FOLIA 292

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 9(4) (2019)
ISSN 2657-8549
DOI 10.24917/26578549.9.4.6

Agnieszka Warchoł
ORCID ID 0000–0003–0786–6440
Uniwersytet Pedagogiczny w Krakowie

Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii Europejskiej

Wprowadzenie

Kiedy Vernor Vinge w 1981 roku po raz pierwszy użył terminu „cyberprzestrzeń" w powieści science fiction pt. *True Names*, zarówno żaden z jego czytelników, jak i on sam nie spodziewali się, że kilka dekad później wyraz ten będzie elementem języka prawnego, a zarazem prawniczego, oraz że znajdzie się w dokumentach państwowych o strategicznym z punktu widzenia bezpieczeństwa znaczeniu. Termin „cyberprzestrzeń" wywodzi się etymologicznie z „cybernetyki". Za ojca cybernetyki jako samodzielnej dyscypliny naukowej uważany jest prof. Norbert Wiener[1], amerykański matematyk. Termin został przez niego wprowadzony w 1948 roku w książce pt. *Cybernetics. Or Control and Communication in the Animal and the Machine*, a zaadaptowany z języka greckiego, od słowa *κυβερνήτης*, które oznacza kogoś, kto steruje statkiem, czyli sternika lub zarządcę, od *kybernan* – sterować, kontrolować[2].

Termin cyberprzestrzeń spopularyzował jednak pisarz – William Gibson – i to pewnie dlatego w opinii wielu teoretyków to on uchodzi za jego prekursora. Autor – także w powieści z gatunku fantastyczno-naukowych – definiował cyberprzestrzeń jako „konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność…"[3].

[1] Norbert Wiener (1894–1964) – amerykański matematyk pochodzenia żydowskiego. Od 1932 roku profesor Massachusetts Institute of Technology w Cambridge. Najważniejsze prace: *Cybernetics. Or Control and Communication in the Animal and the Machine* (1948), *Cybernetyka i społeczeństwo* (1950). Zob. hasło *Norbert Wiener*, http://encyklopedia.pwn.pl/haslo/Wiener-Norbert;3995859.html, [dostęp: 17.10.2019].

[2] *Cybernetyka* [w:] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1989, s. 102.

[3] W. Gibson, *Neuromancer*, Wydawnictwo Książnica, Poznań 1984, s. 53.

To nienaukowe rozumienie cyberprzestrzeni jako wytworu ludzkiej wyobraźni i niezidentyfikowanego zjawiska zaczęło się zmieniać na rzecz pojmowania jej jako niematerialnej sfery realnej ludzkiej działalności, na którą składają się komputery i sieci. Stopniowo określenie „cyberprzestrzeń" zaczęło być wykorzystywane przez naukowców do identyfikacji zjawisk niebędących wytworem ludzkiej wyobraźni, do nazywania powiązań o charakterze wirtualnym[4]. Następnie zaczęło się ono pojawiać w dokumentach państwowych, np. krajowych strategiach bezpieczeństwa.

Tworzenie państwowych cyberstrategii jest obecnie jednym z obowiązków państw członkowskich Unii Europejskiej, który nałożyła na nie w lipcu 2016 roku Dyrektywa Parlamentu Europejskiego i Rady (UE)2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, powszechnie znana jako Dyrektywa NIS. Celem dokumentu jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Dyrektywa NIS weszła w życie w sierpniu 2016 roku i od tamtej pory państwa członkowskie UE miały 21 miesięcy na implementację jej przepisów do prawa krajowego[5]. Państwa, które wcześniej marginalizowały problemy cyberzagrożeń, wprowadziły do krajowych porządków prawnych stosowne zapisy, ukazujące poziom świadomości władz państwowych w sprawach cyberbezpieczeństwa. Jest on wysoce zróżnicowany. Obecnie wszystkie państwa członkowskie Unii Europejskiej posiadają co najmniej jeden oficjalny dokument, w którym zawarte są cele i działania, jakie należy podjąć w celu zapewnienia cyberbezpieczeństwa.

