SANDRA WOSZEK

ORCID: 0000-0003-3146-9779
DOI: 10.4467/20801335PBW.22.056.16947

Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej[1]

Abstrakt Artykuł został poświęcony cyberbezpieczeństwu jako priorytetowi gospodarki narodowej w kontekście globalnych zagrożeń gospodarki światowej mających wpływ na bezpieczeństwo państw. Zagrożenia cybernetyczne są z pewnością jednym z głównych zagrożeń bezpieczeństwa światowej gospodarki, a tym samym cyberbezpieczeństwo staje się priorytetem dla gospodarki narodowej, także dla Rzeczypospolitej Polskiej. Tezę tę potwierdzają m.in. statystyki incydentów cybernetycznych oraz liczne działania podejmowane przez państwa w celu zwalczania cyberzagrożeń.

Słowa kluczowe cyberbezpieczeństwo, bezpieczeństwo cybernetyczne, zagrożenia cybernetyczne, cyberprzestrzeń, cyberprzestępczość, cyberterroryzm.

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, obronionej na Wydziale Ekonomii i Finansów Uniwersytetu Ekonomicznego we Wrocławiu. Autorka wykorzystała rozdziały: I, II oraz III. Praca została nagrodzona w XI edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Cybersecurity of countries in the 21st century on the example of the Republic of Poland

Abstract

The article is devoted to the characteristics of cybersecurity as a priority of the national economy in the context of global threats to the security of the world economy. Cyber threats are certainly one of the main security threats to the global economy, and thus cybersecurity is becoming a priority for the national economy, also for the Republic of Poland. This thesis is confirmed, among others, by statistics of cyber incidents, which are growing dynamically, and numerous actions taken by states to combat cyber threats.

Keywords

cybersecurity, cyber threats, cyberspace, cybercrime, cyberterrorism.

Dynamiczny rozwój naukowo-techniczny, który rozpoczął się w XX w., diametralnie zmienił większość aspektów życia człowieka. Zarówno trzecia rewolucja przemysłowa, jak i czwarta (zwana rewolucją cyfrową) przyczyniły się do wielu zmian na świecie. Najważniejszą z nich jest powstanie komputera oraz sieci Internet[2]. Pierwsze komputery i sieci komputerowe początkowo były wykorzystywane głównie do celów naukowych i militarnych. Dopiero później zaczęły stawać się bardziej dostępne, czemu towarzyszył z kolei wzrost uzależnienia społeczeństwa od technologii teleinformatycznych[3]. Prężnie rozwijające się komputeryzacja, cyfryzacja i telekomunikacja doprowadziły do tego, że korzystanie z tych urządzeń to już codzienność, nieodłączny element życia człowieka. Szybki postęp technologiczny spowodował wprowadzenie nowych technologii określanych terminem „internet rzeczy" (ang. *Internet of Things*, IoT)[4]. To nowoczesna technologia pozwalająca użytkownikom na podłączenie do Internetu dowolnego urządzenia, a także kierowanie nim zdalnie, z każdego miejsca na Ziemi. Nazwa IoT jest stosowana nie tylko do rzeczy uniwersalnych

[2] D. Palka, K. Steculа, *Postęp technologiczny – dobrodziejstwo czy zagrożenie?*, w: *Innowacje w zarządzaniu i inżynierii produkcji*, t. 1, D. Palka, K. Steculа, R. Knosala (red.), Opole 2018, s. 587–588.

[3] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 27–37.

[4] D. Palka, K. Steculа, *Postęp technologiczny*…, s. 592.

jak telefon, komputer czy tablet, lecz także do maszyn i urządzeń w fabrykach. Internet rzeczy umożliwia użytkownikom działanie na niespotykaną wcześniej skalę. Efektem tej rewolucji informatycznej jest powstanie przestrzeni teleinformatycznej, zwanej inaczej cyberprzestrzenią, która jest „nową domeną ludzkiej aktywności"[5]. Powstanie cyberprzestrzeni wymusiło na użytkownikach ochronę sieci informatycznych, urządzeń oraz wykorzystywanych programów przed ich uszkodzeniami, atakami czy nieuprawnionym dostępem, określaną terminem „cyberbezpieczeństwo".

Cyberprzestrzeń

W literaturze przedmiotu cyberprzestrzeń jest określana jako (…) *zależny od czasu zestaw wzajemnie połączonych systemów informatycznych oraz ludzkich użytkowników, którzy wchodzą z tymi systemami w interakcję*[6]. Według rządowego dokumentu *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej* cyberprzestrzeń jest (…) *przestrzenią przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne* (…) *zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne*[7]. Podstawowym elementem tworzącym cyberprzestrzeń są zasoby materialne systemu teleinformatycznego. Jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania. Zapewnia on przetwarzanie, przechowywanie, wysyłanie i odbieranie danych dzięki sieciom telekomunikacyjnym. Siecią telekomunikacyjną możemy nazwać wszelkie urządzenia przekierowujące, systemy transmisyjne oraz nieaktywne elementy sieci[8]. Nie należy utożsamiać przestrzeni cybernetycznej jedynie z siecią Internet, gdyż przestrzeń ta obejmuje również sieci telekomunikacyjne i komputerowe. Można więc mówić, że są to wszystkie systemy informatyczne, które wspólnie tworzą sieć globalną.

---

[5] M. Lakomy, *Bezpieczeństwo teleinformatyczne (cyberbezpieczeństwo)*, w: *Bezpieczeństwo międzynarodowe w XXI wieku*, M. Lakomy, R. Zięba (red.), Warszawa 2018, s. 55.

[6] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, w: *Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton U.S. 2010, https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf [dostęp: 20 XII 2020].

[7] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, s. 5.

[8] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018, s. 25.

Według Tomasza R. Aleksandrowicza cyberprzestrzeń charakteryzuje się niezależnością od miejsca, czasu, odległości czy granic, jak również częściową anonimowością i ograniczoną możliwością ustalenia sprzętu, z którego się korzysta[9].

