Studia Bobolanum 28
nr 3 (2017): 21-40

Polityka ochrony cyberprzestrzeni w państwie współczesnym

Zenon Trejnis

Papieski Wydział Teologiczny w Warszawie – Collegium Bobolanum
Warszawa

Przemysław Z. Trejnis

Uniwersytet Kardynała Stefana Wyszyńskiego
Warszawa

„Informacja to władza, a nowoczesna technologia informatyczna rozpowszechnia informację znacznie szerzej niż kiedykolwiek w historii”[1].

Polityka bezpieczeństwa, rozumiana jako jeden z najważniejszych elementów polityki ogólnej państwa, jest określeniem obejmującym zagadnienia bezpieczeństwa, obrony oraz ochrony obywatela i państwa. Politykę bezpieczeństwa, z jednej strony, należy traktować jako pewną koncepcję celów, wartości, interesów i działań politycznych, które mają zapewnić bezpieczeństwo i obronę (ochronę) państwa oraz jego obywateli, z drugiej zaś strony – rozumieć ją można jako ogół działań stanowiących rezultat wprowadzenia powyższej koncepcji w życie (strategia). Polityka bezpieczeństwa stanowi zatem odpowiedź zarówno na zagrożenie zewnętrzne państwa, jak i na zagrożenie bezpieczeństwa wewnętrznego i porządku publicznego, a także na zagrożenia pojawiające się w wyniku różnego rodzaju przestępczości[2].

---

1 Joseph S. Nye Jr., *Soft Power. Jak osiągnąć sukces w polityce światowej* (Warszawa: Wyd. Akademickie i Profesjonalne, 2007), 30.

2 Zob. Zenon Trejnis, „Problemy polityki bezpieczeństwa w ujęciu praktycznym i ewolucyjnym. Doświadczenia z prowadzonego przedmiotu na Kierunku Bezpieczeństwo Narodowe”, w *Studia nad bezpieczeństwem. Teoria i praktyka. Człowiek – Technika – Środowisko*, red. Jerzy Konieczny, Mirosław Skarżyński, t. 1 (Poznań: Wyd. Nauk WNPiD UAM, 2014), 57-58.

Rozwój technologii informatycznych, a zwłaszcza cyfryzacji, spowodował przeniesienie aktywności ludzkiej, zarówno tej pozytywnej, jak i negatywnej, do globalnej sieci Internetu. Największy wkład w rozwój, kształt i funkcjonowanie Internetu wnieśli Amerykanie i dlatego to oni formułują dziś roszczenia do odgrywania roli „strażnika" dotychczasowego Internetu: wolnego, interoperacyjnego, bezpiecznego, wiarygodnego oraz promowania tych cech w skali globalnej.

Sprawne i efektywne zarządzanie wszelkimi podmiotami, obiektami czy systemami w państwie i świecie odbywa się obecnie za pomocą technologii informatycznych czy też teleinformatycznych, które radykalnie wspomagają i usprawniają wszelkie procesy kierowania i zarządzania. Złożone procesy podejmowania decyzji w sposób zasadniczy wspomagane są dziś przez współczesną informatykę, która coraz częściej oparta jest na technologiach teleinformatycznych i rozwiązaniach sieciocentrycznych.

Trudno jest obecnie wyobrazić sobie funkcjonowanie nowoczesnej instytucji, organizacji, przedsiębiorstwa czy wreszcie państwa bez instrumentalnego i kompleksowego wsparcia ze strony współczesnej informatyki oraz telekomunikacji. Jest to nie tylko znak czasu, ale także wymóg światowych trendów i standardów kierowania i zarządzania. Ani Unia Europejska, ani Organizacja Traktatu Północnoatlantyckiego nie narzucają konkretnych rozwiązań koncepcyjnych projektowania i wdrażania nowoczesnych, narodowych aplikacji teleinformatycznych do wspomagania polityczno-strategicznych systemów zarządzania państwem, a zwłaszcza w procesie kierowania jego bezpieczeństwem.

Powszechne przeniesienie informacji do sieci globalnej spowodowało powstanie nowej przestrzeni zwanej cyberprzestrzenią. Do powszechnego obiegu termin ten wprowadził w 1982 r. William Gibson, wcześniej bowiem cyberprzestrzeń kojarzona była z literaturą *science fiction*[3].

W latach 80. ubiegłego stulecia zaczynają powstawać sieci komputerowe oraz Internet. Na początku lat 90. powstaje sieć www oraz pierwsze przeglądarki internetowe. Przesłanie 17 sierpnia 1991 r. pakietu danych z wykorzystaniem protokołu TCP/IP między Wydziałem Fizyki Uniwersytetu Warszawskiego a Centrum Komputerowym Uniwersytetu w Kopenhadze przyjmuje się za symboliczną datę startu polskiego Internetu. Faktycznie włączenie Polski do globalnej sieci w ramach EARN (*European Academic Reearch Network*) nastąpiło 15 grudnia 1991 r. po zniesieniu przez USA ograniczeń w dostępie do nowoczesnych technologii komputerowych i telekomunikacyjnych dla Polski i innych krajów tzw. realnego

[3] William Gibson, *Neuromancer* (Warszawa: Wyd. Zysk i S-ka, 2001), 43.

socjalizmu. W 1990 r. została utworzona domena pl, a w 1992 r. powstają kolejno gov.pl i org.pl[4].

Termin „cyberprzestrzeń" zaczął od tego momentu funkcjonować w użyciu powszechnym i był postrzegany jako nowy obszar aktywności społecznej. Z technologicznego punktu widzenia cyberprzestrzeń to nie tylko Internet, poza nim bowiem istnieją systemy informatyczne, które połączone są innymi sieciami telekomunikacyjnymi. Cyberprzestrzeń postrzega się więc jako medium komunikacji międzyludzkiej, która służy także do komunikacji między systemami teleinformatycznymi bez udziału człowieka.

