Tomasz Gajowniczek

Międzynarodowe i krajowe strategie ochrony cyberprzestrzeni

Olsztyn 2024

Międzynarodowe i krajowe strategie ochrony cyberprzestrzeni

Tomasz Gajowniczek

Międzynarodowe i krajowe strategie ochrony cyberprzestrzeni

Olsztyn 2024

Recenzent
kmdr por. rez. prof. dr hab. Grzegorz Piwnicki

Stan prawny na dzień 1 maja 2024 roku

Wydawca
Uniwersytet Warmińsko-Mazurski w Olsztynie
Instytut Nauk Politycznych

ISBN 978-83-66259-46-1

Wydanie 1

Olsztyn 2024

Spis treści

Wstęp

Pojęcia cyberprzestrzeni i cyberbezpieczeństwa nieodłącznie wiążą się z przemianami w zakresie dostępu do informacji, które są konsekwencją tzw. rewolucji informatycznej. Rozwój technik informacyjno-komunikacyjnych (ang. *Information and Communication Technologies* – ICT) i ich współczesna powszechność spowodowały wyjątkową łatwość w produkcji i dystrybucji informacji.

Historia internetu – ogólnoświatowej sieci komputerowej – rozpoczęła się na przełomie lat 60. i 70. XX wieku w Stanach Zjednoczonych. Ówczesna Polska – jako państwo bloku wschodniego – była pozbawiona dostępu do technologii, które mogłyby być wykorzystywane do celów militarnych[1]. W październiku 1991 r. polskie sieci komputerowe uzyskały łączność z siecią europejską. Natomiast w grudniu Stany Zjednoczone zniosły ograniczenia łączności z innymi państwami i cofnęły zakaz wykorzystywania internetu do celów komercyjnych, co oznaczało otwarcie polskiej sieci na cały świat[2].

Według danych Głównego Urzędu Statystycznego w Polsce w 2023 r.[3] dostęp do internetu posiadało 93,3% gospodarstw domowych, tj. tyle samo co w roku poprzednim. Natomiast 92,8% ogółu gospodarstw domowych miało w domu szerokopasmowy dostęp do internetu.

---

[1] Na podstawie embraga nałożonego przez istniejący od 1949 r. Coordinating Committee for Multilateral Export Control (COCOM).

[2] *Internet w Polsce ma 30 lat*, NASK – Państwowy Instytut Badawczy; [online:] https://archiwum.nask.pl/pl/aktualnosci/4271,Internet-w-Polsce-ma-30-lat.html [dostęp 10.01.2024].

[3] *Społeczeństwo informacyjne w Polsce w 2023 r.*, Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, Warszawa-Szczecin 2023; [online:] https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2023-roku,1,17.html [dostęp 10.03.2024].

Spośród ogółu gospodarstw posiadających dostęp do Internetu 99,5% korzystało z łączy szerokopasmowych. Połączenia szerokopasmowe umożliwiają przekazywanie wysokiej jakości obrazów, filmów, oglądanie telewizji lub granie w gry internetowe, telefonowanie przez internet z możliwością oglądania rozmówcy oraz pozwalają na korzystanie z różnorodnych zaawansowanych usług internetowych[4].

Cyberprzestrzeń jako szczególny byt stwarza wiele kłopotliwych sytuacji nie tylko interpretacyjnych, lecz np. natury obyczajowej i formalno-prawnej, co ma istotne znaczenie dla tworzenia racjonalnych reguł zachowań społecznych, działalności gospodarczej, a także programów (strategii) bezpieczeństwa narodowego[5].

Problemem badawczym jest eksploracja poziomu cyberbezpieczeństwa w Polsce oraz skuteczności regulacji prawnych na poziomie globalnym, europejskim i krajowym. Teza badawcza brzmi – poziom ochrony cyberprzestrzeni jest przede wszystkim zależny od dobrze przygotowanej strategii ochrony cyberbprzestrzeni, która identyfikuje najbardziej istotne problemy cyberbezpiezpieczeństwa. Niniejsza publikacja ma na celu przedstawienie Czytelnikom najważniejszych dokumentów o charakterze strategicznym z pozycji bezpieczeństwa narodowego (i międzynarodowego) – od umów międzynarodowych i rozwiązań na poziomie globalnym, poprzez rozwiązania regionalne, na strategiach Polski kończąc. W monografii skoncentrowano się na cywilnych organizacjach międzynarodowych i dlatego nie uwzględniono dorobku NATO. W pracy skupiono się na wyjaśnieniu pojęć cyberprzestrzeni

---

[4] Ze względu na szybki postęp techniczny określenie granicznej przepustowości łączy cyfrowych, od której dane połączenie uznajemy za szerokopasmowe jest narażone na dezaktualizację wkrótce po przyjęciu definicji, dlatego na obszarze Unii Europejskiej w badaniach ICT połączenia szerokopasmowe definiuje się na podstawie rodzaju łączy internetowych. Zgodnie z taką definicją dostęp szerokopasmowy umożliwiają technologie z rodziny DSL (ADSL, SDSL itp.), sieci telewizji kablowej (modem kablowy), telefony komórkowe przynajmniej trzeciej generacji (3G) oraz inne, np. łącza satelitarne, stałe połączenia bezprzewodowe (sieć radiowa) – Tamże.

[5] P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9, s. 98.

i cyberbezpieczeństwa. Dokonano eksploracji międzynarodowych i krajowych regulacji prawnych oraz dokumentów o charakterze strategicznym, które nie tworzą porządku prawnego, ale wskazują kierunki polityki cyberbezpieczeństwa.

Autor od wielu lat prowadzi zajęcia na różnych kierunkach (głównie) Wydziału Nauk Społecznych Uniwersytetu Warmińsko-Mazurskiego w Olsztynie z m.in. przedmiotów: bezpieczeństwo informacyjne, cyberterroryzm, cyberbezpieczeństwo, e-governance i społeczeństwo informacyjne. Monografia ma charakter wademekum i stanowi formę przewodnika do dalszego studiowania zagadnień związanych z różnymi aspektami cyberbezpieczeństwa.

Rozdział 1

Cyberprzestrzeń i cyberbezpieczeństwo

1. Pojęcie cyberprzestrzeni

Pojęcie cyberprzestrzeni należy do kategorii pojęć niedookreślonych i nie odnosi się tylko do internetu. Od strony semantycznej „cyberprzestrzeń" jest hybrydą będącą skrótem *cyberspace* od angielskiego sformułowania *cybernetic space*, czyli przestrzeni cybernetycznej[1].

Piotr Sienkiewicz przypomina tradycyjnie ugruntowane trzy fundamentalne znaczenia pojęcia przestrzeni. Pierwsze, zapoczątkowane przez Demokryta i stoików, a następnie rozwinięte przez Izaaka Newtona, przestrzeń utożsamiało ze swoistego rodzaju miejscem, próżnią, w której miały znajdować się napełniające ją poszczególne byty. Drugie rozumienie tego pojęcia, nadające jej wymiar absolutny, to sformułowana przez Immanuela Kanta idea przestrzenności jako formy pojęciowego ujmowania rzeczywistości będącej przedmiotem doświadczenia. Wreszcie trzecie ujęcie, formułowane przez Gottfrieda Wilhelma Leibniza i przywrócone przez Alberta Einsteina, które wiązało przestrzeń z istnieniem materialnym, czyli z rzeczywistością[2].

Warto zwrócić uwagę, że w języku angielskim *space* oznacza także 'kosmos'. Jednym z najbardziej fascynujących i trudnych do zrozumienia zagadnień w kosmologii jest nieograniczoność kosmosu, szczególnie w odniesieniu do jego rozmiarów. Przestrzeń „cyber", podobnie do przestrzeni kosmicznej, nie ma granic – przestrzennych, politycznych, geograficznych.

---

[1] *Cyberbezpieczeństwo. Zarys wykładu*, [red. nauk.] C. Banasiński, Warszawa 2018, s. 23.

[2] P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9, s. 91.

Z kolei słowo „cybernetyka" wywodzi się ze starogreckiego *κυβερνήτης (kybernētes)* 'sternik; zarządca' od *κυβερνᾶν (kybernán)* 'sterować; kontrolować'. Cybernetyka to nauka (dziedzina wiedzy) o systemach sterowania oraz – o związanym z tym – przetwarzaniu u przekazywaniu informacji. W takim znaczeniu użył jej po raz pierwszy, uznawany za twórcę tej nauki, amerykański matematyk Norbert Wiener w pracy *Cybernetics or Control and Communication in the Animal and the Machine*, wydanej w 1948 roku[3]. Podstawowymi gałęziami cybernetyki jest cybernetyka teoretyczna i cybernetyka stosowana[4].