W Dyrektywie NIS znajdujemy także fragment mówiący o konieczności współpracy mającej na celu wymianę informacji i wsparcie państw członkowskich w budowaniu bezpieczeństwa sieci i systemów informatycznych. Warto zaznaczyć, że tego typu współpracę utrudniają zróżnicowane podejścia poszczególnych państw do budowy cyberbezpieczeństwa, co ma źródło w odmiennych interpretacjach podstawowych pojęć w tym zakresie. Na brak jednolitości w definiowaniu cyberprzestrzeni wskazuje Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). W publikacji będącej wynikiem analizy narodowych dokumentów dotyczących bezpieczeństwa w cyberprzestrzeni, zawierającej stosowne rekomendacje, ENISA wśród zaleceń dla państw wymienia m.in. konieczność harmonizacji pojęć z zakresu cyberbezpieczeństwa – zarówno na poziomie europejskim, jak i globalnym[6].

---

[4] T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Wydawnictwo Difin, Warszawa 2014, s. 23.

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE)2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=-CELEX%3A32016L1148, [dostęp: 15.05.2019].

[6] *National Cyber Security Strategies*. *Practical Guide on Development and Execution* 2012, s. 1.

Ujednolicenie definiensów, poszczególnych pojęć definiowanych, znacznie ułatwiłoby projektowanie wspólnych działań w zakresie cyberbezpieczeństwa. Problem natury terminologicznej występuje w tej materii już od lat 90. XX wieku, czyli od momentu, kiedy termin „cyberprzestrzeń" wszedł do powszechnego obiegu. Jaka jest zatem definicja wyrażenia, które powstało z połączenia przedrostka „cyber" i rzeczownika „przestrzeń"? Odpowiedź na to pytanie od lat przysparza wielu kłopotów. Jeden z nich wynika ze sposobu rozumienia cyberprzestrzeni, kolejny – właśnie z niejednolitego jej definiowania.

Współcześnie obserwuje się różnorodność interpretacji terminu, co powoduje wiele niebezpieczeństw. Są to np. problemy związane z egzekwowaniem odpowiedzialności za czyny zabronione popełnione w obrębie cyberprzestrzeni czy niemożność budowania efektywnych systemów bezpieczeństwa.

W kolejnych częściach niniejszego artykułu zostanie przedstawione zestawienie definicji cyberprzestrzeni, które są wykorzystywane w cyberstrategiach państw członkowskich UE. Ten wykaz pozwoli zilustrować różnorodność interpretacji terminu przez poszczególne państwa. Mimo różnic w poszczególnych ujęciach można wskazać wspólne cechy i części składowe definiensów cyberprzestrzeni, co pozwala na opracowanie typologii. Celem pracy jest wyodrębnienie z europejskich strategii pięciu ścieżek interpretacyjnych pojęcia „cyberprzestrzeń" i wskazanie ich empirycznych przykładów. Ma to pomóc w uporządkowaniu podstawowych kwestii terminologicznych w zakresie cyberbezpieczeństwa.

Cyberprzestrzeń osadzona w przestrzeni fizycznej

Pierwsze zaprezentowane podejście początkowo zdaje się budzić kontrowersje, gdyż cyberprzestrzeń co do zasady cechuje aterytorialność. Oznacza to, że pozbawiona jest ona fizycznych granic, co np. ułatwia działania podmiotom o charakterze transnarodowym. Jednak warto wskazać, że po analizie wielu definicji i podejść badawczych możliwe jest wytyczenie granic cyberprzestrzeni za pomocą infrastruktury, która ją tworzy. Oznacza to, że w tym podejściu granice cyberprzestrzeni wyznaczają jej materialne składniki. Niektórzy autorzy określają cyberprzestrzeń jako sieć współzależności infrastruktury informatycznej, w której skład wchodzą Internet, sieci telekomunikacyjne, systemy komputerowe, wbudowane procesory i sterowniki w środowisku przemysłowym o strategicznym znaczeniu[7], a także miedziane kable, routery internetowe, światłowody, wieże przekaźnikowe i transpondery satelitarne[8].

To rozumienie cyberprzestrzeni wskazuje, że jest ona bezpośrednio osadzona w przestrzeni fizycznej za pomocą całej infrastruktury teleinformatycznej. Z tego typu definicji korzysta się zazwyczaj do określenia tzw. „państwowych cyberprzestrzeni".