Cyberbezpieczeństwo

Według literatury przedmiotu (…) *cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa*[10]. Można więc mówić, że cyberbezpieczeństwo jest niczym innym jak (…) *procesem zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni*[11].

W słowniku zawartym w *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*[12] można znaleźć definicję terminu „cyberbezpieczeństwo" rozumianego jako bezpieczeństwo sieci i systemów informatycznych oraz bezpieczeństwo teleinformatyczne. Zgodnie z definicją cyberbezpieczeństwo to (…) *odporność systemów teleinformatycznych, przy danym 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 poprzez te sieci i systemy informatyczne*[13].

Jeszcze inaczej definiuje się to pojęcie w środowisku wojskowym. Według organizacji związanych z wojskowością bezpieczeństwo cybernetyczne dzieli się na obszar cyberobrony (cyberbezpieczeństwo militarne, które jest związane z prowadzoną walką zbrojną i z siłami zbrojnymi) oraz na obszar cyberochrony (cyberbezpieczeństwo o wymiarze pozamilitarnym)[14]. Zakres tak rozumianego bezpieczeństwa ma wymiar strategiczny.

---

[9] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 12.

[10] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Zeszyty Naukowe Wydawnictwa Uniwersytetu Ekonomicznego" 2014, nr 2, s. 138.

[11] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 31.

[12] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2020*, Ministerstwo Cyfryzacji, Warszawa 2017.

[13] Tamże, s. 28.

[14] S. Koziej, *Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO*, https://koziej.pl/wp-content/uploads/2016/10/IBK-Cyberbezpiecze%C5%84stwo-25.10.2016.pdf, s. 5 [dostęp: 20 XII 2020].

Według Tomasza Hoffmana cyberbezpieczeństwo jest nową dziedziną bezpieczeństwa państwa, która ma związek z cyberprzestępczością oraz cyberterroryzmem[15].

Cyberterroryzm a cyberprzestępczość

W obliczu dynamicznego rozwoju technologii informatycznej i uzależnienia państw od udogodnień, które ona oferuje, państwa coraz częściej stają przed nowym wyzwaniem, jakim jest cyberterroryzm (zwany inaczej terroryzmem informacyjnym, hi-tech terroryzmem). W literaturze przedmiotu opisano cyberterroryzm jako (…) *politycznie motywowany atak lub groźbę ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów*[16].

Według Roberta Kośli cyberterroryzm jest działaniem, które blokuje, zniekształca lub niszczy informację przetwarzaną, przechowywaną bądź przekazywaną w systemach teleinformatycznych. Zwraca on również uwagę na to, że wykorzystanie tych systemów prowadzi do dezinformacji, gdyż celem ataku jest właśnie informacja, a nie sam system[17]. Aby jednak móc mówić o cyberterroryzmie, niepożądane działania muszą wywołać potężne szkody i strach wśród społeczeństwa lub też muszą być skutkiem przemocy wobec osób lub mienia, np. może to być atak, który prowadzi do śmierci człowieka bądź znacznych obrażeń ciała.

Również większe ataki na infrastrukturę krytyczną mogą być zaliczane do cyberterroryzmu. Jednocześnie przyjmuje się, że ataki na usługi o niewielkim znaczeniu nie są cyberterroryzmem[18]. Jego sprawcami mogą być zarówno osoby z danego państwa, jak i spoza niego. Mogą to być także organizacje terrorystyczne czy ugrupowania rebelianckie. Cyberterroryzm jest jednym z najbardziej zaawansowanych i największych zagrożeń teleinformatycznych. Można wręcz przyjąć, że cyberterroryzm to jedno z głównych zagrożeń dla świata w XXI w., gdyż wpływa na system

[15] T. Hoffmann, *Główni aktorzy cyberprzestrzeni i ich działalność*, w: *Cyberbezpieczeństwo wyzwaniem XXI wieku*, T. Dębowski (red.), Łódź–Wrocław 2018, s. 27–28.

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

[17] R. Kośla, *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, wystąpienie na konferencji w Bemowie, 29 XI 2002 r., za: P. Jankowski, *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*, „Młody Jurysta" 2018, nr 4, s. 18.

[18] I. Oleksiewicz, *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1, s. 54.

polityczny i gospodarczy państwa, a także stabilność jego instytucji[19]. Często mylnie utożsamia się terroryzm informacyjny z cyberatakiem. Błędem jest uznawanie każdego ataku w cyberprzestrzeni za cyberterroryzm, np. niepożądanych działań skierowanych na bazy danych, nawet jeśli powodują spore straty materialne[20].

Cyberprzestępczość jest jedną z nowszych, a jednocześnie jedną z najszybciej rozwijających się form przestępczości transgranicznych. W polskim prawie nie ma przyjętej jednej definicji legalnej cyberprzestępczości. Według Organizacji Narodów Zjednoczonych cyberprzestępczość można zdefiniować w ujęciu wąskim lub szerokim:

> Cyberprzestępstwo w wąskim sensie oznacza wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych. (…) Cyberprzestępstwo w szerokim sensie jest rozumiane jako przestępstwo dotyczące komputerów, czyli chodzi o wszelkie nielegalne działania popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[21].

W literaturze przedmiotu podaje się, że główną różnicą między już wcześniej wspomnianym terroryzmem a cyberprzestępczością są intencje czy motywy przeprowadzenia ataku, którymi kierują się sprawcy (np. motyw finansowy). Natomiast dla cyberterrorystów są to najczęściej motywy polityczne, religijne bądź społeczne[22]. Kolejną różnicą jest częstość występowania. W przestrzeni cybernetycznej znacznie częstszym zagrożeniem niż cyberterroryzm czy nawet wojna cybernetyczna jest cyberprzestępczość[23].

---

[19] T. Hoffmann, *Główni aktorzy cyberprzestrzeni*…, s. 27–28.

[20] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia informatycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, r. 46, nr 1, s. 178–179.