Początkowo rozwój Internetu nie stanowił dla państw poważnego zagrożenia i nie miał większego znaczenia politycznego i strategicznego. Jednakże w miarę rozwoju i powstania sieci globalnej obejmował coraz to nowe sfery życia człowieka. Pojawił się problem cyberprzestrzeni, takich jak: cyberszpiegostwo, cyberataki, cyberterroryzm, cyberwojna itd. Poza wywiadowczą formą aktywności prowadzone są także defensywne i ofensywne cyberoperacje militarne. Skala możliwości działań skierowanych przeciwko innemu państwu rośnie, mogą one zagrozić jego suwerenności, wywołać destabilizację polityczną, gospodarczą, a nawet utratę integralności terytorialnej.

Potrzeba ochrony interesów narodowych państwa w odniesieniu do cyberprzestrzeni spowodowała powstanie nowego rodzaju bezpieczeństwa w ujęciu przedmiotowym, a mianowicie cyberbezpieczeństwa czy też cyberobrony. Powstały bowiem możliwości niemalże globalnego śledzenia elektronicznej komunikacji – zwłaszcza przez USA, ale nie tylko – ponieważ prawie cała komunikacja sieciowa przechodzi przez amerykańskie serwery oraz prowadzone jest masowe inwigilowanie niewinnych ludzi przez przechwytywanie elektronicznej komunikacji i internetowej aktywności, a także jej zapisywanie w swoich bazach danych.

W najbliższej przyszłości ataki w cyberprzestrzeni mogą być coraz liczniejsze i bardziej zaawansowane. Większość włamań do systemów bezpieczeństwa i obrony państw i organizacji polityczno-militarnych oraz sieci rządowych to akty cyberbezpieczeństwa ukierunkowanego na pozyskiwanie danych. Grupy cyberprzestępcze atakują sektor prywatny i osoby indywidualne. Celem ataków są przeważnie jednak sieci wojskowe i systemy infrastruktury krytycznej w państwie. Przejęcie nad nimi kontroli, usunięcie i zmanipulowanie danych może sparaliżować systemy dowodzenia i łączności wojsk czy też pozbawić ludzi dostępu do usług sektora energetycznego, finansowego i telekomunikacyjnego. Co prawda, do tej pory nie odnotowano ataków powodujących całkowity paraliż najważniejszych

[4] Dariusz Baran, *Internet w Polsce* (Kraków: Oficyna Wyd. AFM, 2013), 76.

dla państwa sektorów, straty w ludziach czy rozległe zniszczenia fizyczne, jednak cyberataki stają się coraz bardziej zaawansowane.

Bezpieczeństwo cyberprzestrzeni stało się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa i obronności każdego państwa. W okresie, kiedy panuje swoboda przepływu osób, towarów, informacji i kapitału, państwo zmuszone jest prowadzić odpowiednią politykę ochrony cyberprzestrzeni pozwalającą skutecznie zapobiegać i zwalczać jej zagrożenia. Celem artykułu jest analiza polityki i ochrony cyberprzestrzeni realizowanej przez państwa, organizacje międzynarodowe i inne podmioty wobec wyzwań i zagrożeń w cyberprzestrzeni.

* * *

Szybki rozwój technologii internetowych a także komputeryzacja i usieciowienie większości dziedzin życia spowodowały, że cyberprzestrzeń przeniesiona została do celów militarnych i realizacji strategii bezpieczeństwa narodowego i międzynarodowego. Komputer, mikroprocesor oraz inne innowacje technologiczne w telekomunikacji doprowadziły do rewolucji informatycznych w armiach rozwijających się państw i obok zagrożeń o charakterze asymetrycznym i hybrydowym stały się nowymi wyzwaniami i przyczynami współczesnych konfliktów zbrojnych. Współczesny teatr działań wojennych charakteryzować się będzie asymetryzacją, sieciocentrycznością zagrożeń oraz dużym udziałem nowych technologii, przy jednoczesnym zmniejszeniu udziału w działaniach wojennych jednostek ludzkich. Cyberprzestrzeń stała się nie tylko wspaniałym narzędziem ułatwiającym prowadzenie wojny, ale także bardzo wrażliwym punktem, w który można uderzyć z dowolnego miejsca globu, zarówno w ramach wojskowych informacji, działalności kryminalnej czy dla zwykłej zabawy.

Armia amerykańska już od końca lat 80. ubiegłego stulecia w ramach INFO RMA (*Information Revolution in Military Affairs*) wykorzystuje rewolucję informatyczną do komputeryzacji, digitalizacji, usieciowienia narzędzi wojny i rozwoju biotechnologii (*Biotechnological RMA*), której głównym celem jest stworzenie zintegrowanego interfejsu człowiek–maszyna. Wielkie mocarstwa, państwa członkowskie NATO, w tym i Polska, w swoich strategiach wskazują cyberprzestrzeń jako piątą kluczową przestrzeń swojej działalności w zakresie obronności i bezpieczeństwa państwa. Walkę informacyjną zdefiniowano, jako działania podejmowane w celu osiągnięcia przewagi informacyjnej przez wpływanie na informację przeciwnika, zależne od informacji procesy, informacyjne systemy i sieci

komputerowe przy jednoczesnej obronie własnych informacji, zależnych od informacji informacyjnych systemów i sieci komputerowych[5].

* * *

Prawdą starą jak świat jest teza, że ten, kto kontroluje przestrzeń informacyjną, ten kontroluje państwo. Natomiast władzę wszystkich istniejących państw teraz i w przeszłości wykorzystują mass media do kształtowania świadomości ludzi, próbując wedle własnych potrzeb zmieniać postrzeganie rzeczywistości społecznej i przyrodniczej oraz życia w świecie iluzji. Rosnące uzależnienie ludzkości od nowoczesnych technologii, sieci komputerowych i Internetu powoduje, że cyberprzestrzeń odgrywa coraz większą rolę w komunikacji strategicznej w państwie i świecie. Uzależnienie to bardzo szybko rośnie, bowiem cyberprzestrzeń wykorzystywana jest nie tylko do odbierania i przekazywania informacji, ale także do koordynacji naszych działań oraz analizy otoczenia w celu oceny potencjalnych zagrożeń i konfliktów. Dlatego ochrona cyberprzestrzeni stała się jedną z form bezpieczeństwa każdego państwa i, pojmowana jako obszar bezpieczeństwa, wymusza konieczność włączenia i skoordynowania z pozostałymi komponentami systemu bezpieczeństwa[6].