Pierwotnie „sterowanie" odnosiło się tylko nawigowania okrętami, jednak dosyć szybko starożytni Grecy (np. Platon) rozszerzyli zakres tego pojęcia o rządzenie. W języku łacińskim odpowiednikiem *kybernán* jest czasownik *gubernare*, co oddawane jest na j. polski jako 'rządzić; panować'. W znaczeniu nauki o rządzeniu ludźmi pierwszy tego terminu użył francuski fizyk i matematyk André-Marie Ampère w *Eseju o filozofii nauki*[5]. W języku polskim po raz pierwszy użył tak rozumianej cybernetyki filozof Bronisław F. Trentowski w pracy *Stosunek filozofii do cybernetyki czyli sztuki rządzenia narodem* z 1843 roku.

Istnieją zatem przynajmniej dwa współczesne rozumienia pojęcia „cybernetyka" – jedno związane ze sterowaniem procesami informacyjnymi (i informatycznymi) i drugie, odnoszące się do rządzenia (poniekąd także „sterowania") narodami i społeczeństwem.

Współcześnie słowa z przedrostkiem „cyber-" kojarzą się z czymś komputerowym, informatycznym, interaktywnym. Oksfordzki słownik *science fiction* podaje, że termin „cyberprzestrzeń"[6] po raz pierwszy pojawił się w literaturze tego gatunku za sprawą pisarza Williama Gibsona

---

[3] Wydanie polskie: N. Wiener, *Cybernetyka czyli sterowanie i komunikacja w zwierzęciu i maszynie*, [tł.] J. Mieścicki, Warszawa 1971.

[4] K. Liederman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 62.

[5] A.-M. Ampère, *Essai sur la philosophie des sciences, ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines*, Paris 1834.

[6] *Brave New Words. The Oxford Dictionary of Science Fiction*, [ed. by] J. Prucher, New York 2007, s. 31.

w opowiadaniu *Burning Chrome* z 1982 roku[7] i później w książce *Neuromancer* z 1984 roku[8]. Od tego czasu cyberprzestrzeń zaczęła nabierać znaczenia kulturowego (humanistycznego) i społecznego. Dzisiaj jest często rozumiana jako przestrzeń wirtualna, cyfrowa, interaktywna, w której spotykają się internauci, czyli użytkownicy internetu.

Jak wskazano wyżej, niedookreśloność pojęcia cyberprzestrzeni zależna jest od pozycji interpretatora. Można potraktować ją wąsko, redukując tylko do internetu i połączeń komputerowych. Można także rozszerzać ją do wirtualnej rzeczywistości generowanej przez komputery, systemy komputerowe i aplikacje. Cyberprzestrzeń stanowi także społeczną megasieć. Ostatecznie można ją uznać za ciągle ewoluujący dynamiczny system złożony – bez eksponowania technicznych, informacyjnych czy społecznych aspektów[9].

Podstawowym czynnikiem tworzącym cyberprzestrzeń jest materialny (rzeczywisty) system teleinformatyczny. Federalna agencja normalizacyjna National Institute of Standards and Technology wskazuje trzy techniczne definicje cyberprzestrzeni[10] opisane w amerykańskich normach: 1) Globalna domena w środowisku informacyjnym składająca się ze współzależnej sieci infrastruktur systemów informatycznych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów; 2) Współzależna sieć infrastruktur informatycznych, która obejmuje Internet, sieci telekomunikacyjne, komputery, systemy informatyczne, przemysłowe systemy sterowania, sieci oraz wbudowane procesory i kontrolery; 3) Współzależna sieć infrastruktur informatycznych, która obejmuje Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery w krytycznych branżach. Podaje także czwartą, wywodzącą się z normy międzynarodowej ISO/IEC 27032-3-21, która stwierdza, że

---

[7] Pierwsze wydanie polskie: W. Gibson, *Wypalić Chrom*, [tł.] P. Cholewa, Warszawa 2018.

[8] Pierwsze wydanie polskie: W. Gibson, *Neuromancer*, [tł.] P. Cholewa, Warszawa 1992.

[9] P. Sienkiewicz, *Ontologia cyberprzestrzeni…*, s. 93.

[10] *Cyberspace*, Computer Security Resource Center, [online :] https://csrc.nist.gov/glossary/term/cyberspace [dostęp: 10.01.2024].

cyberprzestrzeń to złożone środowisko powstałe w wyniku interakcji ludzi, oprogramowania i usług w internecie za pośrednictwem urządzeń technicznych i sieci do niego podłączonych, które nie występuje w żadnej formie fizycznej. W defincji ISO „cyberprzestrzeń" występuje zatem jako metasystem (termin opisujący system, który zajmuje się innymi systemami) dla pojęcia „internet".

W polskim porządku prawnym cyberprzestrzeń jest ściśle powiązana z systemami informatycznymi i siecią telekomunikacyjną. W *Prawie telekomunikacyjnym* z 2000 roku[11] w art. 2 ustawodawca ustalił następującą definicję sieci telekomunikacyjnej: „urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną". Natomiast zakończenie sieci to: „punkt sieci telekomunikacyjnej przeznaczony do zapewnienia użytkownikowi dostępu do sieci".

W *Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* system teleinformatyczny zdefiniowano w art. 2 ust. 3 jako: „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne"[12]. Odniesienie do powyższej definicji znajduje się także w art. 3 ust 3 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*[13] („system teleinformatyczny – system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną").

---

[11] Ustawa z dnia 21 lipca 2000 r. Prawo telekomunikacyjne, Dz.U. 2000.73.852.

[12] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002.144.1204.

[13] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005.64.565.

Definicję sieci telekomunikacyjnej w kolejnych nowelizacjach *Prawa telekomunikacyjnego* lekko zmodyfikowano. W 2017 roku otrzymała brzmienie: „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju”[14].

Cyberprzestrzeń obejmuje w równym stopniu internet, sieci telekomunikacyjne i systemy teleinformatyczne – słowem wszystkie systemy IT połączone w sieć globalną. Można postawić pytanie – czy zatem urządzenia offline, czyli nie włączone do sieci, są poza cyberprzestrzenią? Odpowiedź brzmi – raczej nie. Wszystkie urządzenia IT (komputery, pamięci przenośne itd.) mają możliwość połączenia z innymi urządzeniami, mimo tego że, z perspektywy sieci, są ośrodkami izolowanymi[15]. Pendrive leżący na biurku zawiera już w sobie elementy techniczne i logiczne służące do przetwarzania w nim informacji cyfrowych (danych). Tworzy zatem swoją własną mikrocyberprzestrzeń – tymczasowo nieaktywną, która uaktywni się z chwilą wetknięcia do odpowiedniego portu komputera. Wskazany pendrive jest zatem „nieaktywnym elementem sieci” w myśl cytowanej wyżej definicji ustawowej.

Cyberprzestrzeń w dokumentach o charakterze strategicznym pojawiła się w 2009 roku. W założeniach do *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011*[16] stwierdzono, że „cyberprzestrzeń rozumiana jest jako przestrzeń komunikacyjna tworzona przez

---

[14] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 września 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo telekomunikacyjne, Dz.U. 2017.1907.

[15] Por. *Cyberbezpieczeństwo…*, s. 25-26; M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw,* Katowice 2015, s. 83-84.

[16] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*, [online:] https://archiwum.mswia.gov.pl/pl/aktualnosci/6966,Zalozenia-do-Rzadowego-programu-ochrony-cyberprzestrzeni-RP-na-lata-2009-2011.html [dostęp 10.01.2024].

system powiązań internetowych" oraz że za „cyberprzestrzeń państwa przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa"; dotyczy to także RP i cyberprzestrzeni RP. Cyberprzestrzeń RP „obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne".

Program z 2009 roku nie wszedł w życie[17] i kolejny *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*[18] zdefiniował **cyberprzestrzeń** tym razem jako: „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Natomiast **cyberprzestrzeń RP** to „cyberprzestrzeń w obrębie terytorium państwa polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)".

