istnieją jednak systemy informatyczne, które połączone są innymi sieciami telekomunikacyjnymi. Mimo postrzegania cyberprzestrzeni jako medium komunikacji międzyludzkiej, należy również mieć na uwadze, że służy ona także do komunikacji pomiędzy systemami teleinformatycznymi bez udziału człowieka.

Biorąc powyższe pod uwagę, a także niezwykle szybko postępującą informatyzację wielu obszarów życia, m.in. podmiotów realizujących zadania publiczne, istotne stało się uregulowanie pojęcia cyberprzestrzeni. Tym bardziej, że termin ten, bez podania definicji, został użyty już w 2007 r. w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.

Pierwsza ustawowa[3] definicja cyberprzestrzeni została wprowadzona dopiero 30 sierpnia 2011 r. Wbrew społecznemu utożsamianiu cyberprzestrzeni z Internetem, ustawa zdefiniowała cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[4], odsyłając do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne w sprawie definicji systemu teleinformatycznego. Zgodnie z ustawą o informatyzacji system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za

[3] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw wprowadziła pojęcie cyberprzestrzeni do następujących ustaw: Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej oraz Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.

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

pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[5].

Wprowadzona ustawowo definicja cyberprzestrzeni powiązała ze sobą oba światy – obszar technologii oraz obszar społeczny. Ma ona jednak wymiar globalny. W ustawie pominięto definicję terminu cyberprzestrzeni Rzeczypospolitej Polskiej (RP), który to termin był już używany w oficjalnych dokumentach, np. w Rządowym programie ochrony cyberprzestrzeni RP na lata 2011-2016 z czerwca 2010 r. Program ten definiował cyberprzestrzeń RP jako cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)[6]. Strategia Bezpieczeństwa Narodowego RP z 2014 roku wspomina o cyberprzestrzeni RP, ale nie definiuje tego pojęcia. Dopiero w 2015 roku w Doktrynie cyberbezpieczeństwa RP pojawia się kolejna definicja cyberprzestrzeni RP uwzględniająca wymiar narodowy. Zgodnie z tą definicją cyberprzestrzeń RP, to nie tylko fragment cyberprzestrzeni w obrębie terytorium państwa polskiego, ale także miejsca, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji) [7].

W stosunku do definicji cyberprzestrzeni RP z programu rządowego definicja zawarta w doktrynie rozszerza cyberprzestrzeń RP o „przedstawicielstwa mobilne", czyli jednostki pływające oraz statki powietrzne poza przestrzenią RP.

Cyberprzestrzeń w dokumentach strategicznych

Powstanie cyberprzestrzeni otworzyło ogromne możliwości przed światem przestępczym, stając się ogromnym wyzwaniem dla bezpieczeństwa narodowego. Poniżej przedstawiam krótką charakterystykę przemian z punktu widzenia podejścia do cyberbezpieczeństwa w Polsce w kontekście regulacji.

[5] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565.
[6] Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, MSWiA, Warszawa 2010.
[7] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

Zacznę od 2003 roku i od Strategii Bezpieczeństwa Narodowego RP z tego roku. Dlaczego? Z historycznego punktu widzenia lata 80. to okres budowania sieci komputerowych oraz powstania Internetu. Na początku lat 90. powstaje sieć WWW oraz pierwsze przeglądarki internetowe. Za symboliczny start polskiego Internetu przyjmuje się datę 17 sierpnia 1991 r.[8], kiedy przesłano pierwszy pakiet danych z wykorzystaniem protokołu TCP/IP między Wydziałem Fizyki Uniwersytetu Warszawskiego a Centrum Komputerowym Uniwersytetu w Kopenhadze. Faktyczne włączenie Polski do globalnej sieci w ramach EARN (European Academic Research Network) nastąpiło 15 grudnia 1991 r., po zniesieniu przez Stany Zjednoczone ograniczeń w dostępie do nowoczesnych technologii komputerowych i telekomunikacyjnych m.in. dla Polski (embargo dotyczyło ogólnie krajów byłego bloku wschodniego). W 1990 r. została utworzona domena „pl". Kolejne: „gov.pl" i „org.pl" powstają w 1992 r. [9].

W wyżej wymienionym okresie, w obszarze bezpieczeństwa narodowego, można wskazać następujące dokumenty: Doktryna obronna RP z 1990 r., Założenia polskiej polityki bezpieczeństwa, Polityka bezpieczeństwa i strategia obronna RP z 1992 r. oraz Strategia Bezpieczeństwa RP z 2000 roku. Biorąc pod uwagę ówczesny rozwój technologii, dokumenty te nie uwzględniały zagrożeń związanych z cyberprzestrzenią.

