

Pojęcie cyberbezpieczeństwa w cyberprzestrzeni.

Streszczenie

W artykule dokonano przeglądu najważniejszych definicji cyberbezpieczeństwa oraz cyberprzestrzeni. Przytoczono genezę powstania pojęcia cyberprzestrzeni. Na podstawie tych definicji, podjęto próbę sformułowania definicji cyberbezpieczeństwa w cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, bezpieczeństwo, cyberterrorizm, bezpieczeństwo informacyjne,

Kody klasyfikacji JEL: F52, H56, C88,

Cybersecurity concept in cyberspace.

Abstract

The article reviews the most important definitions of cybersecurity and cyberspace. The genesis of the concept of cyberspace is presented. Based on these definitions, an attempt was made to formulate a definition of cybersecurity in cyberspace.

Keywords: cybersecurity, cyberspace, security, cyberterrorism, information security

JEL Classification Codes: F52, H56, C88,

Wprowadzenie

Postęp technologiczny w dzisiejszych czasach rozwija się w niezwykle szybkim tempie. Sprawia, że jest wiele udogodnień, które są możliwe dzięki użyciu m.in. systemów informatycznych. Współcześnie każda firma korzysta z prostych bądź bardziej zaawansowanych rozwiązań,

których zadaniem jest przede wszystkim gromadzenie, przetwarzane jak i generowanie danych i informacji. Aktualnie bez systemów teleinformatycznych większe podmioty w tym organizacje krajowe czy międzynarodowe nie mogłyby funkcjonować. Niestety korzystanie z systemów teleinformatycznych niesie też ze sobą podatność na wszelkie ataki sieciowe. Najczęściej wyróżnianymi formami zagrożeń teleinformatycznych są: haking, hakytywizm, cyberprzestępczość, cyberterrorizm, cyberszpiegostwo, wykorzystanie cyberprzestrzeni do działań zbrojnych czy użycie w sferze społeczno-psychicznej. Organizacje rządowe, kładą duży nacisk na ochronę danych i bezpieczeństwo w cyberprzestrzeni.

Cyberbezpieczeństwo jest terminem dość szerokimi i obejmuje zagadnienia dotyczące zapewnienia ochrony w zakresie cyberprzestrzeni. Celem artykułu jest wskazanie pochodzenia definicji cyberbezpieczeństwa oraz wskazanie najważniejszych zagrożeń pochodzących z sieci.

W artykule autor zestawia definicje, jakie można znaleźć w literaturze. Niniejszy tekst może stanowić dobry punkt wyjścia do zrozumienia czym jest cyberbezpieczeństwo w cyberprzestrzeni, pojęciami którymi aktualnie posługuje się każdy z nas.

Pojęcie cyberprzestrzeni

Cyberprzestrzeń dla niektórych ma wydźwięk bardzo nowoczesny. Sama historia tego pojęcia sięga już ponad 30 lat. Pierwsze „użycie” bądź „zastosowanie” tego hasła miało miejsce w 1982 r. przez Williama Gibsona¹, w jego powieściach science fiction pt. *Burning Chrome*² jak i

¹ <http://en.wikipedia.org/wiki/Cyberspace> [dostęp: 1 II 2022]

² Nowela została opublikowana w 1982 r. w magazynie „Omni”, amerykańskim piśmie poświęconym tematyce science fiction

Neuromancer³. Autor książek scharakteryzował w nich cyberprzestrzeń, której wizualizacja stała się elementem charakterystycznym dla fantastyki określanej mianem cyberpunku. Jednym z kultowych filmów, świetnie oddający klimat i charakterystykę tego nurtu jest seria filmów Matrix⁴. Sam obraz jak i wizja cyberprzestrzeni zostało ukazane za pomocą grafiki komputerowej (macierzy), trójwymiarowe interaktywne obiekty, poruszające się we wspólnej sferze wykorzystując grawitację.