Kolejna definicja cyberprzestrzeni pojawiła się polskim ustawodawstwie w 2011 roku wraz z uchwaleniem *Ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz*

---

[17] Podobnie jak kilka innych. Najwyższa Izba Kontroli w raporcie pokontrolnym z 2015 r. stwierdziła: „W latach 2008–2011 opracowano siedem kolejnych, niezatwierdzonych projektów narodowej strategii bezpieczeństwa cyberprzestrzeni". –*Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP – Informacja o wynikach kontroli P/14/043*, Najwyższa Izba Kontroli: Warszawa 2015 [online:] https://www.nik.gov.pl/kontrole/P/14/043/ [dostęp 10.01.2024].

[18] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji: Warszawa czerwiec 2010, wersja 1.1.

niektórych innych ustaw[19]. Dokonano wówczas pakietowych zmian w trzech ustawach. W *Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[20], wprowadzono (artykułem 1) nowe brzmienie art. 2 ust. 1: „W razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w **cyberprzestrzeni**, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa". Dodano także ustępy 1a i 1b; ostatni otrzymał treść: „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 (Dz. U. Nr 64, poz. 565, z późn. zm.), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Identycznych zmian dokonano w *Ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym*[21] (nowe brzmienie art. 2 ust. 1 oraz dodanie ust. 1a), a także w *Ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*[22] (w art. 3 ust. 1 dodano pkt 4, natomiast ust. 2 otrzymał brzmienie: „Katastrofę naturalną lub awarię

---

[19] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz.U. 2011.222.1323.

[20] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002.156.1301 z późn. zm.

[21] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002.113.985 z późn. zm.

[22] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U. 2002.62.558, z późn. zm.

techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym").

Powyższą definicję cyberprzestrzeni powiela późniejsza *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*[23] z 2013 roku, *Doktryna cyberbezpieczeństwa RP*[24] z 2015 roku, a także *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*[25]. Omówienie tych dokumentów Czytelnik znajdzie w rozdziale dotyczącym Polski.

Jak napisano w uzasadnieniu do zmian ustawowych[26] projektodawcy uwzględnili, że działania zagrażające bezpieczeństwu państwa mogą skutkować nie tylko w tradycyjnych dotychczas wymiarach (ląd, woda, przestrzeń powietrzna, przestrzeń kosmiczna), ale również w przestrzeni wirtualnej – cyberprzestrzeni. W konsekwencji zaistniała konieczność zdefiniowania pojęcia „cyberprzestrzeń", jako kolejnej sfery potencjalnego ataku na Polskę.

We wszystkich aktach podstawą cyberprzestrzeni są realne systemy teleinformatyczne i ich powiązania, które (razem) tworzą bliżej nieokreśloną przestrzeń przetwarzania i wymiany informacji (w domyśle – przez systemy komputerowe). Ponadto istotne są także „relacje z użytkownikami", aczkolwiek tu ustawodawca nie sprecyzował czy chodzi o relacje między użytkownikami, którzy wymieniają się

---

[23] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013; [archiwum online:] https://web.archive.org/web/20150707164127/ https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf [dostęp 10.01.2024].

[24] *Doktryna cyberbezpieczeństwa RP,* Biuro Bezpieczeństwa Narodowego, Warszawa 2015; [online:] https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [dostęp 10.01.2024].

[25] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*; [online:] https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 [dostęp 10.01.2024].

[26] Przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Druk nr 4355. Uzasadnienie, https://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/$file/4355-uzasadnienie.doc.

informacjami za pośrednictwem systemów teleinformatycznych, czy może o relacje tych systemów z użytkownikami. Jeżeli to drugie to mielibyśmy do czynienia z upodmiotowieniem rzeczy (systemów teleinformatycznych), które wchodzą w jakieś relacje z ludźmi (ich użytkownikami).

Wskazana wyżej *Doktryna cyberbezpieczeństwa RP* z 2015 roku podaje także definicję **cyberprzestrzeni RP**, podobną do tej z *Rządowego program ochrony cyberprzestrzeni RP na lata 2011-2016*: „cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)". Wytyczono zatem granice w odterytorialnionym bycie, który z założenia nie ma granic. Była to próba wskazania „obszaru" cyberprzestrzeni, który podlegałby polskiej jurysdykcji i był miejscem operowania polskich służb bezpieczeństwa i obrony.

Rain Ottis i Peeter Lorents z natowskiego Cooperative Cyber Defence Centre of Excellence w Tallinie twierdzą, że nie ma wspólnej definicji cyberprzestrzeni, a te, które są używane, są często niejasne lub brakuje w nich kluczowych elementów. Autorzy proponują własną definicję: „cyberprzestrzeń to zależny od czasu zestaw połączonych ze sobą systemów informatycznych i użytkowników, którzy wchodzą w interakcje z tymi systemami"[27]. Jako systemy informatyczne autorzy rozumieją informacje, sprzęt, oprogramowanie i elementy, które je łączą. Cyberprzestrzeń tworzą jednak użytkownicy (w oryginale *human users*) – cyberprzestrzeń to sztuczna przestrzeń stworzona przez ludzi dla ludzkich celów.

2. Pojęcie cyberbezpieczeństwa

[27] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications*, [w:] *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010*, Wright-Patterson AFB 2010. Zob. także: M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 129-130.

Trudności ze zdefiniowaniem pojęcia cyberbezpieczeństwa są związane ze wskazanymi wyżej cechami niedookreśloności cyberprzestrzeni. Można je rozumieć jako bezpieczeństwo cybernetyczne, bezpieczeństwo cyberprzestrzeni albo bezpieczeństwo w cyberprzestrzeni.

Należy zauważyć, że w języku angielskim istnieją dwa słowa określające bezpieczeństwo: *safety* i *security*. Pierwsze z nich używane jest często w odniesieniu do bezpieczeństwa osób i zabezpieczenia ich podstawowych potrzeb życiowych, drugie – bezpieczeństwu zasobów (w szczególności w odniesieniu do aspektów ekonomicznych, zarządczych a także technicznych, w tym informatycznych), przede wszystkim w aspekcie potencjalnych zagrożeń spowodowanych celową działalnością człowieka. Słowo *safety*, pochodzi od wyrażenia *to be safe*, a samo słowo *safe* ma źródłosłów łaciński – *salvus* ('zdrowy; cały'). W języku polskim od łacińskiego słowa pochodzi staropolskie „salwować" ('ratować; wybawić; ocalać'). Drugie znaczenie w języku angielskim oddaje słowo *security* pochodzące od łacińskiego *securitas*, będącego zrostem dwóch wyrazów: *se* – oznaczającego oddzielnie, osobno (lub *sine* 'bez') oraz *cura* – troska, staranie, dbałość o coś lub o kogoś, opieka, piecza, jak w wyrażeniu *sine cura vivere* – 'żyć bez troski'[28].

W języku polskim bezpieczeństwo to stan „bez pieczy", czyli inaczej „bez opieki", „bez ochrony", „niewymagający opieki". Podmiot bezpieczny, to taki któremu nic nie zagraża, beztroski[29]. Społeczny wymiar bezpieczeństwa tworzy podstawę dla koncepcji podmiotowych bezpieczeństwa i subiektywnego jego ujęcia. Oznacza to, że bezpieczeństwo ma z jednej strony wymiar obiektywny – rzeczywisty stan braku zagrożenia, jak i subiektywny, odnoszący się do indywidualnie pojmowanego i uświadomionego poczucia istnienia bezpieczeństwa.

---

[28] D. Lisiak-Felicka. M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 15-16.

[29] W.T. Modzelewski, M. Hartliński, *Wprowadzenie do podstawowych kategorii bezpieczeństwa narodowego*, [w:] *Podstawowe kategoria bezpieczeństwa narodowego*, [red.] A. Żukowski, M. Hartliński, W.T. Modzelewski, J. Więcławski, Olsztyn 2015, s. 11.

Definiowanie cyberbezpieczeństwa jest ściśle związane z definicją cyberprzestrzeni. Jeżeli przyjmiemy normatywne ujęcie ISO 27032, to cyberbezpieczeństwo (*cybersecurity*) oznaczać będzie bezpieczeństwo informacji (opisane w normie ISO 27000) rozumiane jako zachowanie przynajmniej trzech jej atrybutów – poufności, integralności i dostępności – w cyberprzestrzeni. Należy zaznaczyć, że norma ta rozróżnia także *cybersafety* definiowane jako stan ochrony przed fizycznymi, społecznymi, duchowymi, finansowymi, politycznymi, emocjonalnymi, zawodowymi, psychologicznymi, edukacyjnymi lub innymi rodzajami skutków awarii, uszkodzeń, błędów, wypadków, krzywd lub jakichkolwiek innych zdarzeń w cyberprzestrzeni, które można uznać za niepożądane.