Dopiero w Strategii Bezpieczeństwa Narodowego RP z 2003 r. zauważono, że coraz bardziej realne stają się dla Polski zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzeniem działań dezinformacyjnych. Szczególną uwagę zwrócono na zagrożenia związane z uzyskaniem nieuprawnionego dostępu do informacji niejawnych ze strony obcych służb spe-

[8] Zdania badaczy są podzielone. W artykule „Prawdziwy początek Internetu w Polsce" napisano, że pierwsze w Polsce łącze internetowe powstało w 1990 r. pomiędzy Instytutem Fizyki Jądrowej PAN w Krakowie a CERN (Międzynarodowy Ośrodek Badań Jądrowych) w Genewie, Komputerswiat.pl, 07.10.2011, http://www.komputerswiat.pl/nowosci/wydarzenia/2011/40/prawdziwy-poczatek-internetu-w-polsce-nieznany-fakt.aspx, [dostęp 08.03.2017].

[9] Dariusz Baran, *Internet w Polsce*, Oficyna Wydawnicza AFM, 2013 r., s. 76.

cjalnych, a także ugrupowań terrorystycznych, ekstremistycznych oraz zorganizowanych grup przestępczych. Strategia zakładała ochronę infrastruktury teleinformatycznej, czyniąc odpowiedzialnym za zwalczanie zagrożeń dla rządowych systemów i sieci teleinformatycznych wyspecjalizowane komórki cywilne i wojskowe służb państwowych. Ich zadaniem miało być zwalczanie przestępczości komputerowej wymierzonej w rządową i samorządową infrastrukturę telekomunikacyjną, w tym przeciwdziałanie atakom na jej elementy. Podjęte miały być wysiłki na rzecz rozwoju nowoczesnej łączności, w tym sprawnej i bezpiecznej strategicznej infrastruktury teleinformatycznej oraz zapewnienia warunków budowy społeczeństwa informacyjnego. Pojęcie cyberprzestrzeni nie było wówczas stosowane.

W kolejnej Strategii Bezpieczeństwa Narodowego RP z 2007 r. użyto pojęcia cyberprzestrzeni oraz przestępczości cybernetycznej. Nie zdefiniowano wówczas tych pojęć. W strategii stwierdzono, że jednym z zagrożeń dla Polski może być oddziaływanie w cyberprzestrzeni skierowane w systemy i sieci teleinformatyczne infrastruktury krytycznej, którego skutkiem mogą być zarówno straty materialne, jak i sparaliżowanie istotnych sfer życia publicznego. Założono także działania w zakresie rozwoju nowoczesnej, zintegrowanej struktury łączności elektronicznej, która byłaby odporna na awarie i potencjalne ataki przestępczości cybernetycznej. Innowacją było stwierdzenie, że rozwój w tym zakresie będzie wymagał wysiłku nie tylko ze strony odpowiednich służb państwowych, ale także współpracy podmiotów prywatnych.

W latach 2010-2012, z inicjatywy Prezydenta RP, przeprowadzony został Strategiczny Przegląd Bezpieczeństwa Narodowego[10]. Zadaniem przeglądu była całościowa ocena stanu bezpieczeństwa narodowego oraz sformułowanie wniosków dotyczących strategicznych celów i sposobów działania państwa w dziedzinie bezpieczeństwa oraz przygotowania systemu bezpieczeństwa narodowego.

Wyniki przeglądu zostały przedstawione w niejawnym Raporcie Strategicznego Przeglądu Bezpieczeństwa Narodowego, który w dniu

[10] Podstawę prawną Strategicznego Przeglądu Bezpieczeństwa Narodowego stanowiło Zarządzenie Nr 4 Prezydenta Rzeczypospolitej Polskiej z dnia 24 listopada 2010 r. w sprawie przeprowadzenia Strategicznego Przeglądu Bezpieczeństwa Narodowego. Zakres merytoryczny oraz sposób i tryb przeprowadzenia Przeglądu zostały określone w Zarządzeniu Nr 29/2010 Szefa Biura Bezpieczeństwa Narodowego z dnia 17 grudnia 2010 r.