Śledząc liczną literaturę, postęp technologiczny oraz gwałtowny rozwój internetu, cyberprzestrzeń możemy śmiało potraktować jako szeroko pojęty dorobek teleinformatyki. Według udostępnionych w internecie danych, liczba urządzeń podłączonych do sieci w roku 2016 wyniosła około 3,5 mld użytkowników i cały czas rośnie⁵. Prognozowane jest przez Strategy Analytics⁶, że w roku 2025 będzie podłączone 38,5 mld użytkowników.

W cyberprzestrzeni pojawia się także aspekt prawa. Pojawiła się konieczność rozpoznawania nowonarodzonego cyfrowego środowiska, które dopuszczało się nowoczesnych form przestępczości. Wiele spośród znanych dotychczas czynności prawnych wyraźnie zmieniło się w cyberprzestrzeni, podczas gdy inne dopiero dzięki niej powstały.

Jedną ze znalezionych definicji w literaturze, powszechnie cytowaną jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika

terminologii wojskowej oraz powiązanej, według której cyberprzestrzeń to: Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery⁷.

Powyższa definicja podkreśla technologiczne fundamenty cyberprzestrzeni – internet, nie odwołuje się do ludzi – użytkowników cyberprzestrzeni i elementów społecznych.

W oficjalnym, elektronicznym słowniku pojęć z zakresu społeczeństwa informacyjnego można przeczytać następującą, zaproponowaną przez Komisję Europejską, definicję cyberprzestrzeni: Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata⁸. Ta z kolei definicja wskazuje nowy aspekt cyberprzestrzeni – przestrzeń wirtualną.

Kolejną definicją cyberprzestrzeni, jaka została poddana analizie, znaleźć można w dokumencie przygotowanym w 2011 r. przez francuską Agencję Bezpieczeństwa Sieci oraz Informacji (ANSSI) zatytułowanym: „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji”. Cyberprzestrzeń określona jest jako: Przestrzeń komunikacyjna utworzona przez globalne połączenie sprzętu służącego do

³ W. Gibson, Neuromancer, New York 1984, Ace Books.

⁴ Matrix – australijsko-amerykański film akcji science fiction, pierwszy z serii filmowej o tej samej nazwie, napisany i wyreżyserowany przez siostry Wachowskie (ówcześnie bracia Wachowscy). Kontynuacjami filmu są obrazy Matrix Reaktywacja (2003) i Matrix Rewolucja (2003) oraz Matrix Zmartwychwstania (2021).

⁵ Por. internet users, <http://www.internetlivestats.com/internet-users/> [dostęp: 05.05.2022]

⁶ <https://www.wirtualnemedi.pl/artykul/22-miliardy-urazden-podlaczonych-do-internetu-na-rok-2025> [dostęp 06.05.2022]

⁷ Słownik terminów wojskowych oraz powiązanych, Joint Publication 1-02 Słownik dostępny na stronie internetowej pod adresem: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

⁸ Słownik jest dostępny na stronie internetowej Komisji Europejskiej pod adresem: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. W oryginale: Virtual space in which the electronic data of worldwide PCs circulate.

automatycznego przetwarzania cyfrowych danych⁹.

Tutaj zauważyć można, że nie zostały poruszone w definicji kwestie użytkowników, kwestie zjawisk społecznych czy ekonomicznych. Skupiono się jednocześnie na tym, że cyberprzestrzeń to przestrzeń komunikacyjna, bazująca na infrastrukturze rozsianej po całym świecie.

Ostatnią definicją, jaką przytoczono, to definicja wprowadzona w Polsce w ustawie. W dniu 2 listopada 2011 r. weszła w życie ustawa nowelizująca regulacje prawne stanów nadzwyczajnych. Na podstawie założeń projektu Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011–2016 (dokumentu przyjętego ostatecznie w połowie 2013 r. pod nazwą Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej – o którym jest mowa dalej), zawarta w noweli definicja pojęcia „cyberprzestrzeń” przyjęła następujące brzmienie: Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami.

Analizując powyższą definicję, zauważyć można, że wprowadzono tutaj ideę jednej cyberprzestrzeni, będącej wydzielonym logicznie obszarem. Przestrzeń w tym przypadku jest tworzona przez systemy teleinformatyczne połączone ze sobą za pomocą sieci. Zauważyć też można, że podkreślono swojego rodzaju dwustronne powiązanie działań w

cyberprzestrzeni z działaniami w „rzeczywistym” świecie jak ich wzajemne konsekwencje.