Z kolei Międzynarodowy Związek Telekomunikacyjny (ITU) w rekomendacji ITU-T X.1205 z 2008[30] roku definiuje cyberbezpieczeństwo jako zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i techniki, które można wykorzystać do ochrony cyberśrodowiska oraz zasobów organizacji i użytkownika. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania poziomu bezpieczeństwa zasobów organizacji i użytkownika przed odpowiednimi zagrożeniami w środowisku cybernetycznym. Generalnie celem cyberbezpieczeństwa jest, podobnie jak w ISO 27032: dostępność, integralność (w tym autentyczność i niezaprzeczalność) oraz poufność. Warto zwrócić uwagę, że ITU nie użyło terminu „cyberprzestrzeń" tylko „środowisko cybernetyczne" (*cyber environment*), co nie jest pozbawione sensu, zwarzywszy na mnogość i rozbieżność definiowania cyberprzestrzeni.

W polskich dokumentach znajdziemy różne definicje cyberbezpieczeństwa, które szerzej zostaną opisane w ostatnim rozdziale. Przykładowo *Strategia Cyberbezpieczeństwa RP na lata 2017-2022* odzwierciedla zapisy normy ISO 27032, ale utożsamia termin pojęcie

[30] *Recommendation X.1205 (04/08)*, International Telecommunication Union, [online:] https://www.itu.int/rec/T-REC-X.1205-200804-I/en [dostęp: 10.03.2024].

cyberbezpieczeństwa z bezpieczeństwem sieci i systemów teleinformatycznych, traktując je jako synonimy. Z kolei przygotowywany w 2009 roku *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011* nie definiował cyberbezpieczeństwa, ograniczając się do stwierdzenia: „Celem strategicznym *Programu* jest wzrost poziomu bezpieczeństwa cyberprzestrzeni państwa". Natomiast osiągnięcie tego celu „wymaga stworzenia ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy podmiotami administracji publicznej oraz innymi podmiotami, których zasoby stanowią krytyczną infrastrukturę teleinformatyczną kraju, na wypadek ataków terrorystycznych wykorzystujących publiczne sieci teleinformatyczne". Wynika z tego, że najważniejszym zagrożeniem był atak terrorystyczny z wykorzystaniem publicznych sieci teleinformatycznych na rządowe i prywatne elementy krytycznej infrastruktury teleinformatycznej (czyli cyberterroryzm).

Z powyższych wstępnych rozważań wynika wniosek, że mamy przynajmniej dwa rozumienia terminu cyberbezpieczeństwo. Pierwszy odnosi się do bezpieczeństwa informacyjnego rozumianego jako bezpieczeństwo podmiotu (człowieka lub organizacji), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. Innymi słowy bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji[31]. Ponieważ w aktualnej rzeczywistości zdecydowana większość informacji i systemów informacyjnych przetwarzana jest w sposób elektroniczny w systemach teleinformacyjnych, zatem cyberbezpieczeństwo oznacza bezpieczeństwo informacyjne w cyberprzestrzeni (lub cyberśrodowisku) – idąc tropem normy ISO 27032. Można też cyberprzestrzeń potraktować fizycznie, jako kolejną sferę działania podmiotów (jak ląd, powietrze, wodę) i wówczas można do niej przenieść normy stosowane w świecie rzeczywistym. Tym tokiem idzie Unia Europejska, która stwierdza w swojej strategii bezpieczeństwa

[31] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22.

cybernetycznego[32], że „cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami", a celem ochrony cyberprzestrzeni powinno być „zapewnienie dostępu i otwartości, poszanowania i ochrony praw podstawowych w internecie oraz utrzymanie niezawodności i interoperacyjności internetu". Zatem zasadniczym założeniem tak pojętego cyberbezpieczeństwa jest zastosowanie tych samych norm, zasad i wartości, które UE wspiera w „realu", tzn. ochrony praw podstawowych, gwarancji demokracji i praworządność.

Podsumowując można stwierdzić, że termin cyberbezpieczeństwo jest ściśle związany z konkretnym rozumieniem cyberprzestrzeni i jest pewną konwencją terminologiczną. Cyberbezpieczeństwo rozumiane jako **bezpieczeństwo cyberprzestrzeni** oznaczać będzie podejmowanie działań chroniących szeroko rozumianą infrastrukturę telekomunikacyjną (sieci teleinformatyczne, komputery, urządzenia, systemy i oprogramowanie) przed różnego rodzaju zagrożeniami (awarie, włamania, terroryzm itp.). Z kolei **bezpieczeństwo w cyberprzestrzeni** dotyczy podmiotu (państw, organizacji, ludzi), który, jako jej użytkownik, powinien czuć się w niej bezpieczny, np. dzięki pewności, że w cyberprzestrzeni obowiązuje prawo takie samo, jak w świecie rzeczywistym (prawo karne, prawo ochrony danych osobowych czy wolność wypowiedzi).

Wskazówki bibliograficzne

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2/2.

Czyżak M, *Bezpieczeństwo w cyberprzestrzeni*, „Teka Komisji Prawniczej PAN Oddział w Lublinie" 2018, nr 11/2.

[32] *Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP))*, [online:] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex:52013JC0001.

Kuzior A., Janczyk J., *Cyberprzestrzeń – poszerzona przestrzeń społeczna – wybrane obszary ewaluacji*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2016, nr 87.

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

Pala M., *Wybrane aspekty bezpieczeństwa w cyberprzestrzeni*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, nr 1.

Przyklenk J., *Cyberprzestrzeń w polskim dyskursie parlamentarnym*, „Forum Lingwistyczne" 2020, nr 7.

Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13/9.

Wasilewski J., *Zarys definicyjny cybeprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 5/9.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe: Status quo i perspektywy*, Warszawa 2020.

Rozdział 2

Problematyka cyberbezpieczeństwa w regulacjach Organizacji Narodów Zjednoczonych i Rady Europy

1. Działalność ONZ

Działania legislacyjne Organizacji Narodów Zjednoczonych w obszarze cyberbezpieczeństwa na poziomie międzynarodowym ograniczają się do rezolucji Zgromadzenia Ogólnego. Rezolucje ZO są wyłącznie zaleceniami kierowanymi do państw członkowskich.

Kwestię cyberbezpieczeństwa ONZ podjęła po raz pierwszy w rezolucji ZO nr 45/121 z 14.12.1990 roku[1]. Zatwierdzono w niej zalecenia VIII Kongresu ONZ w sprawie Zapobiegania Przestępczości. Rezolucja zwraca uwagę na przestępstwa z wykorzystaniem komputera i zaleca państwom członkowskim podjęcie skutecznych działań na rzecz zwalczania nadużyć komputerowych, np. w zakresie dokonania zmian w prawie materialnym i procesowym dostosowujących przepisy uwzględniające nowy charakter przestępczości.

Kwestia bezpieczeństwa informacji, rozwoju ICT i ochrony cyberprzestrzeni znajduje się w porządku obrad ONZ od 1998 roku, kiedy to Federacja Rosyjska przedstawiła projekt rezolucji w tej sprawie w pierwszym Komitecie Zgromadzenia Ogólnego ONZ. Została ona następnie przyjęta bez głosowania przez Zgromadzenie Ogólne jako Rezolucja nr 53/70. Od tego czasu utworzono kilka procesów międzyrządowych w celu uwzględnienia bezpieczeństwa i wykorzystania ICT w kontekście bezpieczeństwa międzynarodowego.

[1] https://digitallibrary.un.org/record/105578?v=pdf [dostęp: 10.12.2023].

Rezolucja ZO nr 53/70 z 4.12.1998 roku dotyczyła rozwoju sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego[2]. W dokumencie podkreślono duże znaczenie nauki i techniki w rozwoju cywilizacji oraz we współpracy dla dobra wspólnego wszystkich państw, wzmocnieniu potencjału twórczego ludzkości oraz usprawnienia obiegu informacji w społeczności globalnej. Wyrażono jednak zaniepokojenie, że nowe technologie mogą zostać wykorzystane do celów zagrażających utrzymaniu stabilności i bezpieczeństwa na świecie. Dlatego wezwano państwa członkowskie do zgłaszania Sekretariatowi Generalnemu rezultatów obserwacji i wniosków odnośnie do opracowania definicji zjawisk związanych z bezpieczeństwem informacji oraz celowości przygotowania międzynarodowych zasad, które zwiększyłyby globalne bezpieczeństwo systemów teleinformatycznych, w tym w zwalczaniu przestępczości i terroryzmu.