8 listopada 2012 r. został przyjęty przez Radę Bezpieczeństwa Narodowego. W jawnym dokumencie przedstawiającym główne wnioski i rekomendacje z przeglądu[11] Biuro Bezpieczeństwa Narodowego zwróciło uwagę m.in. na zagrożenia terrorystyczne i ich przeniesienie do cyberprzestrzeni (cyberterroryzm).

Na podstawie powyższego raportu 23 maja 2013 r. została opublikowana Biała Księga Bezpieczeństwa Narodowego, która adresowana była do wszystkich Polaków, a jej celem było spełnienie obowiązku rzetelnego informowania o sprawach dotyczących bezpieczeństwa. Poza stwierdzeniem, że aktywność terrorystów przenosi się do cyberprzestrzeni w Białej Księdze Bezpieczeństwa Narodowego pojawiła się bardzo istotna informacja – stwierdzono, że cyberprzestrzeń w coraz większym stopniu będzie się stawać obszarem rywalizacji i konfrontacji między państwami. Stwierdzono także, że jednym z najważniejszych wyzwań w dziedzinie bezpieczeństwa pozamilitarnego dla Polski będzie konieczność zapewnienia bezpieczeństwa w cyberprzestrzeni.

W dniu 4 września 2013 r. został powołany Międzyresortowy Zespół do spraw Opracowania Strategii Bezpieczeństwa Narodowego RP, który przystąpił do prac nad nową strategią, opierając się m.in. na wynikach Strategicznego Przeglądu Bezpieczeństwa Narodowego. Nową, obowiązującą obecnie Strategię Bezpieczeństwa Narodowego Prezydent RP zatwierdził 5 listopada 2014 r.

Strategia Bezpieczeństwa Narodowego RP z 2014 r. składa się z wstępu, czterech rozdziałów i zakończenia. Rozdział pierwszy przedstawia umiejscowienie Polski w Europie i w świecie, określa interesy narodowe i cele strategiczne w dziedzinie bezpieczeństwa oraz opisuje budowę systemu bezpieczeństwa narodowego, dzieląc go na podsystem kierowania oraz podsystemy wykonawcze. Podsystem kierowania tworzą organy władzy publicznej i kierownicy jednostek organizacyjnych, wykonujący zadania związane z bezpieczeństwem narodowym, wraz z organami doradczymi i aparatem administracyjnym oraz procedurami funkcjonowania i stosowną infrastrukturą. W tym miejscu należy wspomnieć, że istotnym elementem podsystemu kierowania bezpieczeństwem narodowym jest zarządzanie kryzysowe. Podsystemy wykonawcze to siły i środki przewidziane do realizacji zadań w obszarze bezpieczeństwa

[11] Strategiczny Przegląd Bezpieczeństwa Narodowego, Główne Wnioski i Rekomendacje Dla Polski, Biuro Bezpieczeństwa Narodowego, Warszawa 2012.

narodowego, pozostające w dyspozycji organów kierowania bezpieczeństwem. W ramach podsystemów wykonawczych można wyróżnić podsystemy operacyjne (obronny i ochronne) oraz podsystemy wsparcia (społeczne i gospodarcze). W tym rozdziale jako jeden z celów strategicznych w dziedzinie bezpieczeństwa wskazano zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni.

Rozdział drugi przedstawia środowisko bezpieczeństwa Polski w wymiarze globalnym, regionalnym oraz krajowym. Odniesiono się w nim do znaczenia bezpieczeństwa w cyberprzestrzeni. Zwrócono uwagę, że wraz z rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych oraz cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Zauważono także, że obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju oraz to, że konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw.

Rozdział trzeci prezentuje strategię operacyjną, określa główne kierunki działań w sferze bezpieczeństwa z podziałem na działania obronne, ochronne oraz w sferze bezpieczeństwa społecznego i gospodarczego. Szczególnie istotny zapis tego rozdziału wskazuje cyberprzestrzeń jako kolejne środowisko walki zbrojnej. Zakłada się, że Siły Zbrojne RP muszą być gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny. Zwrócono także uwagę na współpracę i koordynację działań ochronnych, w odniesieniu do zagrożeń w cyberprzestrzeni, z podmiotami sektora prywatnego, przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej.