Istota cyberprzestrzeni zawiera się w dwóch podstawowych aspektach: informacji i komunikacji z tym, że informacja jest w niej generowana i przetwarzana, a następnie transmitowana, tworząc kolejne, cyberprzestrzenne powiązania. Obecnie to Internet stanowi podstawę komunikacji, tworząc globalną sieć komputerową łączącą sieci lokalne. Samo pojęcie cyberprzestrzeni jest szerokie, istnieje wiele jego definicji, które obejmują narzędzia oraz środki komunikacyjne i informacyjne, a zwłaszcza: urządzenia, sieci (*offline, online, interanet, darknet* itp.), techniki, technologie, użytkowników, aktorów i przestrzeń. Natomiast obszar ochrony cyberprzestrzeni, zarówno pod względem formalno-prawnym, jak i ustaleń wynikających ze strategii bezpieczeństwa państwa, implikuje konieczność ro-

---

[5] Łukasz Kamieński, *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych* (Kraków: Wyd. Uniwersytetu Jagiellońskiego, 2009), 212-255; Ryszard Szpyra, *Cyberbezpieczeństwo militarne w amerykańskiej praktyce* (Warszawa: Wyd. Akademii Sztuki Wojennej, 2016).

[6] Bernard Wiśniewski, Monika Szyłkowska, „Bezpieczeństwo w cyberprzestrzeni – wyzwania prawne i organizacyjne", w *Cyberprzestrzeń. Uzależnienia – Zagrożenia*, red. Mieczysław Koziński, Joanna Grubicka, Sylwia Kosznik-Biernacka (Słupsk: Wyd. ProPomerania, 2016), 51.

zumowania i operowania w dwóch płaszczyznach symultanicznie: realnej i wirtualnej[7].

Cyberprzestrzeń w ostatnim okresie stała się miejscem bardzo często wykorzystywanym do wszelkiego rodzaju działań niezgodnych z prawem, a ich wykonawcami są nie tylko amatorzy czy wandale, ale także wysoce wyspecjalizowani hakerzy, a nawet państwa oraz organizacje terrorystyczne. Najczęściej atakowane są strony internetowe związane z nowymi technologiami – 23,2% (odsetek wszystkich zaatakowanych stron w 2015 r.); biznesem – 8,1%; wyszukiwarki – 7,5%; z blogami – 7,0%; edukacją – 4,0%; typem *domain parking* – 3,2%; rozrywką – 2,6%; zakupami – 2,4%[8]. Dane te świadczą, że w 2015 r. najczęściej atakowane były strony dotyczące technologii i stanowiły aż 23,2% wszystkich zaatakowanych stron, a najważniejsze pobudki tych ataków były związane z chęcią uzyskania korzyści materialnych. Głównymi źródłami cyberataków od lat są USA, Chiny oraz Rosja, motywacje atakowania sieci komputerowych są jednakże różnorodne i przedstawiają się następująco:

Typy motywacji	Przykładowe cele motywacji
POLITYCZNE	Promocja ideologii, postaw i wartości politycznych; rywalizacja międzynarodowa
WOJSKOWE	Jako kategoria motywacji politycznych obejmują wykorzystanie cyberprzestrzeni do realizacji określonych operacji militarnych
RELIGIJNE	Promocja idei religijnych; nawracanie; walka z niewiernymi; zemsta za obrazę religii
GOSPODARCZE	Kradzież technologii; zakłócenie systemu finansowego w celu uzyskania korzyści ekonomicznych
SPOŁECZNE	Protest związany z występowaniem określonych problemów społecznych
INDYWIDUALNE	Rozwój umiejętności; poszukiwanie rozrywki; chęć zabicia nudy

Źródło: Miron Łakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw* (Katowice: Wyd. Uniwersytetu Śląskiego, 2015), 136.

[7] Tamże, 54.

[8] *Internet Security Threat Report – April 2016*, t. 21, Symantec, 22.

Cyberprzestrzeń obejmuje ogół środków informacyjnych i komunikacyjnych w zbiorze sieci, technik, użytkowników oraz przestrzeni cyfrowej, której przypisuje się z kolei trzy warstwy: materialną, logiczną i informacyjną. Podział zagrożeń z kolei funkcjonujących w środowisku cyfrowym, wynika z funkcji celu, tj. zakłócenia, kradzieży, przechwycenia, uszkodzenia, manipulacji, przejęcia kontroli, modyfikacji lub zniszczenia informacji i systemów. Narzędziami wykorzystywanymi do realizacji tych celów są odpowiednio przygotowywane, złośliwe programy – wirusy lub robaki komputerowe, takie jak:

– *Spyware* – oprogramowanie, którego celem jest szpiegowanie użytkowników bez ich wiedzy, m.in. rejestrowanie odwiedzanych stron czy haseł wpisanych na klawiaturze, a następnie przesyłanie danych do atakującego;

– Konie trojańskie – oprogramowanie, które, podszywając się pod przydatne lub interesujące dla użytkownika aplikacje, dodatkowo ma niepożądaną, ukrytą funkcjonalność;

– *Hoaxy* – programy, które wyświetlają nieprawdziwą informację o tym, że w komputerze znajduje się wirus;

– Bomby logiczne – uśpiona forma złośliwego oprogramowania aktywizująca się z chwilą spełnienia określonych warunków, np. określonej godziny lub dnia;

– *Phishing* – polega na podstępnym zdobyciu loginów i haseł przez podszywanie się pod godną zaufania instytucję lub osobę.

Istnieją także zagrożenia nazywane atakami ukierunkowanymi Typu APT (*Advanced Persistent Threat*), które łączą różne narzędzia, np. programistyczne czy socjotechniczne. Takie ataki są przygotowywane przez długi okres przez zorganizowanie grupy dysponujące pokaźnymi zasobami finansowymi oraz czasem niezbędnym do konkretnego zinfiltrowania celu, np. instytucji czy firmy, a następnie przeprowadzenia precyzyjnego działania. Z kolei cyfrowe fałszerstwa i wyłudzenia podzielić można na: dokonywane za pomocą fałszywych komunikatorów (e-maila) oraz hybrydowe, a więc fałszywe maile zawierające złośliwe programy lub link do takiego rodzaju programów[9].