Następne rezolucje były konsekwencją X Kongresu ONZ i dotyczyły zwalczania kryminalnych nadużyć w technikach informacyjnych. Były to rezolucje nr 55/63 z 4.12.2000[3] i nr 56/121 z 19.12.2001 roku[4]. Wezwano w nich państwa członkowskie do wprowadzenia regulacji gwarantujących skuteczną ochronę integralności i dostępności danych w systemach komputerowych, a także wprowadzenia przepisów realizujących zwalczanie przestępstw dokonywanych z użyciem IT. Wymaga to współpracy między państwami, organizacjami międzynarodowymi i sektorem prywatnym. Rezolucja 56/121 została podjęta kilka tygodni po podpisaniu Konwencji Rady Europy o cyberprzestępczości (o czym dalej), w której zapisano m.in. konieczność współpracy organów państw w ściganiu przestępców komputerowych. Do tego wzywały także rezolucje ONZ. Należy zauważyć, że walka z przestępczym wykorzystywaniem IT wymaga opracowania rozwiązań uwzględniających ochronę wolności i prywatności jednostki, jak i zachowanie zdolności państw do skutecznego przeciwdziałania tego rodzaju nadużyciom.

---

[2] https://digitallibrary.un.org/record/265311?v=pdf [dostęp: 10.12.2023].

[3] https://digitallibrary.un.org/record/428861?v=pdf [dostęp: 10.12.2023].

[4] https://digitallibrary.un.org/record/454952?v=pdf [dostęp: 10.12.2023].

Globalnej kulturze cyberbezpieczeństwa były poświęcone kolejne dwie rezolucje – nr 57/239 z 20.12.2002[5] oraz 58/199 z 23.12.2003 roku[6]. W pierwszej stwierdzono, że potrzeba cyberbezpieczeństwa wzrasta w miarę zwiększania przez kraje swojego udziału w społeczeństwie informacyjnym. Podkreślono, że ważna jest świadomość, odpowiedzialność i etyka w użytkowaniu internetu, ale także demokracja – bezpieczeństwo powinno być wdrażane w sposób zgodny z wartościami uznawanymi przez społeczeństwa demokratyczne, w tym wolnością wymiany myśli i idei, swobodnym przepływem informacji, poufnością informacji i komunikacji, odpowiednią ochroną danych osobowych, otwartością i przejrzystością. W drugiej rezolucji większy nacisk położono na konieczność ochrony infrastruktury krytycznej, szczególnie IT.

Rezolucja nr 60/177 z 16.12.2005 roku[7] zatwierdziła deklarację końcową XI Kongresu ONZ dotyczącego Zapobieganiu Przestępczości i Wymiaru Sprawiedliwości ws. Karnych (Bangkok, Tajlandia), która stanowi załącznik do rezolucji. Przedmiotem rozważań Kongresu była m.in. analiza użycia systemów komputerowych w działalności przestępczej oraz jej ponadnarodowy charakter. W 16 punkcie deklaracji z zadowoleniem przyjęto wysiłki na rzecz wzmocnienia i uzupełnienia istniejącej współpracy w celu zapobiegania, badania i ścigania przestępstw związanych z wysoką technologią i komputerami, w tym poprzez rozwój partnerstw z sektorem prywatnym. Doceniono wkład Organizacji Narodów Zjednoczonych w regionalne i inne międzynarodowe fora w walce z cyberprzestępczością i zaproszono Komisję ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości w Sprawach Karnych (CCPCJ) do zapewnienia dalszej pomocy w tym obszarze (pod egidą ONZ), we współpracy z innymi podobnie ukierunkowanymi organizacjami.

---

[5] https://digitallibrary.un.org/record/482184?v=pdf [dostęp: 14.01.2024].

[6] https://digitallibrary.un.org/record/509571?v=pdf [dostęp: 14.01.2024].

[7] https://digitallibrary.un.org/record/563311?v=pdf [dostęp: 14.01.2024].

W rezolucji 64/211 z 21.12.2009 roku[8] podsumowano dotychczasowe wysiłki krajowe w zakresie kultury cyberbezpieczeństwa i ochrony teleinformatycznej infrastruktury krytycznej. Wezwano państwa członkowskie do dalszych prac w tej dziedzinie. W odniesieniu do rozwoju krajowej kultury cyberbezpieczeństwa podkreślono konieczność wdrożenia planów cyberbezpieczeństwa dla systemów rządowych, opracowania krajowych programów podnoszenia świadomości zagrożeń, zwłaszcza wśród dzieci i indywidualnych użytkowników internetu, oraz wymagań dotyczących szkoleń w zakresie ochrony infrastruktury.

XII Kongres ONZ obradował w kwietniu 2010 roku w Salwadorze (Brazylia) i jego rekomendacje znalazły odzwierciedlenie w Rezolucji nr 65/230 z 21.12.2010 roku[9]. Rezolucja zobowiązała Biuro NZ ds. Narkotyków i Przestępczości (UNODC) do opracowania i wdrożenia globalnego programu zwalczania cyberprzestępczości. Zwrócono się do Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości w Sprawach Karnych (CCPCJ) o rozważenie zwołania otwartej międzyrządowej grupy ekspertów w celu przeprowadzenia wszechstronnej analizy problemu cyberprzestępczości i reakcji na niego ze strony Państw Członkowskich, społeczności międzynarodowej i sektora prywatnego, w tym wymiany informacji na temat przepisów krajowych, najlepszych praktyk, pomocy technicznej i współpracy międzynarodowej, w celu zbadania możliwości wzmocnienia istniejących i zaproponowania nowych krajowych i międzynarodowych prawnych lub innych reakcji na zjawisko cyberprzestępczości.

Począwszy od 2004 r., sześć grup ekspertów rządowych (*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*) badało zagrożenia związane z wykorzystaniem ICT w kontekście bezpieczeństwa międzynarodowego i sposoby rozwiązania tych zagrożeń. Cztery z tych grup uzgodniły sprawozdania merytoryczne z wnioskami i zaleceniami, które zostały przyjęte z zadowoleniem przez wszystkie państwa

[8] https://digitallibrary.un.org/record/673712?v=pdf [dostęp: 14.01.2024].

[9] https://digitallibrary.un.org/record/700722?v= pdf [dostęp: 14.01.2024].

członkowskie ONZ. Każda grupa opierała się na pracy wykonanej przez poprzednią, co czyni znaczne postępy w zakresie omawianych kwestii. Szósta i ostatnia GGE, która spotkała się w latach 2019–2021, uzgodniła swoje sprawozdanie w drodze konsensusu, które dostarczyło dodatkowej warstwy zrozumienia ram normatywnych dla odpowiedzialnego zachowania państw w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego[10].

Poniżej znajduje się lista sprawozdań merytorycznych uzgodnionych przez grupy ekspertów:

1. 2009–2010 – A/65/201;
2. 2012–2013 – A/68/98;
3. 2014–2015 – A/70/174;
4. 2019–2021 – A/76/135.

W grudniu 2018 r., na mocy rezolucji 73/27[11], Zgromadzenie Ogólne utworzyło otwartą grupę roboczą (OEWG), która była otwarta dla wszystkich państw członkowskich[12]. Grupa rozpoczęła pracę w 2019 roku i odbyła międzysesyjne spotkania konsultacyjne z przemysłem, społeczeństwem obywatelskim i środowiskiem akademickim. Grupa przyjęła sprawozdanie w drodze konsensusu na sesji końcowej w marcu 2021 r. (A/75/816[13]). Sprawozdanie końcowe i zawarte w nim zalecenia zostały zatwierdzone w decyzji Zgromadzenia Ogólnego 75/564.

W 2020 r. Zgromadzenie Ogólne w drodze rezolucji 75/240[14], ustanowiło nową pięcioletnią OEWG w sprawie bezpieczeństwa i wykorzystania technologii informacyjno-komunikacyjnych. OEWG będzie spotykać się regularnie do 2025 roku. Dostępna jest dedykowana strona internetowa dla tej OEWG[15].

---

[10] Dorobek z działalności grupy znajduje się [online:] https://disarmament.unoda.org/group-of-governmental-experts/ [dostęp 14.01.2024].