[21] R. Szymczykiewicz, *Czym jest cyberprzestępstwo?*, Infor, 28 XII 2011 r., https://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,2,Czym-jest-cyberprzestepstwo.html [dostęp: 20 XII 2020].

[22] M. Górka, *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*, „Cywilizacja i Polityka" 2017, t. 15, nr 15, s. 304–305.

[23] Tamże.

Cyberbezpieczeństwo państwa – identyfikacja zagrożeń globalnych związanych z bezpieczeństwem państwa

Współczesne państwa są wystawione na wiele ogólnoświatowych zagrożeń, w tym wiele zjawisk, np. zmiany klimatyczne, które w negatywny sposób oddziałują na ich bezpieczeństwo. Postępująca globalizacja może wywołać skutki zarówno pozytywne, jak i negatywne – z jednej strony ułatwiła dzielenie się informacjami i danymi, z drugiej zaś przyczynia się do rozprzestrzeniania się zagrożeń na cały świat. Również niestabilna sytuacja (m.in. polityczna) na świecie wpływa negatywnie na środowisko bezpieczeństwa, oddziałuje na państwa i pogłębia ich destabilizację. Dodatkowo muszą one zmierzyć się z wyzwaniami i zagrożeniami, które niejednokrotnie nabierają nowego znaczenia[24]. Jednym z nich jest konieczność przystosowania się do wyzwań globalizacji, gdyż nieprzystosowanie się do zmieniającej się rzeczywistości powoduje utratę przez państwo pozycji na arenie międzynarodowej[25].

W celu dobrego zrozumienia zagadnienia zagrożenia globalnego wpływającego na bezpieczeństwo państwa warto przedstawić definicję i dziedziny bezpieczeństwa państwa, jak również klasyfikację zagrożeń. Bezpieczeństwo państwa (bezpieczeństwo narodowe), według słownika Biura Bezpieczeństwa Narodowego (BBN), jest (…) *rodzajem bezpieczeństwa, którego podmiotem jest naród zorganizowany w państwo*[26]. Zintegrowany charakter współczesnego bezpieczeństwa państwa, czyli jego wielowymiarowość i kompleksowość, pozwala na wyróżnienie podstawowych dziedzin, sektorów, jak również obszarów transsektorowych (transdziałowych). Bezpieczeństwo państwa można podzielić na cztery dziedziny i powiązane z nimi sektory[27]:

1) obronna; obejmuje bezpieczeństwo militarne; obejmuje sektory: dyplomatyczny w dziedzinie bezpieczeństwa, militarny, wywiadowczy,
2) ochronna; obejmuje bezpieczeństwo cywilne; obejmuje sektory: kontrwywiadowczy, prawa i porządku publicznego, ratownictwa,
3) społeczna; obejmuje sektory: kulturowy, edukacyjny, socjalny, demograficzny, migracyjny i inne,
4) gospodarcza; obejmuje sektory: finansowy, energetyczny, transportowy, infrastruktury krytycznej, środowiska naturalnego i inne.

[24] S. Koziej, *Identyfikacja zagrożeń globalnych dla bezpieczeństwa międzynarodowego*, „Przyszłość. Świat-Europa-Polska" 2012, nr 2, s. 30–31.

[25] *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, BBN, Warszawa 2013, s. 109–110.

[26] *(MINI)SŁOWNIK BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa*, BBN, http://katedrawiss.uwm.edu.pl/sites/default/files/download/202005/minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.pdf [dostęp: 9 II 2021].

[27] S. Koziej, *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej: aspekty strategiczne*, „Myśl Ekonomiczna i Polityczna" 2013, nr 1, s. 146.

Transsektorowe (transdziedzinowe, transpodmiotowe) obszary bezpieczeństwa to (…) *części zintegrowanego bezpieczeństwa narodowego obejmujące swą treścią problematykę właściwą jednocześnie różnym podmiotom, dziedzinom i sektorom tego bezpieczeństwa*[28], np. cyberbezpieczeństwo czy bezpieczeństwo antyterrorystyczne. Obszary te są tworzone najczęściej ze względu na nowe i pilne potrzeby państwa, jak w wymienionym przypadku – ze względu na globalne zagrożenie cyberprzestępczością i cyberterroryzmem.

Przechodząc do identyfikacji zagrożeń globalnych, warto najpierw przytoczyć definicję samego słowa „zagrożenie". Zagrożenie to (…) *zakres zdarzeń wywołanych celowo lub losowych, które wywierają negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa, na warunki bytowania ludności oraz stan środowiska naturalnego*[29]. Globalne zagrożenia to te, które odnoszą się do całego świata, globu, a nie pojedynczego państwa.

Według Stanisława Kozieja (szefa BBN w latach 2010–2015[30]) istnieje wiele rodzajów zagrożeń, w różnych dziedzinach bezpieczeństwa państwa. Zgodnie z tematyką niniejszego artykułu warto skupić się na dwóch z nich – obronnej i ochronnej. Przywołany autor wyróżnia jedynie trzy zagrożenia transnarodowe o zasięgu globalnym, które są najbardziej dostrzegalne[31]:

1) rozpowszechnianie broni masowego rażenia,
2) terroryzm,
3) cyberzagrożenia.

Ostatnim zagrożeniem wyszczególnionym przez Kozieja są cyberzagrożenia, a dokładniej – podatność państw na nie. Państwo, które jest nowoczesne i rozwinięte, zapewnia obywatelom dostęp do Internetu, co wiąże się z koniecznością zapewnienia bezbłędnego funkcjonowania systemów teleinformatycznych, jak również nieustannym ich sterowaniem i monitorowaniem[32]. W przypadku sieci Internet. mającej ogromny zasięg, i globalnej skali systemów informatycznych nieuniknione jest narażanie się państw na wiele ataków cybernetycznych. Postępujący rozwój technologiczny będzie powodował ciągłe powstawanie i doskonalenie stosowanych metod cyberataków[33]. Wiele zagrożeń, które współcześnie są zaliczane do tradycyjnych,

[28] *(MINI)SŁOWNIK BBN: Propozycje nowych terminów…*

[29] *Zagrożenia we współczesnym świecie jako temat edukacji geograficznej*, T. Michalski (red.), Warszawa 2008, s. 8.