W dobie szybkiego rozwoju technologii cyfrowych[10] cyberprzestępcy i cyberterroryści dysponują nieograniczonymi instrumentami techno-

[9] Szerzej Monika Szyłkowska, Jerzy Kozioł, „Paradygmat wolności cyfrowej sieci w kontrapunkcie bezpieczeństwa – zarys problemu", w Koziński, *Cyberprzestrzeń. Uzależnienia,* 144-146.

[10] Informatyzacji towarzyszą lub są z nią powiązane takie procesy jak: komputeryzacja, elektronizacja, digitalizacja, internalizacja, telematyzacja, wirtualizacja, algorytmizacja. Szerzej Jacek Janowski, *Technologia informacyjna*

logicznymi i mają wiedzę pozwalającą na ich dowolne wykorzystywanie. Spectrum zagrożeń wynikających z procesów globalizacyjnych rośnie w niespotykanym dotąd tempie, a ich autorzy stają się praktycznie niezauważalni i trudni do wykrycia. Mogą to być np. spekulanci giełdowi, handlowcy, korporacje międzynarodowe, firmy świadczące usługi internetowe oraz tajne służby. Dziś wszelkie tradycyjne mechanizmy państwa oparte na idei ochrony granic, porządku, władzy, policji i struktur siłowych są zagrożone, podobnie jak międzynarodowe systemy bezpieczeństwa i obronności oraz struktury gospodarcze i finansowe narażone są także na coraz bardziej zuchwałe, nieprzewidywalne i skomplikowane cyberataki[11].

* * *

Po atakach cybernetycznych przeciwko Estonii w 2006 r. wiele państw uznało potrzebę podjęcia działań w zakresie zwiększenia poziomu ochrony cyberprzestrzeni, uznając takie ataki za jedno z potencjalnych zagrożeń dla bezpieczeństwa państwa. Większość państw opracowała własne polityki, strategie i doktryny związane z bezpieczeństwem w cyberprzestrzeni, co powoduje, że występuje wiele rozbieżności w zakresie nazewnictwa i kryteriów określających konkretne zjawiska w tej dziedzinie. Szybki rozwój technologiczny także pogłębia przepaść w postrzeganiu tych zjawisk. I tak definicja przedstawiona w *Tallin Manual on the International Law Applicable to CyberWarfare* nie uwzględnia czynnika ludzkiego, głosi bowiem, że cyberprzestrzeń to środowisko tworzone przez składniki fizyczne i niefizyczne, charakteryzujące się wykorzystaniem komputerów i widma elektromedycznego do przechowywania, modyfikowania i wymiany danych z wykorzystaniem sieci komputerowych[12].

Podobnie rozbieżność występuje przy określaniu zjawiska cyberwojny. W wydanym prze Biuro Bezpieczeństwa Narodowego RP opracowaniu *Wojna cybernetyczna – wyzwanie XXI wieku* autorzy podają, że cyberwojna to zorganizowana w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określanych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania

dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracyjnym (Warszawa: Wyd. Difin, 2009), 345.

11 Marek Leszczyński, *Bezpieczeństwo społeczne a bezpieczeństwo państwa* (Kielce: Wyd. Uniwersytetu Humanistyczno-Przyrodniczego, 2009), 59.

12 Michael N. Schmitt, red., *Tallin Manual on the International Law Applicable to CyberWarfare* (Cambridge: Cambridge University Press, 2013).

przeciwnika, lub przepływających przez nie informacji oraz ochronę własnych systemów przed podobnym działaniem przeciwnika[13].

* * *

W Polsce w oficjalnych dokumentach termin ten został użyty w *Strategii Bezpieczeństwa Narodowego RP z 2007 r.* Co prawda wcześniej, w *Strategii Bezpieczeństwa RP z 2003 r.*, wspomniano, że zagrożenia w sferze teleinformatycznej stają się dla Polski coraz bardziej realne. Ponadto stwierdzono, że rośnie zagrożenie operacjami mającymi na celu dezorganizację systemów informacyjnych instytucji rządowych i samorządowych oraz niektórych sfer sektora prywatnego, związanych z systemem bezpieczeństwa państwa. Strategia zalecała ochronę infrastruktury krytycznej rządowej i samorządowej przez wyspecjalizowane komórki cywilne i wojskowe służb państwowych przeciwko działaniu ze strony obcych służb specjalnych a także ugrupowań terrorystycznych, ekstremistycznych i zorganizowanych grup przestępczych. Zagrożenia powstają w wyniku penetracji baz danych oraz prowadzenia działań dezinformacyjnych polskiej opinii publicznej i społeczeństwa.

Jak już wspomniano, w *Strategii Bezpieczeństwa Narodowego RP z 2007 r.* użyto pojęcia cyberprzestrzeni a także przestępczości cybernetycznej, nie definiując jednakże tych terminów. W strategii stwierdzono, że jednym z zagrożeń dla Polski może być oddziaływanie w cyberprzestrzeni skierowane przeciwko systemom i sieciom infrastruktury krytycznej, które spowodować mogą zarówno straty materialne, jak i sparaliżować istotne sfery życia publicznego. Zalecono także działania w zakresie rozwoju nowoczesnej, zintegrowanej struktury łączności elektronicznej, która byłaby odporna na awarie i potencjalne cyberataki. Stwierdzono przy tym, że rozwój ten będzie wymagał wysiłku nie tylko ze strony odpowiednich służb państwowych, ale także współpracy podmiotów prywatnych[14].

W przyjętym przez Radę Bezpieczeństwa Narodowego 8 listopada 2012 r. *Strategicznym Przeglądzie Bezpieczeństwa Narodowego RP* zwrócono uwagę na zagrożenia terrorystyczne i ich przeniesienie do cyberprzestrzeni[15]. W opublikowanej 23 maja 2013 r. *Białej Księdze Bezpieczeństwa Narodowego* adresowanej do wszystkich Polaków podkreślano m.in., że aktywność

[13] Krzysztof Liedel, Paulina Piasecka, „Wojna cybernetyczna – Wyzwanie XXI wieku", *Bezpieczeństwo Narodowe. Kwartalnik BBN* 17, nr 1 (2011): 17.

[14] *Strategia Bezpieczeństwa Narodowego RP z 2014 r.* (Warszawa: Wyd. BBN, 2014).