Rozdział czwarty przedstawia strategię preparacyjną dla wszystkich wymienionych wyżej podsystemów, obejmującą zasady i sposoby przygotowania, stosownie do wymagań wynikających ze strategii operacyjnej. W rozdziale tym zwrócono uwagę m.in. na konieczność rozwijania w Siłach Zbrojnych RP zdolności do działań w cyberprzestrzeni, w tym stworzenie mechanizmów cyberobrony i wzmocnienie dedykowanych jej jednostek. Wskazano także na potrzebę wdrożenia i rozwijania systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym oraz konieczność budowy na-

rodowego systemu obrony cybernetycznej, m.in. Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej oraz narodowego ośrodka koordynacji, wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymiany informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa.

Biorąc pod uwagę obszar społeczny, wbrew pozorom bardzo istotny, strategia zakłada zwiększanie świadomości społeczeństwa w obszarze zagrożeń w cyberprzestrzeni poprzez intensyfikację działań edukacyjnych, kampanii społecznych oraz rozwijanie programów badawczych w tym obszarze.

Na bazie postanowień Strategii Bezpieczeństwa Narodowego RP, a także zapisów Polityki ochrony cyberprzestrzeni RP[12] oraz Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń w dniu 22 stycznia 2015 r. ujrzała światło dzienne Doktryna cyberbezpieczeństwa RP. Doktryna jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego RP. Określa cele w dziedzinie cyberbezpieczeństwa, opisuje środowisko, wskazując na zagrożenia, ryzyka i szanse, a także rekomenduje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa[13].

Cyberzagrożenia

Wraz z pojawieniem się cyberprzestrzeni pojawiły się nowe zagrożenia. Cyberprzestrzeń stała się po prostu kolejnym obszarem działania przestępców. Powstało wiele terminów związanych z prowadzeniem określonych działań w cyberprzestrzeni. Zdefiniowanie tych pojęć nie jest łatwe, a poszczególne instytucje podają różne definicje. Nie ulega wątpliwości, że ujednolicenie ich pomogłoby określić odpowiednie działania mitygujące, które należy podjąć zarówno w obszarze krajowym, jak i europejskim.

[12] Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej stanowi załącznik do uchwały nr 111 Rady Ministrów z dnia 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.

[13] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

W Białej Księdze Bezpieczeństwa Narodowego RP jako powszechne wymieniono zagrożenia związane z cyberprzestępczością i cyberterroryzmem. Wspomniano także o cyberprotestach i cyberdemonstracjach, które stają się coraz istotniejszą formą wyrażania dezaprobaty społecznej. Zwrócono także uwagę na cyberprzemoc, cyberszpiegostwo, cyberkonflikty oraz cyberwojnę.

W przypadku Strategii Bezpieczeństwa Narodowego RP z 2014 r. poza cyberprzestępczością wyróżniono dodatkowo następujące zagrożenia: cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojnę, rozumianą jako konfrontację w cyberprzestrzeni między państwami[14].

Doktryna cyberbezpieczeństwa RP jako dokument koncepcyjny oraz wykonawczy w stosunku do strategii wyróżnia dwa wymiary bezpieczeństwa – wymiar wewnętrzny oraz wymiar zewnętrzny.

W ramach wymiaru wewnętrznego stwierdza wręcz, że wszystkie tradycyjne wewnętrzne zagrożenia bezpieczeństwa mogą znajdować odpowiedniki w cyberprzestrzeni, wymieniając cyberprzestępczość, cyberprzemoc, cyberprotesty czy cyberdemonstracje o charakterze destrukcyjnym, zakłócające realizację istotnych zadań administracji. Wśród zagrożeń szczególnie istotnych wymienia zagrożenia dotyczące infrastruktury krytycznej państwa, sterowanej za pomocą systemów informatycznych, np. systemy komunikacji (łączności) zapewniające sprawne funkcjonowanie podsystemu kierowania bezpieczeństwem narodowym, podsystemu obronnego i podsystemów ochronnych, a także podsystemów wsparcia (gospodarczego i społecznego). Innowacją, która znalazła się w Doktrynie cyberbezpieczeństwa RP jest wskazanie zagrożeń istotnych z punktu widzenia pojedynczej osoby, które dotyczą kradzieży tożsamości oraz przejmowania kontroli nad prywatnymi komputerami.

W wymiarze bezpieczeństwa zewnętrznego do nowych zagrożeń doktryna zalicza cyberkryzysy z udziałem podmiotów państwowych i niepaństwowych, stwierdzając, że stanowią one integralną część klasycznych kryzysów i konfliktów polityczno-militarnych (wojen), w ramach ich hybrydowego charakteru.