[7] H. Katzan, *Cybersecurity Service Model*, „Journal of Service Science" 2012, Vol. 5, No. 2, s. 72.

[8] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 82.

Dla przykładu, w *Polityce ochrony cyberprzestrzeni RP* z 2013 roku cyberprzestrzeń Rzeczypospolitej Polskiej została określona jako „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)”[9]. Podobną interpretację prezentują także Węgrzy, wyodrębniając węgierską cyberprzestrzeń obejmującą te części elektronicznych systemów informacyjnych globalnej cyberprzestrzeni, które znajdują się właśnie na terytorium Węgier. Ponadto wymieniają oni także inne składniki krajowej cyberprzestrzeni, takie jak procesy społeczne i gospodarcze zachodzące w systemach elektronicznych globalnej cyberprzestrzeni i za ich pośrednictwem – w postaci danych i informacji – kierowane do Węgier lub wpływające na nie[10].

Tę ścieżkę interpretacyjną prezentują więc państwa, które w swoich strategiach cyberbezpieczeństwa określają cyberprzestrzeń za pomocą jej fizycznych składników, wskazując na jej zakres terytorialny. Taką definicję cyberprzestrzeni przedstawiają Słoweńcy w krajowej strategii cyberbezpieczeństwa (ang. *Cybersecurity strategy*, *2016*). Elementami cyberprzestrzeni według Słowenii są: sieć informatyczna, sieci telekomunikacyjne i komputerowe systemy przetwarzania danych[11]. Podobnie cyberprzestrzeń postrzegają Włosi, co przedstawiają w *National Strategic Framework for Cyberspace Security*. Wymieniają oni poszczególne elementy infrastruktury teleinformatycznej, podkreślając przy tym, że cyberprzestrzeń jest domeną stworzoną przez człowieka[12].

Odniesienia do tego podejścia znajdujemy także w *Narodowej Strategii Cyberbezpieczeństwa 2016–2021* Wielkiej Brytanii, gdzie cyberprzestrzeń zdefiniowana jest jako „sieć współzależności infrastruktury informatycznej, która obejmuje Internet, sieci telekomunikacyjne, systemy komputerowe, urządzenia podłączone do Internetu oraz wbudowane procesory i kontrolery”[13].

Kolejnym państwem, które w cyberstrategii określa cyberprzestrzeń przez pryzmat infrastruktury teleinformatycznej, jest Hiszpania. W stosownym dokumencie (ang. *National Cyber Security Strategy*) Hiszpanie wymieniają następujące

[9] *Polityka ochrony cyberprzestrzeni RP, 2013*, http://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf, [dostęp: 15.05.2019].

[10] *Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map, [dostęp: 15.05.2019].

[11] *Cyber Security Strategy, Slovenia, 2016*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia, [dostęp: 15.05.2019].

[12] *National Strategic Framework for Cyberspace Security*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security, [dostęp: 15.05.2019].

[13] *National Cyber Security Strategy 2016–2021*, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, [dostęp: 15.05.2019].

komponenty cyberprzestrzeni: technologie informacyjne, w tym Internet, sieci i systemy informacyjne oraz telekomunikacyjne[14]. Podobne definicje prezentują także Irlandia[15], Belgia[16] i Bułgaria[17].

Definicjom, których treść skupia się głównie na infrastrukturze teleinformatycznej, czyli materialnym składnikom cyberprzestrzeni umieszczonym na określonym terytorium, można zarzucić to, że pomijają przechowywanie i przetwarzanie danych np. w tzw. chmurze, która niekoniecznie zlokalizowana jest fizycznie na terytorium określonego państwa. Podsumowując, zdefiniowanie cyberprzestrzeni przez wskazanie wyłącznie jej fizycznych składników jest niekompletne.