Pojęcie cyberbezpieczeństwa

Na początku, zastanowić się można co znaczy samo słowo bezpieczeństwo.

Termin ten pochodzi z języka łacińskiego – securitas i składa się z dwóch wyrazów: sine cura i oznacza: stan bez troski, bez strachu, bez zmartwień. Stwierdzić można, że bezpieczeństwo to stan, w którym nie istnieje żadne zagrożenie. Jest pewną wartością jak i potrzebą podmiotową i egzystencjalną, która związana jest z istnieniem danego podmiotu. Bezpieczeństwo można również postrzegać jako swoistą możliwość zaspokojenia potrzeb o charakterze egzystencjonalnym, potrzebie zaspokojenia istnienia, przetrwania i rozwoju¹⁰.

Ukazuje nam się kilka stron podejmowania bezpieczeństwa:

- negatywna – czyli wolność od jakichkolwiek zagrożeń i pewność przetrwania tzw. bezpieczeństwo egzystencjonalne

- pozytywna – czyli swoboda w rozwoju podmiotu bezpieczeństwa, ochrony jego interesów i możliwość przeciwstawienia się współczesnym zagrożeniom¹¹.

Bezpieczeństwo można też analizować według kategorii: podmiotowej, przedmiotowej, procesowej oraz terytorialnej. Tutaj bezpieczeństwo będzie analizowane w kategorii przedmiotowej jako wielokierunkowe i uwarunkowane zakresem interesów danego podmiotu. Nawiązując do tematu artykułu, przykładem takiej definicji będzie

⁹ W oryginale: Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

¹⁰ R. Rosicki, O pojęciu i istocie bezpieczeństwa, <https://wnpid.amu.edu.pl/images/stories/pp/pp-3-2010/023-032.pdf>, s. 24 (dostęp: 20.08.2018 r.)

¹¹ J. Stańczyk, Współczesne pojmowanie bezpieczeństwa, Warszawa 1996, s. 19; por. też P. Sienkiewicz, H. Świeboda, Perspektywy badań nad bezpieczeństwem [w:] Bezpieczeństwo. Wymiar współczesny i perspektywy badań, red. M. Kwieciński, Kraków 2010, s. 12

bezpieczeństwo narodowe, gdzie wyróżnia się bezpieczeństwo ideologiczne, powszechne, a przede wszystkim militarne, publiczne czy ekonomiczne.

Nawiązując do samego pojęcia cyberbezpieczeństwa, w literaturze znaleźć można wiele definicji cyberbezpieczeństwa.

Jedną z podstawowych definicji, znaleźć można w ustawie: cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy¹².

Definicje cyberbezpieczeństwa możemy również znaleźć w Doktrynie cyberbezpieczeństwa Rzeczypospolitej” (RP) z 2015r., która wyodrębnia:

„ - cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) – proces zapewniania 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,

- bezpieczeństwo cyberprzestrzeni RP – część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz

bezpieczeństwa przetwarzanych w niej zasobów informacyjnych,

- środowisko cyberbezpieczeństwa – ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni charakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągnięcia przyjętych celów”¹³

Samo powyższe pojęcie – cyberbezpieczeństwo – zostało zdefiniowane przez organizację zarządzaną przez wydział Edukacji i Świadomości Cyberbezpieczeństwa, działająca na terenie Stanów Zjednoczonych (National Initiative for Cybersecurity Careers and Studies w skrócie: NICCS): „(...) systemy informacyjne lub komunikacyjne oraz informacja zawarta w nich są zabezpieczone czy chronione przed uszkodzeniem, nieautoryzowanym użyciem, modyfikacją bądź wykorzystaniem”¹⁴.

Czyli jest to ogół technik, procesów i praktyk używanych do ochrony sieci informatycznych, programów, danych oraz urządzeń, przed cyberatakami, uszkodzeniami oraz nieautoryzowanym dostępem. Głównym zadaniem jest ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieci.