[30] Strona prof. dr. hab. Stanisława Kozieja, https://koziej.pl/o-mnie/ [dostęp: 9 II 2021].

[31] S. Koziej, *Identyfikacja zagrożeń globalnych…*, s. 31–33.

[32] *Biała Księga Bezpieczeństwa Narodowego…*, s. 116–117.

[33] Tamże.

zacznie występować wówczas w cyberprzestrzeni, jak np. cyberprotesty[34]. Zagrożenia czyhające na państwa w przestrzeni wirtualnej są naprawdę ogromne.

Coraz częściej zwraca się uwagę na to, że właśnie globalne zagrożenia dotyczące cyberprzestępczości i cyberterrorzymu są kwalifikowane jako sytuacja, która zagraża stabilności i bezpieczeństwu państwa. Najlepszym tego przykładem jest art. 12 *Koncepcji strategicznej obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego*, który brzmi:

> Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne, biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności[35].

Cyberzagrożenia powoli naruszają zasadę suwerennej równości państw[36]. Złowrogie ataki w cyberprzestrzeni na państwa mogą powodować przeniesienie sporu na inną płaszczyznę, poza przestrzeń cybernetyczną. Początkowo ta przestrzeń miała inne zastosowanie, jednak z czasem zauważono, że coraz więcej ataków terrorystycznych jest przenoszonych właśnie do cyberprzestrzeni, co destrukcyjnie wpływa na prawidłowe funkcjonowanie sieci poszczególnych państw i ich systemy teleinformatyczne. Znaczenie bezpieczeństwa informacyjnego i cyberbezpieczeństwa dla wielu państw jest priorytetem w utrzymaniu prawidłowego poziomu bezpieczeństwa narodowego[37].

Cyberbezpieczeństwo Rzeczypospolitej Polskiej – krajowy system cyberbezpieczeństwa

Krajowy system cyberbezpieczeństwa musi być regulowany przez państwo w celu zapewnienia bezpieczeństwa cybernetycznego społeczeństwu oraz innym podmiotom narażonym na cyberataki. System ten ma zapewniać bezpieczeństwo cybernetyczne na poziomie krajowym, zwłaszcza niezakłócone świadczenie usług

[34] Zob. *(MINI)SŁOWNIK BBN: Propozycje nowych terminów…*

[35] *Koncepcja strategiczna NATO z 2010 r.*, „Bezpieczeństwo Narodowe" 2014, nr 29, s. 206.

[36] Zob. *Deklaracja zasad prawa międzynarodowego dotyczących przyjaznych stosunków i współdziałania państw zgodnie z Kartą Narodów Zjednoczonych. Rezolucja Zgromadzenia Ogólnego 2625(XXV), 24 października 1970*, http://www.grocjusz.edu.pl/Documents/dekl2625.html (przyp. red.).

[37] *Biała Księga Bezpieczeństwa Narodowego…*, s. 116–117.

kluczowych czy cyfrowych[38]. W Polsce podstawowym aktem prawnym, który reguluje obszar cyberbezpieczeństwa, jest ustawa o krajowym systemie cyberbezpieczeństwa[39] przygotowana przez Ministerstwo Cyfryzacji. Ustawą tą wdrożono do systemu prawnego dyrektywę 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[40], zwanej Dyrektywą NIS, którą musiał przyjąć każdy członek Unii Europejskiej. Celem ustawodawcy oprócz wprowadzenia nadzoru i kontroli zgodnie z przypisami omawianej ustawy jest również określenie organizacji i funkcjonowania całego systemu bezpieczeństwa cybernetycznego państwa oraz ustalenie zakresu strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej. Zgodnie z Dyrektywą NIS ustawa o krajowym systemie cyberbezpieczeństwa nie obejmuje przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy podlegają europejskim i krajowym wymaganiom sektorowym z zakresu cyberbezpieczeństwa, podmiotów wykonujących działalność leczniczą, a także takich, które są tworzone przez szefów Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu[41].

W omawianej ustawie „cyberbezpieczeństwo" definiuje się jako (…) *odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*[42]. Każde wydarzenie, które ma lub może mieć wpływ na bezpieczeństwo cybernetyczne Rzeczypospolitej Polskiej, jest określane w rozumieniu ustawy jako incydent[43]. Wskazano w niej kilka rodzajów incydentów w zależności od podmiotu, który je zgłasza, oraz skutków (wielkości szkody), jakie on powoduje, a także określono zarządzanie tymi incydentami.

Zgodnie z ustawą wyróżnia się[44]:

– incydent krytyczny – wpływa na gospodarkę państwa, skutkuje znaczną szkodą dla bezpieczeństwa i funkcjonowania instytucji publicznych,

---

[38] *Krajowy system cyberbezpieczeństwa*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- [dostęp: 13 IV 2021].

[39] *Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa* (t.j. DzU z 2020 r. poz. 1369, ze zm.).

[40] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. Urz. UE L 194 z 19 VII 2016 r.).

[41] C. Banasiński, W. Nowak, *Europejski i Krajowy System Cyberbezpieczeństwa*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 160.

[42] Ustawa o krajowym systemie cyberbezpieczeństwa, art. 2 ust. 1 pkt 4.

[43] Tamże, art. 2 ust. 1 pkt 5.

[44] Tamże, art. 2 ust. 1 pkt 6, pkt 7, pkt 8, pkt 9.

– incydent poważny – znacząco obniża jakość lub przerywa ciągłość świadczenia usług; progiem, który określa skalę oraz nazwę danego incydentu, jest liczba użytkowników dotknięta incydentem, czas jego oddziaływania oraz obszar, który został nim dotknięty,
– incydent istotny – ma decydujący wpływ na świadczenie usługi cyfrowej,
– incydent w podmiocie publicznym – powoduje lub może powodować obniżenie jakości lub przerywanie realizacji zadania publicznego przez podmiot publiczny wskazany w ustawie.