[11] https://digitallibrary.un.org/record/1655670?v=pdf [dostęp: 14.01.2024].

[12] https://disarmament.unoda.org/open-ended-working-group/ [dostęp: 14.01.2024].

[13] https://digitallibrary.un.org/record/3908015?v=pdf [dostęp: 14.01.2024].

[14] https://digitallibrary.un.org/record/3896458?v=pdf [dostęp: 14.01.2024].

[15] https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021 [dostęp: 14.01.2024].

Prace GGE i OEWG skupiały się na następujących tematach:

- Istniejące i pojawiające się zagrożenia;
- Jak zastosowanie ma prawo międzynarodowe w zakresie korzystania z ICT;
- Normy, zasady i zasady odpowiedzialnego zachowania państw
- Środki budowy zaufania;
- Budowanie potencjału.

W 2022 r. po raz pierwszy przyjęto rezolucję Zgromadzenia Ogólnego (77/37) zatytułowaną „Program działania na rzecz postępu w zakresie odpowiedzialnego zachowania państwa w zakresie technologii informacyjnych i komunikacyjnych w kontekście bezpieczeństwa międzynarodowego”[16], w której z zadowoleniem przyjęto konkluzje zamieszczone w raportach grup ekspertów z 2010, 2013, 2015 i 2021 roku oraz w dotychczasowych raportach OEWG.

Pomimo 25-letniej pracy i opracowaniu kilkunastu raportów i rezolucji, postęp w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego jest raczej niewielki. Działania ONZ ograniczają się do apelowania do państw członkowskich o nieużywanie ICT w sposób inny niż pokojowy oraz do stosowania w cyberprzestrzeni przez państwa pokojowego prawa międzynarodowego (np. nieagresji). ONZ zauważa, że rozpowszechnianie i wykorzystywanie technologii i środków informacyjnych wpływa na interesy całej społeczności międzynarodowej. Wyraża także zaniepokojenie, że te technologie i środki mogą być potencjalnie wykorzystywane do celów niezgodnych z celami utrzymania międzynarodowej stabilności i bezpieczeństwa i mogą niekorzystnie wpłynąć na integralność infrastruktury państw ze szkodą dla ich bezpieczeństwa zarówno w sferze cywilnej, jak i wojskowej.

Rezolucje i decyzje Zgromadzenia Ogólnego w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego (*field of information and telecommunications in the context of international security*):

---

[16] https://digitallibrary.un.org/record/3997617?v=pdf [dostęp: 14.01.2024].

2023 – A/RES/78/237, A/RES/78/16, A/DEC/78/541;
2022 – A/RES/77/36, A/RES/77/37, A/DEC/77/512;
2021 – A/RES/76/19;
2020 – A/RES/75/240;
2019 – A/RES/74/28; A/RES/74/29;
2018 – A/RES/73/266; A/RES/73/27;
2017 – A/72/404;
2016 – A/RES/71/28;
2015 – A/RES/70/237;
2014 – A/RES/69/28;
2013 – A/RES/68/243;
2012 – A/RES/67/27;
2011 – A/RES/66/24;
2010 – A/RES/65/41;
2009 – A/RES/64/25;
2008 – A/RES/63/37;
2007 – A/RES/62/17;
2006 – A/RES/61/54;
2005 – A/RES/60/45;
2004 – A/RES/59/61;
2003 – A/RES/58/32;
2002 – A/RES/57/53;
2001 – A/RES/56/19;
2000 – A/RES/55/28;
1999 – A/RES/54/49;
1998 – A/RES/53/70.

Kwestiami powiązanymi z cyberbezpieczeństwem zajmowały się także inne agencje ONZ. Wysoki Komisarz Narodów Zjednoczonych do spraw praw człowieka (UNHCR) podjął temat prawa do prywatności w erze cyfrowej (sprawozdania: A/HRC/43/52, A/HRC/46/37, A/HRC/49/55, A/75/147 i A/76/220), organizując w tej sprawie dwa warsztaty ekspertów, które odbyły się w dniach 19-20 lutego 2018 oraz

27-28 maja 2020 roku. W rezolucji nr 77/211 z 15.12.2022 roku[17] doceniono postęp w rozwoju ICT jednak zauważono, że zwiększają one możliwości rządów, przedsiębiorstw i osób fizycznych do podejmowania nadzoru, przechwytywania, hakowania i gromadzenia danych, co może naruszać lub nadużywać praw człowieka, w szczególności prawa do prywatności. Naruszenia i nadużycia prawa do prywatności w erze cyfrowej mogą mieć wpływ na wszystkie osoby, ze szczególnym uwzględnieniem kobiet, dzieci, w szczególności dziewcząt, osób niepełnosprawnych i osób starszych, a także osób znajdujących się w trudnej sytuacji. Zgromadzenie Ogólne potwierdziło, że prawa, które ludzie mają w trybie offline, muszą być również chronione w trybie online, w tym prawo do prywatności, ze szczególnym uwzględnieniem ochrony dzieci. Przypomniano, że państwa powinny zapewnić, aby wszelka ingerencja w prawo do prywatności była zgodna z zasadami legalności, konieczności i proporcjonalności.

Należy także wspomnieć o dorobku Forum Zarządzania Internetem (Internet Governance Forum – IGF), które zostało wyłonione w 2005 roku podczas Światowego Szczytu Społeczeństwa Informacyjnego (The World Summit on the Information Society – WSIS), działającego pod auspicjami ONZ. Rezolucją ZO nr 70/125 z grudnia 2015 roku[18] przedłużono mandat IGF o kolejne 10 lat (do 2025 r.). Mandat obejmuje m.in. omawianie polityki publicznej związanej z kluczowymi elementami zarządzania internetem w celu wspierania stabilności, bezpieczeństwa i rozwoju internetu, w tym omawianie zagadnień, które nie wchodzą w zakres jakiegokolwiek innego organu międzynarodowego, wymianę informacji i najlepszych praktyk, identyfikacja pojawiających się problemów oraz ewentualne wydawanie zaleceń czy wcielanie zasad WSIS w procesach zarządzania internetem. WSIS posiada stronę

[17] https://digitallibrary.un.org/record/3999709?v=pdf [dostęp: 14.01.2024].
[18] https://digitallibrary.un.org/record/819076?v=pdf [dostęp: 14.01.2024].

internetową[19], podobnie jak IGF[20]. W 2021 roku doroczne spotkanie IGF odbyło się w Katowicach.

W dziedzinie cyberbezpieczeństwa IGF poszukuje rozwiązań w następujących sześciu obszarach:

1. Praktyki i mechanizmy cyberbezpieczeństwa: Jakie są dobre praktyki cyberbezpieczeństwa i międzynarodowe mechanizmy, które już istnieją? Gdzie te mechanizmy zawodzą i co można zrobić, aby wzmocnić bezpieczeństwo i zaufanie?
2. Zapewnienie bezpiecznej przestrzeni cyfrowej: W jaki sposób rządy, firmy internetowe i inne zainteresowane strony powinny chronić obywateli, w tym obywateli narażonych na ataki, przed wykorzystywaniem i nadużyciami online?
3. Normy międzynarodowe: W jaki sposób normy międzynarodowe powinny uwzględniać różne wymagania i preferencje rządów i obywateli w różnych krajach?
4. Role i obowiązki w zakresie ochrony przed cyberatakami: Które zainteresowane strony odpowiadają za ochronę rządów krajowych, firm i obywateli przed cyberatakami?
5. Przepisy międzynarodowe i odpowiedzialność państwa: W jaki sposób należy wzmocnić przepisy międzynarodowe, aby chronić suwerenność narodową i obywateli przed atakami złośliwych podmiotów państwowych i niepaństwowych? Co można zrobić, aby lepiej pociągnąć państwa narodowe do odpowiedzialności za cyberataki?
6. Odpowiedzialność sektora prywatnego: Co można zrobić na szczeblu krajowym i międzynarodowym, aby zająć się firmami sektora prywatnego, które pomagają i podżegają atakujących z państw narodowych?[21]

Ostatnią organizacją podejmującą tematykę cyberbezpieczeństwa jest Międzynarodowy Związek Telekomunikacyjny (International

[19] https://www.itu.int/net/wsis/

[20] https://www.intgovforum.org/en.

[21] https://www.intgovforum.org/en/content/trust-security-and-stability [dostęp: 15.01.2024].