Cyberbezpieczeństwo jest też zdefiniowane przez Strategię bezpieczeństwa cybernetycznego Unii Europejskiej jako: „Otwarta, bezpieczna i chroniona cyberprzestrzeń”¹⁵.

Każda z przytoczonych powyżej definicji posiada wspólny mianownik, a mianowicie cyberprzestrzeń musi być chroniona przed szkodliwymi działaniami, zarówno pośrednimi jak i bezpośrednimi,

¹² Ustawa o krajowym systemie cyberbezpieczeństwa (2018), Dz.U. 2018 poz. 1560

¹³ <https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html>

¹⁴ Za Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach*

członkowskich, „*Studia z Polityki Publicznej*” 2016/2(10), s. 108

¹⁵ Wspólny komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomicz

no-Społecznego i Komitetu Regionów, Społecznego i Komitetu Regionów (JOIN (2013) 1 final, s. 2).

zakłócającymi lub destrukcyjnymi oddziaływaniami na dany podmiot.

Cyberbezpieczeństwo w ujęciu wybranych autorów

Przy obecnej zwiększonej świadomości dotyczącej bezpieczeństwa w sieci, powstaje coraz to więcej literatury, publikacji naukowych, które przedstawiają problematykę dotyczącą cyberbezpieczeństwa z uwzględnieniem systemowego podejścia do tej problematyki. Bazują one głównie na normach międzynarodowych i krajowych z zakresu bezpieczeństwa informacji. Przedstawiają one ogólne modele bezpieczeństwa informacji, przedstawiają definicję cyberbezpieczeństwa oraz opisują zagrożenia internetowe.

Poniżej przedstawiono kilku autorów, którzy przedstawili cyberbezpieczeństwo z różnych perspektyw w tym teoretycznej i praktycznej.

Godną uwagi jest książka Cezarego Banasińskiego oraz Marcina Rojszczaka pt. „Cyberbezpieczeństwo”, w której cyberbezpieczeństwo omawiane jest z perspektywy technologii oraz prawa. Publikacja przeznaczona jest m.in. dla prawników, sędziów czy pracowników organów administracji publicznych. Przedstawiono w niej najistotniejsze regulacje wpływające na obszar cyberbezpieczeństwa.

Cyberbezpieczeństwo zostało ujęte również jako proces wraz przedstawieniem w jaki sposób możliwe jest zdefiniowanie mierników jego oceny. Warto również wspomnieć, że autorzy przedstawili procedury postępowania w przypadku wystąpienia cyberataku.

Redakcja naukowa pod przewodnictwem Tomasza Dębowskiego pt. „Cyberbezpieczeństwo wyzwaniem XXI wieku”, ukazuje z kolei wielorakie aspekty bezpieczeństwa w cyberprzestrzeni. Autorzy pokazują spojrzenie bezpieczeństwa w kontekście prawno-

politycznym jak i rozprzestrzeniania się zagrożeń pochodzących z cyberprzestrzeni, tworzonych przez organizację państwowe i niepaństwowe. Autorzy poruszają również problematykę religijną w cyberprzestrzeni, zwracając uwagę na sprawę penetrowania wirtualnej przestrzeni przez destrukcyjne grupy religijne.

Innym spojrzeniem na cyberbezpieczeństwo z perspektywy cyberataku jest książka autora Adama Shostack'a pt. „Treat modeling designing for security / Modelowania zagrożeń: projektowania pod kątem bezpieczeństwa”. Autor w głównej mierze przedstawia praktyki modelowania zagrożeń, które stosowano lub były skuteczne w sposobach radzenia sobie z zagrożeniami w jednej ze światowych firm informatycznych: Microsoft. W powyższej książce, cyberbezpieczeństwo przedstawiono już bezpośrednio jako system budowania zabezpieczeń, autor opiera się wyłącznie na działaniu i przedstawione instrukcje są tak przedstawione, że specjaliści ds. cyberbezpieczeństwa mogą zastosować je w praktyce codziennego radzenia sobie z zagrożeniami.