[15] *Strategiczny Przegląd Bezpieczeństwa Narodowego, Główne wnioski i rekomendacje dla Polski* (Warszawa: Wyd. BBN, 2012).

terrorystów przenosi się do cyberprzestrzeni, która w coraz większym stopniu będzie się stawać obszarem rywalizacji i konfrontacji między państwami, dlatego też jednym z najważniejszych wyzwań w dziedzinie bezpieczeństwa pozamilitarnego dla Polski będzie konieczność zapewnienia bezpieczeństwa w cyberprzestrzeni[16]. Także *Strategia Bezpieczeństwa Narodowego z 2014 r.,* przedstawiając środowisko bezpieczeństwa Polski w wymiarze globalnym, regionalnym i krajowym, podkreśla znaczenie bezpieczeństwa w cyberprzestrzeni oraz zwraca uwagę, że wraz z rozwojem sieci Internet pojawiły się nowe zagrożenia, mogące poważnie zakłócić funkcjonowanie społeczeństw i państw, takie jak: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty, z udziałem podmiotów niepaństwowych, i cyberwojna rozumiana jako konfrontacja między państwami.

W rozdziale trzecim zaprezentowana została strategia operacyjna, która określa głównie kierunki działania w sferze bezpieczeństwa z podziałem na działania obronne, ochronne a także w sferze bezpieczeństwa społecznego i gospodarczego, podkreślając jednocześnie, że cyberprzestrzeń to nowe środowisko walki zbrojnej. *Strategia* zakłada, że siły zbrojne muszą być gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie konfliktu 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.

W rozdziale czwartym *Strategii* wskazano potrzebę wdrożenia i rozwijania systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym oraz konieczność budowy nowego systemu obrony cybernetycznej, m.in. Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP (CSIRT) oraz narodowego ośrodka koordynacji, wspierającego organizację współpracy między podmiotami w zakresie cyberbezpieczeństwa i wymiany informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa. *Strategia* zakłada też podjęcie działań na rzecz zwiększania świadomości społeczeństwa w obszarze zagrożeń w cyberprzestrzeni poprzez prowadzenie kampanii społecznych, edukację i rozwijanie programów badawczych w tym obszarze[17].

W Polsce dopiero w 2008 r. zapoczątkowano prace mające na celu przygotowanie przez administrację państwową kompleksowej strategii przeciwdziałania zagrożeniom w cyberprzestrzeni, bowiem w listopadzie

[16] *Biała Księga Bezpieczeństwa Narodowego RP* (Warszawa: Wyd. BBN, 2013).

[17] *Strategia Bezpieczeństwa Narodowego RP*.

tegoż roku przedstawiono *Rządowy program ochrony cyberprzestrzeni na lata 2008-2011*, który można przyjąć za formalny początek działań rządu i administracji państwowej na rzecz bezpieczeństwa cyberprzestrzennego. W czerwcu 2013 r. Rada Ministrów RP przyjęła uchwałą *Politykę ochrony cyberprzestrzeni RP*[18]. Wcześniej, w zrealizowanej ustawie o stanie wojennym z 30 sierpnia 2011 r., zdefiniowano cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt. 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. System teleinformatyczny, zgodnie z tą ustawą, to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przekazywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[19].

Uchwała o polityce ochrony cyberprzestrzeni z 2013 r. miała stać się podstawą działań na rzecz bezpieczeństwa cybernetycznego dla administracji rządowej i samorządowej oraz innych podmiotów państwowych, a także pozostałych użytkowników cyberprzestrzeni, takich jak prywatni przedsiębiorcy czy operatorzy infrastruktury krytycznej. Mimo że od podjęcia działań przez administrację państwową na rzecz zapewnienia bezpieczeństwa cybernetycznego upłynęła blisko dekada, ocena działań przeprowadzenia przez Najwyższą Izbę Kontroli pozostaje negatywna. NIK podkreśla, że główną przyczyną niskiej skuteczności działań związanych z zapewnieniem bezpieczeństwa cybernetycznego jest brak spójnych regulacji prawnych dla krajowego systemu ochrony cyberprzestrzeni, mimo przyjęcia nowej *Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022* uzupełnianej podtytułami: *Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa*[20]. Brakuje zatem podstawowego elementu ram prawnych, w których

[18] *Polityka ochrony cyberprzestrzeni Rzeczypospolite Polskiej* (Warszawa: Wyd. Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, 2013).

[19] *Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP oraz niektórych innych ustaw*, Dz. U. z 2011 r. Nr 222, poz. 1323; *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*, Dz. U. z 2005 r. Nr 64, poz. 565.

[20] *Strategia Cyberbezpieczeństwa RP na lata 2017-2022* (Warszawa: Wyd. Ministerstwo Cyfryzacji, 2017).

określane zostałyby ogólne zasady funkcjonowania systemu ochrony cyberprzestrzeni, rola i zadania a także zakres odpowiedzialności podmiotów państwowych i prywatnych. Wynika to m.in. z braku jednolitej ustawy o funkcjonowaniu systemu bezpieczeństwa narodowego w Polsce, trudno więc oczekiwać, aby ministerstwa i inne instytucje państwowe i samorządowe oddolnie utworzyły spójny system ochrony bezpieczeństwa cybernetycznego. Jak z tego wynika, bezpieczeństwo cybernetyczne nie było traktowane przez najważniejsze organy i instytucje z należytą uwagą. Zapewne nie zdawano sobie sprawy, jak konieczne są pilne działania w odpowiedzi na pojawianie się nowych jakościowo zagrożeń. Z kontroli NIK wynika natomiast, że działania podejmowane na rzecz ochrony cyberprzestrzeni przez decydentów i pracowników administracji państwowej są ograniczone i prowadzone fragmentarycznie. Wynika to z niskiego poziomu świadomości co do skali zagrożeń cybernetycznych i ich następstw, dlatego realizacja zadań w tym zakresie prowadzona była w sposób chaotyczny i intuicyjny. Podejście takie utrudniło wypracowanie w ramach całej instytucji spójnego systemu zarządzania bezpieczeństwem informatycznym.