Biorąc pod uwagę ograniczoną objętość artykułu, skupię się tylko na pojęciu cyberprzestępczości. Przedstawione do tej pory dokumenty nie zawierały precyzyjnej definicji cyberprzestępczości. Biała Księga

[14] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 r., s. 19.

Bezpieczeństwa Narodowego scharakteryzowała termin cyberprzestępczość poprzez wyliczenie związanych z nim zagrożeń: oszustwa i fałszerstwa komputerowego, wyłudzenia informacji, kradzieży lub zniszczenia danych i informacji, szpiegostwa gospodarczego, naruszenia praw autorskich, pornografii dziecięcej oraz hazardu[15].

Jak już wcześniej pisałem Doktryna cyberbezpieczeństwa RP z 2015 roku została oparta m.in. na Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. W przeciwieństwie do strategii europejskiej w doktrynie nie zamieszczono wyjaśnienia pojęcia cyberprzestępczość.

Według strategii europejskiej cyberprzestępczość odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Cyberprzestępczość obejmuje tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w Internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług/systemów oraz złośliwe oprogramowanie)[16].

Można powiedzieć, że cyberprzestępczość stała się podstawowym obszarem działania zorganizowanych grup przestępczych. Dotyka ona nie tylko pojedynczych osób, ale także przedsiębiorstw i państw. Poniżej przedstawiam kilka spektakularnych cyberataków z ostatnich lat.

Blokada Estonii

W 2007 r. władze Estonii podjęły decyzję o przeniesieniu pomnika żołnierzy radzieckich z centrum Tallina na cmentarz wojskowy. Doprowadziło to do protestów Moskwy oraz zamieszek mniejszości rosyjskiej, w wyniku których 1300 osób zostało aresztowanych, 100 osób

[15] Biała Księga Bezpieczeństwa Narodowego RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, s. 118.

[16] Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, 2013 r., http://www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf, [dostęp 02.03.2017 r.].

zostało rannych, a jedna osoba została zabita[17]. Kryzys ten rozpętał falę ataków DDoS (Distributed Denial of Service), które przeprowadza się przy użyciu wielu komputerów, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania. W określonym momencie komputery te wykonują jednoczesny atak poprzez zasypanie atakowanego systemu żądaniami wykonania usługi, którą ten system realizuje. Przy odpowiednio dużej liczbie atakujących komputerów doprowadza to do wyczerpania zasobów atakowanego systemu i do zablokowania jego działania.

Choć ataki trwały trzy tygodnie, od 27 do 18 kwietnia, dla zwykłego Estończyka były raczej frustrujące niż niebezpieczne, np. brak dostępu do usług bankowych. Dotkliwiej cyberataki odczuły instytucje państwa. Estoński system obrony musiał na kilka dni zamknąć część połączeń zagranicznych, w efekcie izolując kraj od reszty świata. Cybernetyczne „oblężenie" uniemożliwiło też Estończykom podróżującym za granicę dostęp do ich kont bankowych, a zagraniczne biura podróży organizujące wycieczki do Estonii nagle odkryły, że ich system rezerwacji przestał funkcjonować. Kiedy przestawały działać strony rządowe, informowanie obywateli o rozwoju sytuacji także stawało się trudniejsze, stwarzając ryzyko wybuchu paniki – na co prawdopodobnie liczyli napastnicy[18].

Estonia stanowi prawdopodobnie najbardziej spektakularny przykład działań w cyberprzestrzeni, który przytaczany jest w ostatnich latach. Atak ten stanowi przykład działań wymierzonych nie w przypadkową grupę ludzi lub przedsiębiorstw, ale w całe państwo. Mimo że nie udowodniono, że za atakami na Estonię stał rosyjski rząd, to przypadek Estonii stanowi przykład działań wojennych w cyberprzestrzeni, krótko mówiąc – cyberwojnę.