Socjologiczny wymiar cyberprzestrzeni

Pierre Lévy, francuski socjolog i autor pojęcia „cyberkultura", określa cyberprzestrzeń jako „nową przestrzeń umożliwiającą komunikację, kontakty towarzyskie, organizowanie się i prowadzenie transakcji[18]". Socjolog zwraca także uwagę na powstanie nowego rynku informacji i wiedzy, będącego rezultatem współczesnej ewolucji technicznej. Cyberprzestrzeń jest przedmiotem badań socjologów, a odniesienia do dorobku tej dyscypliny naukowej znajdują się w niektórych państwowych strategiach cyberbezpieczeństwa.

Na socjologiczny wymiar cyberprzestrzeni zwracają uwagę Francuzi w dokumencie pt. *Information Systems Defence and Security: France's Strategy*, nazywając cyberprzestrzeń „Nową Wieżą Babel"[19]. Jest to właśnie socjologiczne rozwinięcie koncepcji cyberprzestrzeni jako obszaru komunikacji o globalnym zasięgu[20]. W tym znaczeniu cyberprzestrzeń jako nowy kanał komunikacji powoduje mieszanie się kultur, języków, idei i informacji z całego świata[21]. Francuski dokument zawiera także inne określenia i cechy charakterystyczne dla cyberprzestrzeni, m.in. definiuje ją jako wirtualne pole bitwy, a zarazem sferę komunikacji o międzynarodowym

---

[14] *National Cyber Security Strategy, Spain, 2013*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy, [dostęp: 16.05.2019].

[15] *National Cyber Security Strategy 2015–2017*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf, [dostęp: 16.05.2019].

[16] *Cyber Security Strategy, Belgium, 2012*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/view, [dostęp: 15.05.2019].

[17] *Национална стратегия за киберсигурност „Киберустойчива България 2020"*, https://cyberbg.eu/, [dostęp: 16.05.2019].

[18] P. Lévy, *Drugi potop,* http://portal.tezeusz.pl/cms/tz/index.php?id=287, [dostęp: 20.04.2019].

[19] *Information Systems Defence and Security: France's Strategy* 2011, s. 3.

[20] Z. Ciekanowski, H. Wyrębek, *Współczesne technologie informatyczne – szanse i zagrożenia*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2017, nr 1 (3), s. 9.

[21] Ibidem.

zasięgu, stworzoną przez wzajemnie połączone, zautomatyzowane i cyfrowe urządzenia do przetwarzania danych[22].

Podobny kontekst ma definicja zamieszczona w austriackiej strategii cyberbezpieczeństwa (ang. *Austrian Cyber Security Strategy*), w której czytamy, że cyberprzestrzeń jest przestrzenią ogólnej interakcji społecznej i jest używana przez ludzi do socjalizowania się, prowadzenia życia towarzyskiego[23].

Socjologiczny wymiar cyberprzestrzeni dostrzegamy także w portugalskim dokumencie dotyczącym ochrony cyberprzestrzeni (ang. *National Cyberspace Security Strategy*), w którym autorzy zwracają uwagę na to, że do cyberprzestrzeni przenosi się prawdziwe życie codzienne. Powstają w niej nowe typy interakcji, relacji, a czyny zabronione popełniane w świecie fizycznym zmieniają swą formę i przenoszą się w obszar wirtualny[24]. Estończycy także w państwowej strategii cyberbezpieczeństwa (ang. *Cyber Security Strategy*) wielokrotnie odwołują się do podstawowego pojęcia socjologicznego, a mianowicie do społeczeństwa, a dokładnie konieczności jego ochrony przez zapewnienie bezpieczeństwa cyberprzestrzeni[25].

Podsumowując, cyberprzestrzeń w ujęciu socjologicznym określana jest jako nowe miejsce międzyludzkich interakcji, jako przedłużenie fizycznego świata. Jest ona elementem naszego życia codziennego, nową płaszczyzną życia społecznego.

Cyberprzestrzeń jako przestrzeń wirtualna

W kolejnym ujęciu termin „cyberprzestrzeń" używany jest do określenia powiązań o charakterze wirtualnym, powstałych i funkcjonujących przez ich fizyczne manifestacje – komputery oraz infrastrukturę telekomunikacyjną. W tym sposobie interpretacji cyberprzestrzeni nierzadko traktuje się ją jako synonim Internetu. Zgodnie z definicją zawartą w *Encyklopedii PWN* Internet to „ogólnoświatowa sieć komputerowa, łącząca lokalne sieci, korzystające z pakietowego protokołu komunikacyjnego TCP/IP, mająca jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) oraz protokoły udostępniania informacji"[26]. Bez wątpienia definiens cyberprzestrzeni jest znacznie szerszy. Jej fundamentem niezaprzeczalnie jest sieć Internet, jednak nie można pominąć wchodzących w jej skład różnego typu urządzeń teleinformatycznych i właśnie połączeń między nimi, które w tym podejściu pełnią ważną funkcję.