Na poziom świadomości w zakresie zagrożeń cybernetycznych wpływa działalność administracji rządowej w zakresie monitorowania incydentów komputerowych. Podczas kontroli NIK stwierdził, że w Polsce nie został zorganizowany system zbierania i rejestrowania informacji o incydentach komputerowych, ponieważ nie istniał wówczas prawny obowiązek zgłaszania takich incydentów przez najważniejszych użytkowników i administratorów cyberprzestrzeni. W 2014 r. w sieciach administracji publicznej zarejestrowano kilkanaście tysięcy incydentów, a ponad 40 mln przez dziesięciu operatorów komunikacyjnych w Polsce[21].

Ponadto z raportu kontroli NIK wynika, że podmioty państwowe nie prowadzą systemowych działań w zakresie edukacji dla cyberbezpieczeństwa, których celem byłoby uświadamianie społeczeństwa o zagrożeniach związanych z korzystaniem Internetu czy też metodach ochrony przed zagrożeniami cybernetycznymi. Prowadzone przez Policję, Naukową i Akademicką Sieć Komputerową (NASK), Rządowe Centrum Bezpieczeństwa oraz Agencję Bezpieczeństwa Wewnętrznego działania edukacyjne i szkoleniowe miały charakter oddolny i nie były koordynowane w ramach rządowego systemu szkoleń i działań edukacyjnych[22].

---

[21] *Realizacja przed podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni. Informacja w wynikach Kontroli. KPB – 4101 – 002 – 00/2014 Nr ewid. 42/2015/p/14/043/KPB* (Warszawa: Departament Porządku i Bezpieczeństwa Wewnętrznego, NIK, 2016), 57-58, 68.

[22] Tamże, 68-89.

Na potrzebę tworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez społeczeństwo wskazuje wspomniana już *Strategia cyberbezpieczeństwa RP na lata 2017-2022*[23]. Problematyka bezpiecznego korzystania z cyberprzestrzeni powinna być uwzględniana już w ramach programu nauczania wczesnoszkolnego, a kadra nauczycielska odpowiednio przygotowywana do prowadzenia zajęć z ochrony cyberprzestrzeni i płynących z niej zagrożeń. W *Strategii* zakłada się działania związane z kształtowaniem świadomości społeczeństwa na zagrożenia cybernetyczne. Przewiduje się też szeroką współpracę administracji publicznej ze środowiskami akademickimi i organizacjami pozarządowymi, a także wspieranie działań edukacyjnych prowadzonych przez operatorów usług kluczowych i dostawców usług cyfrowych. Na potrzebę działań edukacyjnych na rzecz cyberbezpieczeństwa wskazuje także Polskie Forum Cyberbezpieczeństwa.

Strategia cyberbezpieczeństwa RP na lata 2017-2022 także krytycznie ocenia dotychczasowe działania w zakresie cyberbezpieczeństwa podmiotów ze strony sfery cywilnej, wojskowej, sektora publicznego i prywatnego oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości ze względu na niską efektywność istniejącego systemu ochrony oraz rozproszony charakter. W dokumencie tym zdefiniowano m.in. cyberprzestrzeń, która oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne oraz z powiązaniami między nimi i relacjami z użytkownikami. Określono także, że „bezpieczeństwo sieci i systemów informatycznych" (inaczej „cyberbezpieczeństwo" lub „bezpieczeństwo teleinformatyczne") oznacza odporność systemów teleinformatycznych przy dawnym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych przez te sieci i systemy informatyczne[24].

Strategia cyberbezpieczeństwa RP na lata 2017-2022 firmowana jest przez Ministerstwo Cyfryzacji. Zakłada ona cel główny, którym jest zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych, a także cztery cele szczegółowe. Pierwszym celem szczegółowym jest osiągnięcie zdolności do skoordynowania w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa. Drugim celem jest wzmocnienie zdolności do przeciwdziałania

[23] *Strategia cyberbezpieczeństwa RP na lata 2017-2022*, pkt. 7.5.

[24] Tamże, pkt. 11. 1 i 2.

cyberzagrożeniom. Trzecim celem jest zwiększenie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. I wreszcie czwartym zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa[25].

W *Strategii cyberbezpieczeństwa RP na lata 2017-2022*, podobnie jak w poprzednich dokumentach dotyczących rozwiązania tego problemu, zauważyć można kilka słabości. Jedną z nich jest to, że za cyberbezpieczeństwo w Polsce odpowiada wiele instytucji i każda we własnym zakresie, a tymczasem cyberzagrożenia są ściśle ze sobą powiązane, bo przecież nie są to osobno problemy sektorów bankowego, telekomunikacji czy administracji rządowej i samorządowej lub sektora prywatnego. W *Strategii* nie wskazano, kto jest głównym odpowiedzialnym za koordynację i stworzenie systemu ochrony cyberprzestrzeni w państwie. Brakuje wskazań, jak mają wyglądać programy i plany działania, terminy realizacji zadań wynikających z założonych celów, kto będzie odpowiedzialny za nie i kto będzie je finansował. Wydaje się, że plan realizacji celów i zadań powinien być spójny ze *Strategią,* podobnie jak stworzenie systemu zarządzania ryzykiem na poziomie krajowym. Zgodnie z zapowiedzią Ministerstwo Cyfryzacji przygotuje szczegółowy plan działań za pół roku.

Mało przejrzyście sformułowane zostały w *Strategii* zasady finansowania kosztów wdrażania jej w życie. W *Strategii* zobowiązuje się podmioty realizujące zadania publiczne do uwzględnienia w swoich planach finansowych wydatków na cyberbezpieczeństwo. Szczegółowe oszacowanie wielkości i struktury kosztów wdrażania założeń *Strategii cyberbezpieczeństwa na lata 2017-2022* będzie możliwe dopiero w procesie inicjowania poszczególnych jednostek i inicjowania konkretnych projektów. Obok środków jednostek zaangażowanych w jej wdrażanie wskazuje się także potencjalne źródła finansowania pochodzące z Narodowego Centrum Badań i Rozwoju oraz funduszy z Unii Europejskiej. Nadrobienie opóźnień w stosunku do innych państw europejskich wymagać będzie, jak twierdzą niektórzy eksperci, nakładów rzędu kilku miliardów złotych w perspektywie najbliższych 3-5 lat. W *Strategii* zabrakło też zapisów dotyczących partnerstwa publiczno-prywatnego i systemu zachęt dla sektora prywatnego w celu finansowania rozbudowy infrastruktury i podejmowania działań związanych z ochroną cyberprzestrzeni. Warto też podkreślić stanowisko resortu obrony i zaangażowanie sił zbrojnych w tym zakresie. Resort obrony w 2017 r. zamierza wydać miliard złotych na tworzenie wyspecjalizowanych komórek cyberobrony[26].