Telecommunication Union – ITU), który jest organizacją wyspecjalizowaną ONZ ustanowioną w celu standaryzowania oraz regulowania rynku telekomunikacyjnego i radiokomunikacyjnego. W ramach ITU działają trzy sektory. Każdy z nich jest odpowiedzialny za wybrany obszar związany z celami określonymi w Konstytucji Związku:

ITU-T – Sektor Normalizacji Telekomunikacji;

ITU-R – Sektor Radiokomunikacji;

ITU-D – Sektor Rozwoju Telekomunikacji.

Sektor Normalizacji Telekomunikacji wydał np. zalecenie ITU-T X.1500 odnoszące się do wymiany informacji dotyczących bezpieczeństwa cyberprzestrzeni (CYBEX), czy cytowaną w rozdziale 1 ITU-T X.1205, w której podano definicję cyberbezpieczeństwa. Różnymi aspektami cyberbezpieczeństwa zajmuje się przede wszystkim Sektor Rozwoju Telekomunikacji, szczególnie w ramach „programu cyberbezpieczeństwa". Program oferuje członkom ITU – szczególnie krajom rozwijającym się – możliwość i narzędzia do zwiększania możliwości cyberbezpieczeństwa na poziomie krajowym, w celu zwiększenia bezpieczeństwa, budowania zaufania do korzystania z technologii ICT – czyniąc przestrzeń cyfrową bezpieczniejszą i pewniejszą dla wszystkich. Praca i mandat programu cyberbezpieczeństwa opierają się na 5. priorytecie planu działań ITU-D przyjętego na Światowej Konferencji Rozwoju Telekomunikacji w 2022 roku. Więcej informacji o działalności ITU-D w zakresie cyberbezpieczeństwa można znaleźć na dedykowanej stronie internetowej[22].

Ponadto ITU w 2007 roku uruchomiło Globalny Program Cyberbezpieczeństwa (ITU Global Cybersecurity Agenda – GCA), stanowiący ramy współpracy międzynarodowej, którego celem jest zwiększenie zaufania i bezpieczeństwa w społeczeństwie informacyjnym. GCA wspiera inicjatywy, takie jak ochrona dzieci w internecie (Child Online Protection[23]), i wspólnie ze wsparciem wiodących globalnych graczy ze wszystkich grup interesariuszy, wdraża rozwiązania z zakresu

[22] https://www.itu.int/itu-d/sites/cybersecurity/

[23] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx

cyberbezpieczeństwa w krajach na całym świecie. GCA opiera się na pięciu filarach strategicznych, znanych również jako obszary robocze:

- środki prawne;
- środki techniczne i proceduralne;
- struktury organizacyjne;
- budowanie potencjału;
- współpraca międzynarodowa.

2. Konwencja Rady Europy

Na poziomie regionalnym (europejskim) podstawy międzynarodowoprawne cyberbezpieczeństwa tworzy *Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 roku.* Weszła ona w życie 1 lipca 2004 roku jako pierwsza umowa międzynarodowa, która regulowała kwestię przestępczości komputerowej. Polska była sygnatariuszem *Konwencji*, jednak jej ratyfikacja prze RP nastąpiła dopiero w 2014 roku, a ogłoszenie w Dzienniku Ustaw – w 2015 roku[24].

Rada Europy już w latach 80. XX wieku zaczęła koncentrować się na cyberprzestępczości jako kwestii prawa karnego. Zaowocowało to dwoma dokumentami prawa miękkiego Komitetu Ministrów: pierwszy – Rekomendacja nr R (89) 9 w sprawie przestępstw komputerowych, czyli prawa karnego materialnego, zostało przyjęte w 1989 roku[25]; a drugi – Rekomendacja nr R (95) 13 dotycząca problemów prawa karnego procesowego związanego z techniką informatyczną, została przyjęta w 1995 roku[26].

W połowie lat 90. problem cyberprzestępczości stał się coraz bardziej palący. W związku z tym w lutym 1997 roku Komitet Ministrów Rady Europy postanowił powołać Komitet Ekspertów ds. Przestępczości w Cyberprzestrzeni (Committee of Experts on Crime in Cyberspace –

[24] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015.728.

[25] https://search.coe.int/archives?i=0900001680910c99

[26] https://search.coe.int/archives?i=0900001680910c9c

PC-CY), którego zadaniem było opracowanie wiążącej międzynarodowej konwencji o cyberprzestępczości. Od samego początku traktat ten miał być stosowany także poza obszarem Rady Europy, dlatego w jego negocjacjach uczestniczyły takie pozaeuropejskie państwa jak np. Kanada, Japonia, Republika Południowej Afryki i Stany Zjednoczone Ameryki. Po dwudziestu pięciu spotkaniach PC-CY i jej „grupy redakcyjnej" oraz kolejnych sesjach zwołanych między kwietniem 1997 a czerwcem 2001 roku w celu sfinalizowania tekstu i raportu wyjaśniającego do konwencji, *Konwencja o cyberprzestępczości* została przyjęta i otwarta do podpisu 23 listopada 2001 r. w Budapeszcie[27].

Zgodnie z zapisami ujętymi w preambule, celem Konwencji jest prowadzenie wspólnej polityki, która ma za zadanie ochronę społeczeństwa przed przestępczością cybernetyczną, poprzez prowadzenie działań mających powstrzymać czynności związane z łamaniem zasad poufności, integralności, dostępności do systemów teleinformatycznych oraz ich nieprawidłowym wykorzystaniu. W celu zapewnienia skuteczności powyższych działań, niezbędne było przyjęcie odpowiednich przepisów prawnych, które miały opierać się na współpracy międzynarodowej, nie tylko organów państwowych, ale także z prywatnymi przedsiębiorcami i organizacjami. Tylko szeroka współpraca wszystkich zainteresowanych stron umożliwia podjęcie skoordynowanych działań, które ułatwią wykrywanie przestępstw, prowadzenie śledztw, gromadzenie materiału dowodowego oraz skazanie winnych łamania przepisów. W preambule podkreślono, że wszystkie wskazane wyżej działania powinny być prowadzone z poszanowaniem praw człowieka, w szczególności – dotyczących wolności opinii, wypowiedzi i poszanowania prywatności.

Konwencja Budapeszteńska wyróżnia następujące cztery rodzaje cyberprzestępstw:

1. Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów:

---

[27] *Convention on cybercrime. Special edition dedicated to the drafters of the Convention (1997-2001)*, Council of Europe 2022, s. 6 [online:] https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e.

a) Nielegalny dostęp (art. 2);
b) Nielegalne przechwytywanie danych (art. 3);
c) Naruszenie integralności danych (art. 4);
d) Naruszenie integralności systemu (art. 5);
e) Niewłaściwe użycie urządzeń (art. 6);

2. Przestępstwa komputerowe:
   a) Fałszerstwo komputerowe (art. 7);
   b) Oszustwo komputerowe (art. 8);
3. Przestępstwa ze względu na charakter zawartych informacji (związane z pornografią dziecięcą) – art. 9;
4. Przestępstwa związane z naruszeniem praw autorskich i pokrewnych (art. 10).

Ponadto za przestępstwo jest uznawane także usiłowanie, pomocnictwo lub podżeganie do popełnienia powyższych czynów (art. 11). Co istotne ścigane i karane za przestępstwa mają być nie tylko osoby fizyczne, ale także osoby prawne, np. przedsiębiorcy, którzy oferują oprogramowanie służące łamaniu kodów, dostawcy usług internetowych z pedofilskimi treściami czy oferujący miejsce na serwerach z piracką muzyką.

Uzupełnieniem *Konwencji* są dwa protokoły dodatkowe:

1. Protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący kryminalizacji aktów o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych (ETS Nr 189) – otwarty do podpisu 28.01.2003 roku[28];
2. Drugi protokół dodatkowy do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania dowodów elektronicznych (CETS Nr 224) – otwarty do podpisu 12.05.2022 roku[29].

Należy zaznaczyć, że m.in. tematyce przestępstw związanych z pornografią dziecięcą jest poświęcony także inny, późniejszy akt prawa międzynarodowego – *Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach*

[28] Dz.U. 2015.730.

[29] Dz.Urz. UE, L 2023.63.28.

seksualnych, sporządzona w Lanzarote dnia 25 października 2007 r.[30], w której preambule przywoływana jest *Konwencja Budapeszteńska*.