W ustawie podjęto również temat analizy ryzyka oraz zarządzania nim. Ryzyko w obszarze cyberbezpieczeństwa to (…) *kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji*[45].

Strategia cyberbezpieczeństwa państwa na lata 2019–2024

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[46] – aktualnie obowiązująca – jest narzędziem, dzięki któremu państwo może koordynować krajowy system cyberbezpieczeństwa. Wprowadzenie *Strategii* było wymogiem europejskiej Dyrektywy NIS oraz wspomnianej już ustawy o krajowym systemie cyberbezpieczeństwa. Jej wdrożenie jest istotne dla bezpieczeństwa kraju ze względu na zawarte w niej zapisy dotyczące przeciwdziałania incydentom cybernetycznym i reagowania na nie. *Strategię* opracowuje minister właściwy ds. informatyzacji wraz z pełnomocnikiem ds. cyberbezpieczeństwa, innymi ministrami, jak również kierownikami urzędów centralnych, a zaakceptować ją musi Rada Ministrów[47].

Realizacja celów strategicznych ma m.in. wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym. W omawianym dokumencie uwzględniono cele strategiczne, środki polityczne i regulacyjne podjęte przez państwo w celu osiągnięcia, a następnie utrzymania wysokiego poziomu bezpieczeństwa cybernetycznego. W dokumencie ochroną objęto głównie kluczowe sektory, które są wymienione w ustawie o krajowym systemie cyberbezpieczeństwa, usługi cyfrowe i podmioty publiczne. Cele strategiczne są ustalane na pięć lat, a co dwa lata następuje ich przegląd.

[45] Ustawa o krajowym systemie cyberbezpieczeństwa, art. 2 ust. 1 pkt 12.

[46] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2019–2024*, Ministerstwo Cyfryzacji, Warszawa 2019, s. 8–9.

[47] C. Banasiński, W. Nowak, *Europejski i Krajowy System Cyberbezpieczeństwa*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 171–172.

Strategia jest monitorowana i na bieżąco weryfikowana przez ministra właściwego ds. informatyzacji pod kątem wdrażania jej w życie. W *Strategii* wyróżniono pięć celów szczegółowych, których realizacja pomaga osiągnąć główny cel, którym jest (…) *podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym*[48].

Pierwszy cel szczegółowy *Strategii* to rozwój krajowego systemu cyberbezpieczeństwa. Jego realizacja zapewni cyberbezpieczeństwo na poziomie krajowym, m.in. zwiększy cyberbezpieczeństwo świadczenia usług w najważniejszych sektorach i usług cyfrowych wchodzących w skład infrastruktury krytycznej, a także zwiększy zdolność zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym. Drugim celem szczegółowym jest podniesienie poziomu odporności systemów, zarówno administracji publicznej, jak i sektora prywatnego, oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. Tutaj można wyróżnić skupienie się na dobrych praktykach, szkoleniach, audytach w zakresie cyberbezpieczeństwa. Trzeci cel szczegółowy *Strategii* to zwiększenie potencjału narodowego dotyczącego bezpieczeństwa w cyberprzestrzeni. Jego realizacja polega m.in. na rozbudowie zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa, a także uzyskaniu zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni. Czwarty cel to budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. Osiągnięcie tego celu jest bardzo ważne, gdyż wiele zależy od nas samych. Zwraca się przy tym uwagę na znaczenie podnoszenia kompetencji nie tylko osób zajmujących się cyberbezpieczeństwem, lecz także pozostałych obywateli, aby stworzyć warunki bezpiecznego korzystania z cyberprzestrzeni. Ostatnim celem zawartym w *Strategii* jest zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa przez aktywną współpracę międzynarodową z organizacjami, np. Organizacją Narodów Zjednoczonych czy Organizacją Bezpieczeństwa i Współpracy w Europie[49].

Działania państwa prowadzone w celu utrzymania poziomu cyberbezpieczeństwa

Cyberbezpieczeństwo to ważny element istnienia państwa powiązany z wieloma organizacjami oraz innymi podmiotami. Znaczenie bezpieczeństwa cybernetycznego systematycznie rośnie, dlatego też państwa stoją przed ważnym zadaniem, jakim

[48] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*…, s. 10.

[49] Tamże, s. 11–29.

jest zapewnienie poziomu cyberbezpieczeństwa swoim obywatelom, przedsiębiorstwom oraz instytucjom. Oprócz zagwarantowania dostatecznego poziomu bezpieczeństwa należy skupić się na funkcjonowaniu podmiotów w warunkach zagrożenia i rozwijaniu ich świadomości istnienia takich zagrożeń.

Pod terminem „cyberzagrożenie" rozumie się wszystkie czynności, które uniemożliwiają danemu podmiotowi zaspokojenie potrzeby informacyjnej, będącej (…) *podstawą procesów decyzyjnych*[50], a więc również podstawą kształtowania działania. Utrzymanie danego poziomu cyberbezpieczeństwa państwa wymaga wprowadzenia modelu systemu działania. Ważną częścią systemu utrzymującego dany poziom bezpieczeństwa cybernetycznego państwa jest moduł kierowania. Za podstawowy element w tym module uznaje się świadomość sytuacji, czyli – w tym przypadku – wiedzę na temat występowania cyberzagrożeń i ryzyka, jakie one niosą za sobą. Bez niej dany podmiot nie jest w stanie podjąć odpowiednich działań, aby zapobiec cyberzagrożeniu i jego skutkom. Dlatego też przyjmuje się, że w module kierowania istotną rolę odgrywa informacja i to ona jest najważniejsza przy utrzymaniu danego poziomu cyberbezpieczeństwa państwa. Dzięki odpowiedniej wiedzy o cyberbezpieczeństwie podejmowane działania są działaniami racjonalnymi. W modelu systemu działania wyróżnia się trzy ważne moduły[51].