[25] Tamże, pkt 5, 6, 7 i 8.

[26] Eugeniusz Cieślak, „Ocena wybranych działań administracji państwowej na rzecz bezpieczeństwa cybernetycznego", w *Rola i zadania administracji*

W pierwszej wersji *Strategii* z 2016 r., która była odpowiedzią na zarzuty kontroli NIK, za system ochrony cyberprzestrzeni w Polsce odpowiedzialne miało być Ministerstwo Cyfryzacji; kolejnymi poziomami odpowiedzialności miały być punkty kontaktowe do zbierania informacji na temat incydentów w skali całego kraju i punkt kontaktowy dla operatorów infrastruktury krytycznej jako jednostki pomocnicze dla operatorów telekomunikacyjnych na wypadek cyberataków. Narodowe Centrum Cyberbezpieczeństwa miało być odpowiedzialne za przygotowanie rekomendacji dla wszystkich instytucji, zaś CERT/CSIRT Narodowy – miał być zespołem reagującym na naruszenia bezpieczeństwa w sieciach i pomagać neutralizować najgroźniejsze incydenty. Obok wspomnianych jednostek funkcjonować miały działające już zespoły CERT przy ABW, NASK i MON, odpowiedzialne za kontrolę i pomoc w poszczególnych sektorach. W tym celu przewidywano nowelizację dotychczasowych ustaw[27].

* * *

Trudno dziś także stwierdzić, na jakim etapie znajdują się prace legislacyjne nad przygotowaniem ustawy o bezpieczeństwie cybernetycznym, która zapobiegałaby sporom kompetencyjnym między resortami i instytucjami. Bez ustawy o ochronie cyberprzestrzeni na poziomie unijnym i krajowym oraz przedłużającej się w tym zakresie „Polski resortowej" trudno będzie zharmonizować działania do walki z zagrożeniami z cyberprzestrzeni, bowiem brak jest jednym z głównych narzędzi prawnych zarówno dla przeciwników, jak i organów ścigania oraz przeciwdziałania.

Zapewnienie ochrony cyberprzestrzeni wymaga też współpracy i współdziałania wszystkich użytkowników globalnej sieci, którzy świadomi są niebezpieczeństw, jakie niosą zagrożenia dla cyberbezpieczeństwa. Potrzebne jest także kształcenie specjalistów z dziedziny ochrony środowiska cyberprzestrzeni i kadry urzędniczej. Powinny temu towarzyszyć działania konsultacyjne i doradcze oraz współpraca z firmami całego sektora teleinformatycznego, a także działania o charakterze edukacyjno-prewencyjnym wśród społeczeństwa. Natomiast tworząc normy prawne na poziomie krajowym i przepisy regulujące współpracę międzynarodową oraz strategie i polityki bezpieczeństwa, które w większości mają – jak do-

publicznej w zarządzaniu bezpieczeństwem informacji, red. Jerzy Kisielnicki i in. (Rzeszów: Oficyna Wyd. Politechniki Rzeszowskiej, 2017), 131.

[27] *Strategia cyberbezpieczeństwa RP na lata 2016-2020. Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa* (Warszawa: Wyd. Ministerstwo Cyfryzacji, 2016).

tychczas – charakter deklaratywny, w praktyce należy oprócz systemu krajowego o charakterze organizacyjno-prawnym stworzyć także podsystem szybkiego reagowania na zagrożenia ze strony grup przestępczych działających w cyberprzestrzeni, w tym ich ścigania i karania[28].

Największą bolączką działalności podmiotów na szczeblu państwowym jest prowadzenie działań rozproszonych o bardzo różnym poziomie jakości i bez spójnej wizji systemowej podejścia do zagadnienia cyberbezpieczeństwa. Oprócz powstania Narodowego Centrum Cyberbezpieczeństwa postuluje się także powołanie do życia ciała doradczego w postaci Narodowej Rady Cyberbezpieczeństwa, złożonej z reprezentantów różnych podmiotów, zarówno przedstawicieli biznesu, uczelni i ośrodków naukowo-badawczych oraz organizacji pozarządowych. Niezbędne są także szeroko rozumiane zasoby ludzkie i finansowe, bez odpowiednich kadr oraz dodatkowych środków budżetowych trudno będzie zrealizować założone przez Ministerstwo Cyfryzacji cele[29].

Bibliografia:

Baran Dariusz. *Internet w Polsce*. Kraków: Oficyna Wyd. AFM, 2013.

Biała Księga Bezpieczeństwa Narodowego RP. Warszawa: Wyd. BBN, 2013.

Cieślak Eugeniusz. „Ocena wybranych działań administracji państwowej na rzecz bezpieczeństwa cybernetycznego". W *Rola i zadania administracji publicznej w zarządzaniu bezpieczeństwem informacji*, redakcja Jerzy Kisielnicki i in. Rzeszów: Oficyna Wyd. Politechniki Rzeszowskiej, 2017.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. Warszawa: Wyd. Biuro Bezpieczeństwa Narodowego, 2015.

Gibson William. *Neuromancer*. Warszawa: Wyd. Zysk i S-ka, 2001.

[28] Zob. Paweł Gibuła, „Niebezpieczna cyberprzestrzeń – działania na rzecz bezpieczeństwa teleinformatycznego Polski", *Kontrola Państwowa NIK* 369, nr 4 (2016).

[29] Joanna Świątkowska, „Cyberbezpieczeństwo Polski w obliczu aktualnych i przyszłych wyzwań", *Bezpieczeństwo i obronność,* nr 1 (2016): 70-78.

Gibuła Paweł. „Niebezpieczna cyberprzestrzeń – działania na rzecz bezpieczeństwa teleinformatycznego Polski". *Kontrola Państwowa NIK* 369, nr 4 (2016).