---

[22] *Information Systems Defence and Security…*, op. cit., s. 21.

[23] *Austrian Cyber Security Strategy*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf, [dostęp: 21.04.2019].

[24] *National Cyberspace Security Strategy – Portugal*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf, [dostęp: 16.05.2019].

[25] *Cyber Security Strategy, Estonia, 2014*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy, [dostęp: 17.05.2019].

[26] *Internet*, http://encyklopedia.pwn.pl/haslo/Internet;3915155.html, [dostęp: 26.04.2019].

Państwem, które w ten sposób interpretuje cyberprzestrzeń, jest Republika Federalna Niemiec. Definicja zamieszczona w państwowej strategii cyberbezpieczeństwa z 2011 roku określa cyberprzestrzeń jako wirtualną przestrzeń systemów IT połączonych na poziomie danych w skali globalnej. Same systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią cyberprzestrzeni, gdyż jej podstawą jest Internet[27].

Podobne stanowisko prezentują Łotysze, którzy określają cyberprzestrzeń wyłącznie jako domenę wirtualną, nazywając ją „interaktywnym środowiskiem". W dokumencie państwowym (ang. *Cyber Security Strategy of Latvia*) wskazują oni, że w cyberprzestrzeni funkcjonują użytkownicy, sieci, technologia komputerowa, oprogramowanie, informacje, aplikacje, serwisy oraz procesy, które mogą być bezpośrednio lub pośrednio połączone z Internetem, sieciami telekomunikacyjnymi i komputerowymi[28]. Mimo umieszczenia w łotewskiej definicji cyberprzestrzeni elementów infrastruktury teleinformatycznej nie można zakwalifikować jej do kategorii „definicji osadzonych w przestrzeni fizycznej", gdyż w strategii cyberbezpieczeństwa czytamy, że nie jest możliwe wytyczenie fizycznych granic cyberprzestrzeni. Na brak geograficznych granic cyberprzestrzeni wskazują także Litwini[29].

W strategii cyberbezpieczeństwa Rumuni (ang. *Cyber security strategy of Romania*) czytamy, że cyberprzestrzeń to wirtualne środowisko generowane przez cybernetyczną infrastrukturę, w tym informacje: przetwarzane, przechowywane, przekazywane, a także działania podejmowane przez użytkowników[30]. Zdaniem Holendrów cyberprzestrzeń należy postrzegać jako cyfrową domenę pozbawioną terytorialnych granic. W holenderskim dokumencie z 2018 roku (ang. *National Cyber Security Agenda. A cyber secure Netherlands*), który określa państwowe priorytety w zakresie cyberbezpieczeństwa, wskazano, że środowisko cyfrowe, które należy chronić, składa się z danych, połączeń, Internetu oraz oczywiście – podmiotów[31].

Słowacja także definiuje cyberprzestrzeń jako aterytorialną przestrzeń wirtualną obejmującą połączone światowe sieci sprzętu komputerowego, oprogramowania

---

[27] *Cyber Security Strategy for Germany*, s. 9, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany, [dostęp: 17.05.2019].

[28] *Cyber Security Strategy of Latvia*, s. 19–20, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss, [dostęp: 17.05.2019].

[29] *Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019*, s. 3.

[30] *Cyber security strategy of Romania*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania, [dostęp: 17.05.2019].

[31] *National Cyber Security Agenda. A cyber secure Netherlands, 2018*, https://www.enisa.europa.eu/news/member-states/new-national-cyber-security-agenda-published-by-the-netherlands, [dostęp: 18.05.2019].

i informacji[32]. Podobne stanowisko prezentuje także Dania, skupiająca się na ochronie połączeń między systemami, w tym połączeń z Internetem[33]. W tej grupie państw znalazła się również Malta, wskazująca że „nie jest wyspą w cyberprzestrzeni"[34]. To sformułowanie zwraca uwagę właśnie na sieć wzajemnych powiązań, z których składa się cyberprzestrzeń, oraz na jej atrybuty – aterytorialność i transnarodowość.