Gruzja – atak hybrydowy

Ciekawym przykładem powiązania działań w cyberprzestrzeni z działaniami w tzw. świecie „realnym" jest cyberatak na Gruzję,

[17] Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, 17.05.2007, The Guardian, https://www.theguardian.com/world/2007/may/17/topstories3.russia, [dostęp 01.03.2017].
[18] Jussi Jalonen, *Dni, które wstrząsnęły Estonią*, „Tygodnik Powszechny", 12.05.2009, https://www.tygodnikpowszechny.pl/dni-ktore-wstrzasnely-estonia-136573, [dostęp 3.03.2017 r.].

który towarzyszył wojnie pomiędzy Gruzją a Federacją Rosyjską. W 2008 r. gruzińska infrastruktura IT została zaatakowana prawie w tym samym czasie, kiedy rosyjskie wojska zbliżały się do Tbilisi. 20 lipca niektóre rządowe strony zostały podmienione. Po tym nastąpiły ataki DDoS, pojawiły się sfałszowane komunikaty BBC i CNN, które w rzeczywistości infekowały komputery, a potem nastąpiły dalsze ataki. Atakowane były głównie serwisy rządowe, ale nie tylko. Również strony banków czy ambasad wspierających Gruzję państw. Ataki były koordynowane przez serwisy, które miały powiązanie z podziemiem internetowym, prowadzącym przestępczą działalność w Internecie. Podobnie jak w przypadku Estonii związki pomiędzy Moskwą a rosyjskim podziemiem internetowym są oficjalnie tylko domysłem, bo nie ma na nie dowodów. Odnajdywane powiązania pomiędzy środowiskiem przestępczym a środowiskiem rządowym były komentowane przez Rosjan jako przypadkowe[19].

Atak na Bundestag

Jednym z ostatnich medialnych ataków, jeżeli można tak to określić, był atak w czerwcu 2015 r. na Bundestag. W jego wyniku przestępcy przejęli kontrolę nad siecią komputerową Bundestagu oraz wykradli tajne dokumenty należące do amerykańskiej Narodowej Agencji Bezpieczeństwa (NSA), które były przechowywane w siedzibie Bundestagu z powodu śledztwa prowadzonego wspólnie przez niemieckie i amerykańskie agencje bezpieczeństwa. Śledztwo dotyczyło udostępnienia przez Edwarda Snowdena tajemnicy państwowej oraz przedstawienia przez niego dokładnych mechanizmów działania służb wywiadowczych wobec obywateli w różnych krajach[20].

Polska cyberprzestrzeń także nie jest pozbawiona działań przestępczych, o czym mogą świadczyć poniższe, najbardziej nagłośnione przez media, przypadki.

---

[19] *Gruzja – Rosja – konflikt w cyberprzestrzeni*, Fundacja bezpieczna cyberprzestrzeń, 14.11.2011, https://www.cybsecurity.org/gruzja-rosja-konflikt-w-cyberprzestrzeni/, [dostęp 03.03.2017].

[20] *Rosjanie przygotowują się do kolejnego ataku na Bundestag*, cyberdefence24.pl, 13.12.2016, http://www.cyberdefence24.pl/508172,rosjanie-przygotowuja-sie-do-kolejnego-ataku-na-bundestag, [dostęp 03.03.2017].

Atak DDoS na LOT

21 czerwca 2015 r. przez około 4 godziny Polskie Linie Lotnicze LOT nie wykonywały zaplanowanych rejsów z portu lotniczego im. Fryderyka Chopina w Warszawie. Jako przyczynę podano początkowo awarię jednego z systemów, po czym poinformowano, że naziemne systemy IT stały się „przedmiotem ataku teleinformatycznego". Według kolejnych informacji przyczyną problemów był najprawdopodobniej atak DDoS, którego skutkiem był brak możliwości komunikacji z Eurocontrol (European Organisation for the Safety of Air Navigation/Europejska Organizacja ds. Bezpieczeństwa Żeglugi Powietrznej). W efekcie niemożliwe było przesyłanie planów lotu, bez których rejsy nie mogą się odbywać. Według zapewnień LOT w żaden sposób nie ucierpiały systemy wpływające na bezpieczeństwo pasażerów, w szczególności te zainstalowane w samolotach[21].

UKNF i polskie banki

W styczniu 2017 roku wykryto, że nieznani sprawcy uzyskali dostęp do stacji roboczych oraz serwerów w co najmniej kilku bankach i wykradli z nich dane. Zainfekowane zostały zarówno komputery pracowników, jak i serwery bankowe. Z przeprowadzonych analiz wynikało, że przestępcy mogli niezauważeni atakować wewnętrzne sieci banków od co najmniej kilku tygodni, a prawdopodobnie w niektórych przypadkach nawet od jesieni 2016 r. Stwierdzono, że pierwotnym sposobem ataku było złośliwe oprogramowanie umieszczone na serwerze Urzędu Komisji Nadzoru Finansowego[22].