Moduł kierowania pozwala podmiotowi na pozyskiwanie informacji o cyberzagrożeniach oraz wykorzystanie jej do racjonalnego działania. Moduł kierowania to ciągłe podejmowanie decyzji i koordynowanie poczynań podczas osiągania danego stanu cyberbezpieczeństwa w każdej sytuacji, w jakiej znajduje się lub może się znaleźć podmiot – stanie normalnego funkcjonowania, kryzysu bądź wojny[52].

Moduł informacyjny, jak sama nazwa wskazuje, odnosi się do istotnych informacji. Wynika z niego świadomość stanu bezpieczeństwa (cyberświadomość), dlatego jest on tak ważny dla podmiotu. Świadomość sytuacyjną zdefiniowano jako (…) *świadomą znajomość najbliższego otoczenia i wydarzeń w nim zachodzących. Świadomość sytuacyjna obejmuje postrzeganie elementów otoczenia, rozumienie ich znaczenia i relacji między nimi oraz projekcję ich przyszłych stanów*[53]. Dzięki świadomości sytuacyjnej możliwe jest utrzymywanie stanu świadomości cybernetycznej, a co za tym idzie – rozwijanie systemów wczesnego wykrywania cyberzagrożeń[54].

---

[50] R. Szpyra, *Cyberbezpieczeństwo i cyberaktywność militarna*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 233.

[51] Tamże, s. 234–238.

[52] Tamże.

[53] *APA Dictionary of Psychology*, American Psychological Association, https://dictionary.apa.org/situation-awareness [dostęp: 21 IV 2021].

[54] R. Szpyra, *Cyberbezpieczeństwo i cyberaktywność*…, s. 234–238.

Moduł operacyjny, w przeciwieństwie do modułów kierowania i informacyjnego, jest nastawiony na redukowanie cyberzagrożeń. Chęć utrzymywania wysokiego poziomu cyberbezpieczeństwa zmusza podmiot (w tym przypadku państwo) do ciągłych działań przeciw zagrożeniom cybernetycznym. Rezultatem tych działań jest tworzenie cyberodporności państwa[55]. Można zatem mówić o odstraszaniu przed cyberatakami przed ich wystąpieniem albo o niwelowaniu cyberataków już po ich wystąpieniu. Bardzo dobry system powstrzymywania cyberataków to najczęściej też najlepszy sposób odstraszania. Dla państw do najgroźniejszych zagrożeń w cyberprzestrzeni należy zbrojny cyberatak militarny. Dobrą praktyką państwa w takim przypadku jest odstraszanie, lecz nie zawsze okazuje się ono efektywne. Należy wówczas zadbać o to, aby dany cyberatak został zahamowany. Wszystko jednak zależy od cyberzdolności militarnych, np. wyszkolenia jednostki wojskowej odpowiedzialnej za obronę cyberprzestrzeni czy przyjętej polityki i ustalonych standardów.

Nie ma wątpliwości, że aby osiągnąć wysoki poziom cyberbezpieczeństwa, państwo musi zarówno wyznaczyć cele strategiczne, do których będzie dążyć, jak i realizować zadania z zakresu bezpieczeństwa cybernetycznego infrastruktury krytycznej, która jest ważnym elementem tego całego procesu[56].

Ochrona infrastruktury krytycznej Rzeczypospolitej Polskiej w cyberprzestrzeni

Infrastruktura krytyczna stała się jednym z głównych elementów bezpieczeństwa narodowego, który podlega szczególnej ochronie, gdyż jest podstawą zapewnienia rozwoju gospodarczego oraz prawidłowego funkcjonowania państwa. Infrastruktura krytyczna, jak podaje Rządowe Centrum Bezpieczeństwa, to (…) *rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa*[57]. W ustawie o zarządzaniu kryzysowym[58] infrastrukturą krytyczną nazwano (…) *systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji*

[55] Zob. szerzej: https://itwiz.pl/od-bezpieczenstwa-do-cyberodpornosci-nowy-paradygmat-ochrony/ (przyp. red.).

[56] R. Szpyra, *Cyberbezpieczeństwo i cyberaktywność*…, s. 234–239.

[57] *Infrastruktura krytyczna*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp: 14 IV 2022].

[58] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j. DzU z 2022 r. poz. 261, ze zm.).

i przedsiębiorców[59]. W jej skład nie wchodzą wszystkie obiekty, lecz tylko te, które są wyróżnione w ustawie. W Rzeczypospolitej Polskiej do infrastruktury krytycznej zalicza się 11 systemów, w tym: zaopatrzenia w wodę, zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatyczny finansowe, ochrony zdrowia czy też transportowe[60]. Te systemy są ze sobą połączone, czego przykładem może być system sieci teleinformatycznych, wykorzystywany również w systemie ochrony zdrowia.

Systemy infrastruktury krytycznej mogą zostać zniszczone, uszkodzone bądź mogą wystąpić zakłócenia w ich funkcjonowaniu na skutek awarii spowodowanych siłami natury lub działaniami człowieka. W przypadku wystąpienia zagrożenia lub kryzysu ich wzajemne połączenie naraża sieci i systemy na powstanie efektu domina, czyli załamania się relacji między nimi[61]. Wadliwy system infrastruktury krytycznej jest dla państwa nie lada wyzwaniem, nie tyle finansowym, związanym z naprawą obiektu, ile z możliwością wystąpienia zagrożenia życia obywateli czy pogorszeniem się komfortu ich bytu. Dlatego też tak istotną sprawą jest zapewnienie bezpieczeństwa systemom tworzącym infrastrukturę krytyczną, co uchroni społeczeństwo przed skutkami działań zarówno natury, jak i drugiego człowieka (np. cyberataków).