Aspekt informacyjny cyberprzestrzeni

Czesi przy definiowaniu cyberprzestrzeni zwracają szczególną uwagę na aspekt informacyjny. W *Zákon o kybernetické bezpečnosti* (ang. *Act on Cyber Security)* z 2014 roku czytamy, że cyberprzestrzeń to cyfrowe środowisko umożliwiające tworzenie, przetwarzanie i wymianę informacji, tworzone przez systemy i usługi informacyjne oraz elektroniczne sieci komunikacyjne[35].

Podobnie cyberprzestrzeń interpretuje Chorwacja. W dokumencie państwowym dotyczącym cyberbezpieczeństwa z 2015 roku znajduje się definicja cyberprzestrzeni, zgodnie z którą jest to przestrzeń, gdzie odbywa się komunikacja między systemami informacyjnymi. W chorwackiej strategii ta sfera obejmuje Internet i wszelkie podłączone do niego systemy[36]. Irlandczycy także nawiązują do aspektu informacyjnego cyberprzestrzeni. W narodowej strategii cyberbezpieczeństwa (ang. *National Cyber Security Strategy 2015–2017*) występują liczne odwołania do potrzeby ochrony danych znajdujących się w cyberprzestrzeni, zarówno podmiotów z sektora publicznego, jak i prywatnego. Szczególnie uwypuklona została konieczność ochrony obywateli jako indywidualnych użytkowników sieci, a konkretnie – ich danych osobowych[37].

Bez wątpienia w tym podejściu cyberbezpieczeństwo jawi się jako część bezpieczeństwa informacyjnego państwa. Bezpieczeństwo informacyjne można dzielić na bezpieczeństwo informacji oraz bezpieczeństwo teleinformatyczne. To właśnie w tej drugiej kategorii zazwyczaj umieszcza się cyberbezpieczeństwo. Podobne

---

[32] *Cyber Security Concept of the Slovak Republic 2015–2020*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic, [dostęp: 18.05.2019].

[33] *Danish Cyber and Information Security Strategy 2018–2021*, https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/, [dostęp: 18.05.2019].

[34] *Malta Cyber Security Strategy, 2016*, https://mita.gov.mt/en/maltacybersecurity-strategy/Pages/Malta-Cyber-Security-Strategy-2016.aspx, [dostęp: 18.05.2019].

[35] *§ 2 Zákon o kybernetické bezpečnosti* (ang. *Act No. 181 of 23 July 2014 On Cyber Security and Change of Related Acts* (*Act on Cyber Security*).

[36] *The National Cyber Security Strategy of the Republic of Croatia, 2015*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/croatian-cyber-security-strategy, [dostęp: 18.05.2019].

[37] *National Cyber Security Strategy 2015–2017...*, op. cit.

definicje, opierające się na aspekcie informacyjnym cyberprzestrzeni, prezentują także inne kraje członkowskie UE, takie jak Grecja[38], Cypr[39] oraz Finlandia.

Cyberprzestrzeń jako piąte pole walki

Cyberprzestrzeń stała się systemem nerwowym państwa[40], a w latach 90. XX wieku uzyskała miano kolejnego pola walki – obok lądu, morza, powietrza i przestrzeni kosmicznej. Jej powstanie zdeterminowało tworzenie bądź uaktualnianie nowych państwowych taktyk i strategii wojskowych. *The Enemy as a System*, tekst Johna A. Wardena z 1995 roku, jest przełomowy z co najmniej dwóch powodów. Po pierwsze z uwagi na zaprezentowanie w nim modelu, w którym cyberprzestrzeń została ukazana obok lądu, morza, powietrza i przestrzeni kosmicznej jako jedna ze strategicznych płaszczyzn walki z wrogiem. Po drugie dlatego, że Warden wskazuje, iż walka z wrogiem może zakończyć się sukcesem tylko wtedy, gdy postrzegamy go jako całość, jako system[41]. Tę ścieżkę interpretacji terminu cyberprzestrzeni – jako kolejnego pola walki – wykorzystali Szwedzi w narodowej strategii cyberbezpieczeństwa z 2016 roku (ang. *A national cyber security strategy*). W dokumencie podkreślono, że cyberprzestrzeń jest jedną z kilku aren, w których muszą działać tamtejsze siły zbrojne[42].