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

Informacja o wynikach kontroli: Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych, Nr ewid. P/15/042. Warszawa: Wyd. NIK, 2016.

Internet Security Threat Report – April 2016. T. 21. Symantec.

Janowski Jacek. *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracyjnym*. Warszawa: Wyd. Difin, 2009.

Kamieński Łukasz. *Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych*. Kraków: Wyd. Uniwersytetu Jagiellońskiego, 2009.

Leszczyński Marek. *Bezpieczeństwo społeczne a bezpieczeństwo państwa.* Kielce: Wyd. Uniwersytetu Humanistyczno-Przyrodniczego, 2009.

Liedel Krzysztof, Piasecka Paulina. „Wojna cybernetyczna – Wyzwanie XXI wieku". *Bezpieczeństwo Narodowe. Kwartalnik BBN* 17, nr 1 (2011).

Łakomy Miron. *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw.* Katowice: Wyd. Uniwersytetu Śląskiego, 2015.

Nye S. Joseph Jr. *Soft Power. Jak osiągnąć sukces w polityce światowej.* Warszawa: Wyd. Akademickie i Profesjonalne, 2007.

Polityka ochrony cyberprzestrzeni Rzeczypospolite Polskiej. Warszawa: Wyd. Ministerstwo Administracji i Cyfryzacji, 2013.

Rządowy Program Ochrony Cyberprzesztrzeni Rzeczypospolitej Polskiej na lata 2011-2016. Warszawa: Wyd. MSWiA, 2010.

Strategia Bezpieczeństwa Narodowego RP z 2014 r. Warszawa: Wyd. BBN, 2014.

Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016-2020. Poszanowanie praw i wolności w cyberprzestrzeni, Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa. Warszawa: Wyd. Ministerstwo Cyfryzacji, 2016.

Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Poszanowanie praw i wolności w cyberprzestrzeni, Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa. Warszawa: Wyd. Ministerstwo Cyfryzacji, 2017.

Strategiczny Przegląd Bezpieczeństwa Narodowego. Główne Wnioski i Rekomendacje dla Polski. Warszawa: Wyd. Biuro Bezpieczeństwa Narodowego, 2012.

Szpyra Ryszard. *Cyberbezpieczeństwo militarne w amerykańskiej praktyce*. Warszawa: Wyd. Akademii Sztuki Wojennej, 2016.

Szyłkowska Monika, Kozioł Jerzy. „Paradygmat wolności cyfrowej sieci w kontrapunkcie bezpieczeństwa – zarys problemu". W *Cyberprzestrzeń. Uzależnienia – Zagrożenia*, redakcja Mieczysław Koziński, Joanna Grubicka, Sylwia Kosznik-Biernacka. Słupsk: Wyd. ProPomerania, 2016.

Świątkowska Joanna. „Cyberbezpieczeństwo Polski w obliczu aktualnych i przyszłych wyzwań". *Bezpieczeństwo i Obronność,* nr 1(2016): 70-78.

Trejnis Zenon. „Problemy polityki bezpieczeństwa w ujęciu praktycznym i ewolucyjnym. Doświadczenia z prowadzonego przedmiotu na Kierunku Bezpieczeństwo Narodowe". W *Studia nad bezpieczeństwem. Teoria i praktyka. Człowiek – Technika – Środowisko*, redakcja Jerzy Konieczny, Mirosław Skarżyński. T. 1. Poznań: Wyd. Nauk WNPiD UAM, 2014.

Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP oraz niektórych innych ustaw. Dz. U. z 2011 r. nr 222, poz. 1323. [Ustawa ta wprowadziła pojęcie cyberprzestrzeni do następujących ustaw: *Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski* żywiołowej. Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.; *Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym*. Dz. U. z 2002 r. Nr 117, poz. 985,

z późn. zm.; *Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnej organom Rzeczypospolitej Polskiej*. Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.].

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.

Wiśniewski Bernard, Szyłkowska Monika. „Bezpieczeństwo w cyberprzestrzeni – wyzwania prawne i organizacyjne". W *Cyberprzestrzeń. Uzależnienia – Zagrożenia*, redakcja Mieczysław Koziński, Joanna Grubicka, Sylwia Kosznik-Biernacka. Słupsk: Wyd. ProPomerania, 2016.

Polityka ochrony cyberprzestrzeni w państwie współczesnym

Streszczenie

Rozwój technologii informatycznych, a zwłaszcza cyfryzacji spowodował powstanie globalnej sieci informatycznej i przeniesienie aktywności ludzkiej – zarówno tej pozytywnej, jak i negatywnej – do cyberprzestrzeni. Cyberprzestrzeń postrzega się jako medium komunikacji międzyludzkiej, która służy także do komunikacji między systemami teleinformatycznymi bez udziału człowieka. W okresie, kiedy panuje swoboda przepływu osób, towarów, informacji i kapitału państwo zmuszone zostało do prowadzenia odpowiedniej polityki ochrony cyberprzestrzeni pozwalającej skutecznie zapobiegać i zwalczać zagrożenia.

Celem artykułu nie jest przedstawienie historii rozwoju ochrony cyberprzestrzeni w Polsce i świecie, a jedynie zarysowanie problematyki związanej z analizą polityki ochrony cyberprzestrzeni – realizowanej przez administrację rządową, samorządową i inne podmioty działające w państwie – wobec wyzwań i zagrożeń w niej powstających.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, technologie informatyczne, zagrożenia, polityka

Policy on Cyberspace Protection in the Modern State

Summary

The development of information technology, especially digitisation, has resulted in the emergence of a global IT network and the transfer of human activity, both positive and negative into cyberspace. Cyberspace is perceived as a medium of interpersonal communication, which also serves to communicate between ICT systems without the participation of a human being. During the period of freedom of movement of people, goods, information and capital, the state was forced to pursue an appropriate cyber-security policy that would effectively prevent and combat threats to cyberspace.

The aim of this paper is not to present the history of cyberspace protection in Poland and the world, but rather to pinpoint the issues related to the analysis of cyber-security policy implemented by the government, the local governments and other entities active in the country to face the challenges and the threats arising in the cyberspace.

Keywords: cyberspace, cyber-security, information technology, threats, politics