Przypadki te nie są jedyne. Stały się bardzo medialne ze względu na istotną infrastrukturę krytyczną. Liczba cyberprzestępstw ciągle rośnie, co pokazują dane z raportu CERT.GOV.PL[23], który w 2015 roku zarejestrował łącznie 16.123 zgłoszeń, z których aż 8.914 zostało zakwa-

[21] Krajobraz bezpieczeństwa polskiego Internetu 2015, Raport roczny z działalności CERT Polska, NASK, 2016 r.

[22] *Techniczna analiza scenariusza przebiegu ataku na polskie banki*, Zaufana Trzecia Strona, 16.02.2017, https://zaufanatrzeciastrona.pl/post/techniczna-analiza-scenariusza-przebiegu-ataku-na-polskie-banki/, [dostęp 03.03.2017].

[23] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL.

lifikowanych jako faktyczne incydenty. Dla porównania w 2014 roku odnotowano 12.017 zarejestrowanych zgłoszeń, z czego 7.498 zostało zakwalifikowanych jako faktyczne incydenty.

Cyberbezpieczeństwo

Biorąc pod uwagę powyższe przykłady, można pokusić się o stwierdzenie, że wokół Polski zaciska się cybernetyczna pętla. Miejmy nadzieję, że Polska nie będzie teatrem tak spektakularnych działań. Można zadać pytanie czy cyberprzestrzeń jest w Polsce chroniona? Z tym pytaniem zmierzyła się w ostatnich latach Najwyższa Izba Kontroli, która przeprowadziła kontrolę realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[24] oraz kontrolę zapewnienia bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych[25].

Głównym celem pierwszej kontroli było sprawdzenie, w jaki sposób administracja państwowa zarządza ryzykiem związanym z zagrożeniami występującymi w cyberprzestrzeni RP. Jako cele cząstkowe wskazano następujące zagadnienia: opracowanie spójnego systemu działań organów administracji państwowej, mających na celu monitorowanie zagrożeń występujących w cyberprzestrzeni RP, przeciwdziałanie im oraz minimalizowanie skutków incydentów, funkcjonowanie w Polsce rozwiązań instytucjonalno-prawnych zapewniających skuteczne szacowanie ryzyk związanych z zagrożeniami występującymi w cyberprzestrzeni oraz sprawdzono czy obowiązujące obecnie regulacje prawne oraz działania realizowane przez podmioty państwowe w zakresie bezpieczeństwa systemów teleinformatycznych są spójne, kompletne oraz odwołują się do uznanych międzynarodowych wzorów dobrych praktyk. Z raportu wynika, że do czasu kontroli administracja państwowa nie podjęła niezbędnych działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski, a bezpieczeństwo Polski w dalszym ciągu jest postrzegane jedynie w sposób konwencjonalny, tzn. jako dzia-

[24] Informacja o wynikach kontroli: Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Nr ewid. P/14/043, NIK, 2015.

[25] Informacja o wynikach kontroli: Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych, nr ewid. P/15/042, NIK, 2016.

łania z zakresu zapobiegania i reagowania na tradycyjne zagrożenia, takie jak: powodzie, pożary, akty terroru z wykorzystaniem przemocy fizycznej, tradycyjne konflikty zbrojne itd.

Działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji państwowej. W rezultacie:

- nie podjęto spójnych i systemowych działań, mających na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów;
- nie oszacowano ryzyk dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne;
- nie określono struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań;
- nie przygotowano procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią.

Zgodnie ze stanowiskiem NIK należy mieć na uwadze, że powyższa kontrola i wynikająca z niej ocena dotyczyły systemowych działań w zakresie ochrony cyberprzestrzeni RP, natomiast nie dotyczyły stanu bezpieczeństwa teleinformatycznego poszczególnych podmiotów ani wykorzystywanych przez nie systemów. Biorąc to pod uwagę, NIK postanowiła dokonać kontroli w tym obszarze.

Celem drugiej kontroli było sprawdzenie czy w kontrolowanych jednostkach zapewnione jest bezpieczeństwo danych gromadzonych w systemach przeznaczonych do realizacji istotnych zadań publicznych. W ramach celów cząstkowych badano m.in. czy: prowadzone jest zarządzanie bezpieczeństwem IT, wdrożono plany zapewnienia bezpieczeństwa IT, testuje się, nadzoruje i monitoruje bezpieczeństwo IT, zdefiniowano incydenty związane z bezpieczeństwem IT, zarządza się kluczami kryptograficznymi, wdrożono ochronę przed złośliwym oprogramowaniem, jego wykrywanie i dystrybucję poprawek, zapewniono bezpieczeństwo sieciowe, a także czy zarządza się tożsamościami i kontami

użytkowników oraz czy chroni się technologie zabezpieczeń i wrażliwe dane.