Ochrona infrastruktury krytycznej polega m.in. na szybkim usuwaniu usterek, tak aby w jak najmniejszym stopniu negatywnie wpłynęły na funkcjonowanie państwa i samopoczucie obywateli. Według Rządowego Centrum Bezpieczeństwa ochrona infrastruktury krytycznej to (…) *wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie*[62]. Warto zwrócić również uwagę na to, że infrastruktura krytyczna państwa to elementy, które funkcjonują samodzielne, lecz są ze sobą połączone. Wpływ na nią mają również sieci teleinformatyczne istniejące w innych państwach. Te zależności powodują, że infrastruktura krytyczna jest narażona na ataki cybernetyczne przeprowadzane zarówno z danego kraju, jak i spoza niego – praktycznie z całego świata.

Ważne pytanie badawcze, które należy postawić, brzmi: dlaczego infrastruktura tak istotna dla funkcjonowania państwa jest tak podatna na uszkodzenia? Systemy

[59] Tamże, art. 3 ust. 1 pkt 2.

[60] Tamże, art. 3 ust. 1 pkt 2.

[61] W. Nowak, *Ochrona infrastruktury krytycznej w cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 175.

[62] *Systemy infrastruktury krytycznej*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej [dostęp: 14 IV 2022].

infrastruktury krytycznej są tworzone przez ludzi. To właśnie ten czynnik – jako jeden z czterech – jest wyróżniany w zagrożeniach, które mogą dotknąć infrastrukturę krytyczną. Do zagrożeń, które mogą być wywołane przez czynnik ludzki, można zaliczyć m.in.: brak szkoleń załogi, brak znajomości polityki bezpieczeństwa, luki prawne oraz terroryzm[63]. Najczęściej to właśnie człowiek jest odpowiedzialny za niewłaściwe wykorzystywanie systemów czy też za mało efektywne rozwiązania w obszarze bezpieczeństwa cybernetycznego. Czynnika ludzkiego nie można wyeliminować, dlatego znaczenia nabierają działania prewencyjne, polegające na dokształcaniu społeczeństwa na jak najwcześniejszym etapie nauki, a także dzieleniu się dobrymi praktykami w zakresie cyberbezpieczeństwa z innymi państwami.

Innym czynnikiem mającym wpływ na zagrożenia infrastruktury krytycznej jest technologia. Mowa tu głównie o błędach popełnianych podczas produkcji sprzętów, na które podmiot kupujący produkt nie ma wpływu. Jedyną radą jest współpraca z wieloma dostawcami, u których są dokonywane zakupy sprzętu do poszczególnych instytucji czy przedsiębiorstw. Zwraca się również uwagę na to, że w tym obszarze najważniejsze jest zapewnienie bezpieczeństwa oprogramowania i transmisji danych[64].

Koordynowanie infrastruktury krytycznej powinno odbywać się na poziomie centralnym lub regionalnym, aby w sytuacji zagrożenia móc jak najszybciej zareagować na daną sytuację. Państwo, które jest odpowiedzialne za zapewnienie bezpieczeństwa, musi na bieżąco regulować i wprowadzać nowe rozwiązania, m.in. nadzorować podmioty będące właścicielami poszczególnych elementów infrastruktury krytycznej. W literaturze przedmiotu wyróżniono pięć zagrożeń związanych z cyberatakami, które mogą stworzyć niebezpieczeństwo dla poprawnego funkcjonowania infrastruktury krytycznej[65]:

1) przerwanie przepływu informacji,
2) zaburzenie przepływu informacji (spowolnienie lub zablokowanie dostępu),
3) zmiana informacji (nieuprawniony dostęp),
4) kradzież danych,
5) kompromitacja osoby.

W uwagi na te zagrożenia najważniejsze w ochronie cybernetycznej infrastruktury krytycznej są m.in. współpraca sektorowa, kontrola dostępu, plany awaryjne, bezpieczeństwo oprogramowania oraz bezpieczeństwo sieci bezprzewodowych[66].

---

[63] W. Nowak, *Ochrona Infrastruktury Krytycznej w Cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*…, s. 179.

[64] Tamże, s. 178.

[65] Tamże, s. 180–181.

[66] *Narodowy Program Ochrony Infrastruktury Krytycznej.* Załącznik nr 1: *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, Rządowe

Jak podaje Rządowe Centrum Bezpieczeństwa, (…) *cyberataki na systemy IK stały się częścią konfliktów cybernetycznych cyberprzestrzeni, w tym konfliktów między państwami*[67]. Nie można więc bagatelizować tego zjawiska i z całą starannością należy zadbać o ochronę cybernetyczną wszystkich sektorów infrastruktury krytycznej, zwłaszcza tych, które są połączone z systemem sieci teleinformatycznych.

Podsumowanie

Z przedstawionej charakterystyki cyberbezpieczeństwa państw, cyberterroryzmu oraz cyberprzestępczości wynika, że zagrożenia cybernetyczne są z pewnością jednym z głównych zagrożeń globalnych gospodarki światowej związanej z bezpieczeństwem. Dlatego też priorytetem gospodarki narodowej każdego państwa, w tym również Rzeczypospolitej Polskiej, staje się bezpieczeństwo cybernetyczne. Z analizy opracowań poświęconych temu zagadnieniu można wywnioskować, że problem cyberzagrożeń będzie dynamicznie wzrastał. Cyberataki zmusiły państwa do wykreowania nowego rodzaju bezpieczeństwa, zwanego cyberbezpieczeństwem. Zagrożenia w cyberprzestrzeni są dla państwa bardzo kosztowne, powodują wiele szkód, szczególnie jeśli zostały zaatakowane sektory infrastruktury krytycznej. Dlatego też państwa muszą dołożyć wszelkich starań, aby zapewnić bezpieczeństwo właśnie tym sektorom.