Jednym, z najbardziej znanych ogólnosiatakowych poradnikiem dotyczących bezpieczeństwa w sieci, jest książka Georga Kurtz, Steve'a McClure i Joel'a Scambray pt. „Hacking / Zdemaskowany”. W przeciwieństwie do wyżej przytoczonej polskiej literatury, autorzy nie skupiają się tutaj na przedstawieniu teorii, lecz na praktyce. Przedstawiają jak krok po kroku lokalizować luki w systemie oraz wyjaśniają co należy bezwzględnie wiedzieć, by zachować czujność przed cyberatakami. Opisują i omawiają niszczycielskie metody hackingu oraz jak jemu przeciwdziałać.

Istota pojęcia cyberbezpieczeństwa w cyberprzestrzeni.

Z uwagi na postępującą informatyzację, samo określenie czym jest cyberprzestrzeń

oraz cyberbezpieczeństwo stanowi niezbędny warunek do identyfikacji zagrożeń jakie są w sieci.

Analizując powyższe przytoczone w artykule definicje, ujęte i zdefiniowane w różnych krajach na świecie, wywnioskować można, że istotę cyberprzestrzeni tworzy koncepcja powołania do życia swojego rodzaju równoległego środowiska, które jest nowym wymiarem dla ludzkich działań. Nie można jego podzielić geograficznie i nadać miar fizycznych.

Podsumowanie

W obliczu współczesnych wydarzeń, takich jak wybuch wojny na Ukrainie, w tym cyberwojny, podniesiony alarm III-ciego stopnia z uwagi na cyberataki terrorystyczne, zagadnienia te oraz odpowiednie wprowadzone zarządzanie nimi zwiększą świadomość oraz poziom bezpieczeństwa obywateli polski i jednocześnie Państwa.

Artykuł ukazuje po krótko interpretację kwestii cyberprzestrzeni i cyberbezpieczeństwa w ujęciu różnych autorów. Definicje te z uwagi na dynamikę rozwoju tego obszaru postępującego wraz z rozwojem technologii informatycznych, będą ciągle ewoluowały.

Używając najprostszych definicji, można zdefiniować: cyberbezpieczeństwo jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Należy zwrócić uwagę, że bezpieczeństwo informacji w tym danych, wiąże się z zapewnieniem poufności, odpowiedniego dostępu informacji dla osób do tego upoważnionych oraz integralności, która zapewni kompletność i dokładność informacji.

Bibliografia

[1] Banasiński C., (red. naukowa), Cyberbezpieczeństwo – zarys wykładu, Wolters Kluwer, Warszawa 2018

[2] Bógdał-Brzezińska A., Gawrycki M.F., Cyberterrorizm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003;

[3] Chmielewski Z., Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich, „Studia z Polityki Publicznej” 2016/2(10), s. 108

[4] Dębowski T., Cyberbezpieczeństwo wyzwaniem XXI wieku, Wydawnictwo ArchaeGraph, Łódź – Wrocław 2018,

[5] Gwoździewicz S., Tomaszycy K., Prawne i społeczne aspekty cyberbezpieczeństwa, Warszawa, Międzynarodowy Instytut Innowacji «Nauka – Edukacja – Rozwój» w Warszawie, Warszawa 2017,

[6] Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013

[7] Nakielski K., Cyberbezpieczeństwo, czyli jak zapewnić tajność dokumentów w firmie, Harvard Business Review Polska

[8] Stańczyk J., Współczesne pojmowanie bezpieczeństwa, Warszawa 1996, s. 19; por. też P. Sienkiewicz, H. Świeboda, Perspektywy badań nad bezpieczeństwem [w:] Bezpieczeństwo. Wymiar współczesny i perspektywy badań, red. M. Kwieciński, Kraków 2010, s. 12.

[9] Ustawa o krajowym systemie cyberbezpieczeństwa (2018), Dz.U. 2018 poz. 1560

[10] Ustawa o ochronie danych osobowych (2018), Dz.U. 2018 poz. 1000

[11] Wasilewski J., Zarys definicyjny cyberprzestrzeni, Agencja Bezpieczeństwa Wewnętrznego, 2013, str. 225-234