Wnioski

Brak jednolitych definicji na poziomie regionalnym, a nawet globalnym, generuje problem związany z egzekwowaniem odpowiedzialności za czyny zabronione popełnione w obrębie cyberprzestrzeni. Klasyfikacje i kwalifikacje czynów zabronionych w poszczególnych państwach różnią się od siebie, czego skutkiem jest niejednokrotnie brak zidentyfikowania oraz zdefiniowania danego cyberzagrożenia. U genezy leży – warto jeszcze raz podkreślić – brak jednolitej definicji cyberprzestrzeni, która byłaby powszechnie uznawana. Dobrze ilustruje to przegląd definicji terminu „cyberprzestrzeń", które znajdują się w krajowych strategiach cyberbezpieczeństwa państw członkowskich Unii Europejskiej, w znacznej części przygotowanych i wprowadzonych dopiero po wejściu w życie Dyrektywy NIS w 2016 roku.

[38] *National Cyber Security Strategy – Version 3.0., Greece 2017*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view, [dostęp: 18.05.2019].

[39] *Cyber Security Strategy of the Republic of Cyprus, 2012*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-cyprus/view, [dostęp: 18.05.2019].

[40] T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne*…, op. cit., s. 24.

[41] J.A. Warden, *The Enemy as a System*, „Airpower Journal" 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm, [dostęp: 10.05.2019].

[42] *A national cyber security strategy 2016*, s. 18, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf, [dostęp: 15.05.2019].

W tych wszystkich definicjach, które – jak wyżej wspomniano – znacznie różnią się od siebie, można jednak znaleźć wspólne elementy pozwalające na wyodrębnienie kilku ścieżek interpretacyjnych cyberprzestrzeni. Różne stanowiska są także widoczne wśród politologów, sekuritologów, socjologów i innych badaczy zajmujących się problemami bezpieczeństwa w cyberprzestrzeni. Skonfrontowanie ich w jednym tekście pozwala na dostrzeżenie różnic, ale i podobieństw, co może być pomocne przy współpracy w zakresie cyberbezpieczeństwa.

Problem braku jednorodności terminologii nie dotyczy jedynie pojęcia „cyberprzestrzeń", ale właściwie wszystkich terminów, których nazwy składają się z przedrostka „cyber". Zakres pojęciowy każdego z tych terminów jest trudny do określenia, co w rezultacie powoduje brak powszechnie akceptowanych definicji i trudności we współpracy na tej płaszczyźnie między podmiotami. To z kolei wpływa na niemożność budowania efektywnych systemów bezpieczeństwa, które mają chronić państwa przed – jak się wydaje, mniej problematycznymi pod względem terminologicznym – cyberzagrożeniami.

Bibliografia

Aleksandrowicz T.R., Liedel K., *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Wydawnictwo Difin, Warszawa 2014.

Austrian Cyber Security Strategy, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf, [dostęp: 21.04.2019].

Ciekanowski Z., Wyrębek H., *Współczesne technologie informatyczne – szanse i zagrożenia*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2017, nr 1 (3).

Cyber Security Concept of the Slovak Republic 2015–2020, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic, [dostęp: 18.05.2019].

Cyber Security Strategy for Germany, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany, [dostęp: 17.05.2019].

Cyber Security Strategy of Latvia, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss, [dostęp: 17.05.2019].

Cyber security strategy of Romania, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania, [dostęp: 17.05.2019].

Cyber Security Strategy of the Republic of Cyprus, 2012, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-cyprus/view, [dostęp: 18.05.2019].

Cyber Security Strategy, Estonia, 2014, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy, [dostęp: 17.05.2019].

Cyber Security Strategy, Belgium, 2012, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/view, [dostęp: 15.05.2019].