Walkę z zagrożeniami cybernetycznymi podejmuje wiele organizacji i stowarzyszeń międzynarodowych. Celem ich działania jest głównie upowszechnianie w społeczeństwie wiedzy o cyberatakach oraz budowanie odporności państw na zagrożenia w cyberprzestrzeni, np. poprzez przeprowadzanie szkoleń personelu odpowiedzialnego za cyberbezpieczeństwo czy dzielenie się z innymi państwami dobrymi praktykami. W ostatnich latach cyberbezpieczeństwo stało się dla Rzeczypospolitej Polskiej jednym z głównych priorytetów działania. Rok 2021 był dla Polski rokiem rekordowym pod względem zgłoszonych incydentów teleinformatycznych (762 175), z czego 26 899 było faktycznymi incydentami. O eskalacji zagrożeń cybernetycznych świadczy porównanie z danymi z 2020 r., w którym liczba zgłoszonych incydentów potencjalnych wynosiła 246 107, a faktycznych – 23 309[68]. Przyczyn tego

Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/wp-content/uploads/Za%C5%82%C4%85cznik-nr-1-Standardy-s%C5%82u%C5%BC%C4%85ce-zapewnieniu-sprawnego-funkcjonowania-infrastruktury-krytycznej-%E2%80%93-dobre-praktyki-i-rekomendacje.pdf, s. 76 [dostęp: 14 IV 2021].

[67] Tamże, s. 72.

[68] *Rośnie liczba cyberzagrożeń*, Serwis Rzeczypospolitej Polskiej, 23 II 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosnie-liczba-cyberzagrozen [dostęp: 24 IV 2022].

zjawiska należy upatrywać w powstawaniu coraz to nowszych metod działania w cyberprzestrzeni, jak również w rozwijaniu przez cyberaktorów swoich umiejętności.

Bibliografia

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 11–28.

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018.

Banasiński C., Nowak W., *Europejski i Krajowy System Cyberbezpieczeństwa*, w: *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2013.

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

Górka M., *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*, „Cywilizacja i Polityka" 2017, t. 15, nr 15, s. 295–315.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Zeszyty Naukowe Wydawnictwa Uniwersytetu Ekonomicznego" 2014, nr 2, s. 125–139.

Hoffmann T., *Główni aktorzy cyberprzestrzeni i ich działalność*, w: *Cyberbezpieczeństwo wyzwaniem XXI wieku*, T. Dębowski (red.), Łódź–Wrocław 2018, s. 11–30.

Jankowski P., *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*, „Młody Jurysta" 2018, nr 4, s. 13–27.

Koncepcja strategiczna NATO z 2010 r., „Bezpieczeństwo Narodowe" 2014, nr 29, s. 203–216.

Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, wystąpienie na konferencji w Bemowie, 29 XI 2002 r.

Koziej S., *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej: aspekty strategiczne*, „Myśl Ekonomiczna i Polityczna" 2013, nr 1, s. 143–168.

Koziej S., *Identyfikacja zagrożeń globalnych dla bezpieczeństwa międzynarodowego*, „Przyszłość. Świat-Europa-Polska" 2012, nr 2, s. 30–33.

Lakomy M., *Bezpieczeństwo teleinformatyczne (cyberbezpieczeństwo)*, w: *Bezpieczeństwo międzynarodowe w XXI wieku*, M. Lakomy, R. Zięba (red.), Warszawa 2018, s. 55–69.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Nowak W., *Ochrona infrastruktury krytycznej w cyberprzestrzeni*, w: Cyberbezpieczeństwo. Zarys wykładu, C. Banasiński (red.), Warszawa 2018.

Oleksiewicz I., *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1, s. 53–67.

Palka D., Stecuła K., *Postęp technologiczny – dobrodziejstwo czy zagrożenie?*, w: *Innowacje w zarządzaniu i inżynierii produkcji*, t. 1, D. Palka, K. Stecuła, R. Knosala (red.), Opole 2018.

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

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2019–2024, Ministerstwo Cyfryzacji, Warszawa 2019.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2020, Ministerstwo Cyfryzacji, Warszawa 2017.

Szpyra R., *Cyberbezpieczeństwo i cyberaktywność militarna*, w: *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia informatycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, r. 46, nr 1, s 173–187.

Zagrożenia we współczesnym świecie jako temat edukacji geograficznej, T. Michalski (red.), Warszawa 2008.

Źródła internetowe

APA Dictionary of Psychology, American Psychological Association, https://dictionary.apa.org/situation-awareness [dostęp: 21 IV 2021].

Infrastruktura krytyczna, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp: 14 IV 2022].

Koziej S., *Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO*, https://koziej.pl/wp-content/uploads/2016/10/IBK-Cyberbezpiecze%C5%84stwo-25.10.2016.pdf [dostęp: 20 XII 2020].

Krajowy system cyberbezpieczeństwa, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- [dostęp: 13 IV 2021].

(MINI)SŁOWNIK BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa, BBN, http://katedrawiss.uwm.edu.pl/sites/default/files/download/202005/minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.pdf [dostęp: 9 II 2021].

Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 1: *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/wp-content/uploads/Za%C5%82%C4%85cznik-nr-1-Standardy-s%C5%82u%C5%BC%C4%85ce--zapewnieniu-sprawnego-funkcjonowania-infrastruktury-krytycznej-%E2%80%93-dobre--praktyki-i-rekomendacje.pdf [dostęp: 14 IV 2021].

Ottis R., Lorents P., *Cyberspace: Definition and Implications*, w: *Materiały z konferencji pt.: „Proceedings of the 5th International Conference on Information Warfare and Security"*, Dayton U.S. 2010, https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf [dostęp: 20 XII 2020].

Powstała nowa mapa internetu, Benchmark 13 IX 2010 r., https://www.benchmark.pl/aktualnosci/powstala-nowa-mapa-internetu.html [dostęp: 21 04 2021]

Rośnie liczba cyberzagrożeń, Serwis Rzeczypospolitej Polskiej, 23 II 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosnie-liczba-cyberzagrozen [dostęp: 24 IV 2022].

Systemy infrastruktury krytycznej, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej [dostęp: 14 IV 2022].

Szymczykiewicz R., *Czym jest cyberprzestępstwo?*, Infor, 28 XII 2011 r., https://www.infor.pl/prawo/prawokarne/przestepstwa-komputerowe/298370,2,Czym-jest-cyberprzestepstwo.html [dostęp: 20 XII 2020].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19 VII 2016 r.).

Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2020 r. poz. 1369, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2022 r. poz. 261, ze zm.).