Kontrolą objęto sześć instytucji realizujących ważne zadania publiczne, a w każdej z nich wybrano jeden z istotnych systemów informatycznych i objęto go szczegółowym badaniem.

Z raportu wynika, że stopień przygotowania oraz wdrożenia systemu zapewnienia bezpieczeństwa informacji nie zapewniał akceptowalnego poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych. Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny. W większości zbadanych jednostek prace w tym obszarze dopiero zostały rozpoczęte i były na wstępnym etapie obejmującym opracowanie niezbędnych podstaw formalnych – polityk bezpieczeństwa i powiązanych z nimi szczegółowych procedur.

Innym zauważonym problemem, bardzo istotnym, był fakt, że główny ciężar zapewnienia bezpieczeństwa IT w kontrolowanych jednostkach spoczywał na koordynatorze ds. bezpieczeństwa, który jednak nie posiadał w praktyce kompetencji w zakresie zarządzania całym procesem. Często zadania te były realizowane jednoosobowo. Powoływano wprawdzie zespoły specjalistów lub zawierano umowy z wykonawcami zewnętrznymi, jednakże nie sporządzano niezbędnych analiz, czy usługi świadczone przez nich zaspakajają potrzeby jednostki w zakresie bezpieczeństwa.

Obydwie kontrole przeprowadzone przez NIK pokazały druzgocząco duże braki zarówno w sferze regulacyjnej, jak i wykonawczej. Z przeprowadzonych przez NIK działań pokontrolnych dotyczących pierwszej kontroli wynika, że przeprowadzona kontrola nie spowodowała istotnych zmian w działalności poszczególnych podmiotów w zakresie ochrony cyberprzestrzeni. Z otrzymanych przez NIK materiałów wynika wręcz, że pół roku po przekazaniu najważniejszym osobom w państwie druzgoczącej oceny działań związanych z bezpieczeństwem IT w poszczególnych podmiotach (MON, MSW, RCB, NASK, UKE, MAiC) występowały dokładnie te same zjawiska i problemy, które wypunktowano w dokumentacji pokontrolnej NIK. Za szczególnie niepokojący należy także uznać fakt, że w przypadku niektórych podmiotów (MON)

zmaterializowało się wskazywane przez NIK ryzyko pogorszenia warunków realizacji zadań związanych z ochroną cyberprzestrzeni[26].

Podsumowanie

Na zakończenie można zadać pytanie, czy zmiany, które dokonały się w przedstawionych regulacjach na przestrzeni analizowanych w artykule lat wpłynęły na kulturę bezpieczeństwa związaną z postrzeganiem cyberprzestrzeni w bezpieczeństwie narodowym. Biorąc pod uwagę, że kultura bezpieczeństwa to sposób myślenia o bezpieczeństwie i odczuwania bezpieczeństwa, a także sposoby osiągania bezpieczeństwa[27], trudno nie zauważyć tendencji rozwojowych. Wyróżniając trzy elementy kultury bezpieczeństwa – sferę kultury mentalnej, organizacyjnej i materialnej[28] – można stwierdzić, że zdecydowany rozwój nastąpił w sferze kultury mentalnej oraz organizacyjnej, biorąc pod uwagę zmiany w postrzeganiu cyberprzestrzeni i związanych z nią zagrożeń oraz zmiany w dokumentach strategicznych dotyczących bezpieczeństwa RP. Niestety sfera kultury materialnej, w szczególności zabezpieczenia techniczne, pozostawia wiele do życzenia. Potwierdzają to kontrole przeprowadzone przez NIK, które jednoznacznie pokazują, że przełożenie wytycznych na działanie nie jest proste.

*Mgr **Piotr Michałkiewicz** – absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie.*

[26] Paweł Gibuła, *Niebezpieczna cyberprzestrzeń – działania na rzecz bezpieczeństwa teleinformatycznego Polski*, „Kontrola państwowa" nr 4(369)/2016, NIK, s. 63
[27] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wydawnictwo Akademii Podlaskiej, Siedlce 2009, s. 157.
[28] Ibidem.