Cyber Security Strategy, Slovenia, 2016, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia, [dostęp: 15.05.2019].

Danish Cyber and Information Security Strategy 2018–2021, https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/, [dostęp: 18.05.2019].

Dyrektywa Parlamentu Europejskiego i Rady (UE)2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, [dostęp: 15.05.2019].

Gibson W., *Neuromancer*, Wydawnictwo Książnica, Poznań 1984.

Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map, [dostęp: 15.05.2019].

Information Systems Defence and Security: France's Strategy 2011.

Internet, http://encyklopedia.pwn.pl/haslo/Internet;3915155.html, [dostęp: 26.04.2019].

Katzan H., *Cybersecurity Service Model*, „Journal of Service Science" 2012, Vol. 5, No. 2.

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

Lévy P., *Drugi potop,* http://portal.tezeusz.pl/cms/tz/index.php?id=287, [dostęp: 20.04.2019].

Malta Cyber Security Strategy, 2016, https://mita.gov.mt/en/maltacybersecuritystrategy/Pages/Malta-Cyber-Security-Strategy-2016.aspx, [dostęp: 18.05.2019].

National Cyber Security Agenda. A cyber secure Netherlands, 2018, https://www.enisa.europa.eu/news/member-states/new-national-cyber-security-agenda-published-by-the-netherlands, [dostęp: 18.05.2019].

National Cyber Security Strategies. *Practical Guide on Development and Execution* 2012.

National Cyber Security Strategy – Version 3.0., Greece 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view, [dostęp: 18.05.2019].

National Cyber Security Strategy 2015–2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf, [dostęp: 16.05.2019].

National Cyber Security Strategy, Spain, 2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy, [dostęp: 16.05.2019].

National Cyberspace Security Strategy – Portugal, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf, [dostęp: 16.05.2019].

National Strategic Framework for Cyberspace Security, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security, [dostęp: 15.05.2019].

Polityka ochrony cyberprzestrzeni RP, 2013, http://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf, [dostęp: 15.05.2019].

Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019.

The National Cyber Security Strategy of the Republic of Croatia, 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/croatian-cyber-security-strategy, [dostęp: 18.05.2019].

Warden J.A., *The Enemy as a System*, „Airpower Journal" 1995, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm, [dostęp: 10.05.2019].

Zákon o kybernetické bezpečnosti (ang. *Act No. 181 of 23 July 2014 On Cyber Security and Change of Related Acts* (*Act on Cyber Security*).

Национална стратегия за киберсигурност „Киберустойчива България 2020", https://cyberbg.eu/, [dostęp: 16.05.2019].

Cyberspace in the security strategies of the Member States of the European Union

Abstract

The aim of the article is to present and analyze definitions of cyberspace of the Member States of the European Union. The article is based on the content of their cyber strategies. This is possible because countries create these documents after the introduction of The NIS Directive, which obliges all EU Member States to adopt a national strategy on the security of network and information systems. The author's analysis points out a multiplicity and diversity of definitions.

Słowa kluczowe: cyberprzestrzeń, cyberstrategia, cyberbezpieczeństwo

Key words: cyberspace, cyber strategy, cybersecurity

Agnieszka Warchoł

Politolog i administratywista, doktor w dziedzinie nauk społecznych, w dyscyplinie nauki o polityce, specjalność – polityka bezpieczeństwa. Adiunkt w Katedrze Bezpieczeństwa Wewnętrznego Instytutu Nauk o Bezpieczeństwie na Wydziale Politologii Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Autorka monografii naukowej pt. *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku* (Stalowa Wola 2016), współautorka kilku monografii oraz autorka licznych artykułów naukowych dotyczących cyberbezpieczeństwa, bezpieczeństwa informacyjnego państwa, wykorzystania nowych technologii w bezpieczeństwie narodowym oraz zagrożeń dla bezpieczeństwa państwa w cyberprzestrzeni. Prelegentka na konferencjach krajowych i międzynarodowych, podczas których poruszała tematy związane przede wszystkim z funkcjonowaniem państwa w globalnej cyberprzestrzeni. E-mail: agnieszka.warchol@up.krakow.pl