Konwencja w dalszych częściach reguluje zasady prawa procesowego, jurysdykcji oraz współpracy międzynarodowej. Przykładowo art. 35 zobowiązuje państwa do utrzymywania punktu kontaktowego dostępnego 24 godziny na dobę przez 7 dni w tygodniu w celu zapewnienia natychmiastowej pomocy dla celów prowadzenia czynności śledczych, w tym np. zbierania dowodów w postaci elektronicznej dokonywanych przestępstw.

Konwencji o cyberprzestępczości nie sposób nie docenić. Stanowi ona efektywne narzędzie międzynarodowej ochrony podmiotów wykorzystujących techniki teleinformatyczne oraz podmiotów, wobec których ICT umożliwiają lub ułatwiają popełnianie czynów zabronionych. *Konwencja* jest pierwszym (i na razie jedynym) aktem prawa międzynarodowego w tym zakresie. Zgodnie z pojęciem cyberprzestrzeni, która nie jest wytyczona granicami, zakres jej oddziaływania wykracza poza „obszar cyberprzestrzeni państw członkowskich Rady Europy". Jej stroną są m.in. USA, Kanada, Japonia i RPA. ONZ, także w omawianych wyżej rezolucjach, stawia *Konwencję Budapeszteńską* za wzór prawa międzynarodowego i namawia inne międzynarodowe organizacje kontynentalne do przyjęcia podobnych rozwiązań w swoich regionach.

* * *

W 2019 roku zapisy *Konwencji* zakwestionowała Federacja Rosyjska, mimo że nie jest uczestnikiem. Rosja postawiła sprawę na forum ONZ i po kilku latach pracy w 2023 roku pojawiły się projekty nowej konwencji[31], która – według pierwotnych planów – powinna zastać przyjęta na sesji ONZ na przełomie stycznia i lutego 2024 roku.

Projekt traktatu o cyberprzestępczości, ma na celu zdefiniowanie, czym właściwie jest przestępczość internetowa i w jaki sposób państwa

[30] Dz.U. 2015.608.

[31] https://digitallibrary.un.org/record/4067171?ln=en&v=pdf [dostęp: 10.01.2024].

członkowskie mogą lepiej współpracować, aby ograniczyć rosnący globalny problem. Wiele rządów i obrońców praw obywatelskich obawia się jednakże, że traktat – pierwotnie zaproponowany przez Rosję, przy wsparciu takich państw jak Chiny, Korea Północna, Iran, Wenezuela i Nikaragua – utoruje drogę reżimom do legalizacji inwigilacji ponad granicami oraz kryminalizacji wypowiedzi online, pozornie przy wsparciu społeczności międzynarodowej[32].

Podczas negocjacji strony nie zgadzały się, czy konwencja powinna dotyczyć przestępstw, które mogą być popełnione wyłącznie przy użyciu komputerów lub sieci, czy też obejmować również inne przestępstwa popełnione przy użyciu ICT. W przypadku pierwszego, traktat zdefiniowałby i kryminalizował szereg przestępstw zależnych od cyberprzestrzeni oraz przewidywałby środki proceduralne, za pomocą których państwa mogłyby wspólnie badać i egzekwować te działania. Niektóre państwa, które zgadzają się z tą wizją – w tym Nowa Zelandia, Kanada i Stany Zjednoczone – zasugerowały, że określone przestępstwa z wykorzystaniem cyberprzestrzeni mogą również wchodzić w zakres traktatu, jeśli ich skala znacząco się rozprzestrzeniła dzięki wykorzystaniu ICT (oszustwa cyfrowe i rozpowszechnianie materiałów przedstawiających wykorzystywanie seksualne dzieci). Po drugiej stronie debaty niektóre państwa, w tym Rosja i Chiny, oczekiwały, że konwencja będzie dotyczyć szerokiego zakresu działań przestępczych prowadzonych przy użyciu ICT (z wykorzystaniem cyberprzestrzeni) oprócz przestępstw zależnych od cyberprzestrzeni. Indie, Chiny i Indonezja były wśród państw, które zaproponowały, aby konwencja kryminalizowała rozpowszechnianie dezinformacji lub „szkodliwych informacji". Wniosek Rosji z 2021 r. wymieniał 24 bezprawne czyny, które miałyby zostać ustanowione na

---

[32] P. Gołąb, *Traktat ONZ o cyberprzestępczości może stać się „globalnym paktem nadzoru" ostrzegają obrońcy praw człowieka*, ITReseller, 28.08.2023, [online:] https://itreseller.pl/traktat-onz-o-cyberprzestepczosci-moze-stac-sie-globalnym-paktem-nadzoru-ostrzegaja-obroncy-praw-czlowieka/; K. Ławniczak, *Konwencja ONZ przeciwko cyberprzestępczości w ogniu krytyki. Może zwiększyć inwigilację rządową*, ITHARDWARE.PL, 22.08.2024 [online:] https://ithardware.pl/aktualnosci/konwencja_onz_cyberprzestepczosc_krytyka_inwigilacja-34638.html.

mocy traktatu, w tym handel narkotykami, zmuszanie do samobójstwa i „przestępstwa związane z ekstremizmem”[33].

Ostateczny projekt *Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości* wpłynął do Sekretariatu ONZ w dniu 7 sierpnia 2024 roku[34]. Podtytuł projektu brzmi: „Wzmocnienie współpracy międzynarodowej w celu zwalczania niektórych przestępstw popełnianych przy użyciu systemów informatycznych i telekomunikacyjnych oraz udostępniania dowodów w formie elektronicznej dotyczących poważnych przestępstw”. W projekcie stworzono katalog następujących przestępstw:

1. Nielegalny dostęp (art. 7);
2. Nielegalne przechwytywanie (art. 8);
3. Zakłócanie danych elektronicznych (art. 9);
4. Zakłócanie pracy systemu informatycznego i komunikacyjnego (art. 10);
5. Niewłaściwe użycie urządzeń (art. 11);
6. Fałszerstwo związane z systemami informatycznymi i komunikacyjnymi (art. 12);
7. Kradzież lub oszustwo związane z systemami informatyczno-komunikacyjnymi (art. 13);
8. Przestępstwa związane z wykorzystywaniem seksualnym dzieci w internecie lub materiałami przedstawiającymi wykorzystywanie seksualne dzieci (art. 14);
9. Nakłanianie lub przygotowywanie do popełnienia przestępstwa seksualnego wobec dziecka (art. 15);
10. Rozpowszechnianie intymnych wizerunków bez zezwolenia (art. 16);
11. Legalizowanie dochodów pochodzących z przestępstwa (art. 17).

---

[33] C. Plumb, *Understanding the UN's new international treaty to fight cybercrime*, UNU-CPR, 30.07.2024, [online:] https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

[34] https://digitallibrary.un.org/record/4066282?v=pdf [dostęp: 10.08.2024].

Prawdopodobnie na przełomie 2024 i 2025 roku nowa konwencja na poziomie globalnym zostanie przyjęta i otwarta do podpisu. Czas pokaże czy rozwiązania globalne zastąpią konwencję europejską.

Wskazówki bibliograficzne

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Maciejczuk M., Wnorowski K., Olchanowski M., *Cyberprzestrzeń a bezpieczeństwo dzieci w świetle rozwiązań Organizacji Narodów Zjednoczonych oraz Rady Europy*, „Zeszyty Naukowe Zbliżenia Cywilizacyjne" 2018, nr 14/3.

Pawlak A., *Ochrona dzieci przed cyberprzestępczością w systemie Organizacji Narodów Zjednoczonych*, [w:] *Potrzeby jako współczesny determinant treści praw człowieka*, [red.] E. Ura, B. Sitek, T. Graca, Józefów 2017.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Skrzypczak J., *Bezpieczeństwo teleinformatyczne w świetle Europejskiej konwencji i cyberprzestępczości*, „Przegląd Strategiczny" 2011, nr 1.

Wąsik K., *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni*, „Cybersecurity and Law" 2023, nr 10/2.

Rozdział 3

Cyberbezpieczeństwo w dokumentach Unii Europejskiej

1. Rozwój europejskiego społeczeństwa informacyjnego

Kwestia cyberbezpieczeństwa w Unii Europejskiej jest nierozłącznie związana z jej wizją społeczeństwa informacyjnego. W latach 80. XX wieku rewolucja komunikacyjna spowodowała radykalne zmiany w europejskim systemie audiowizualnym. W 1982 roku powstała Euromedia Research Group, będącą europejską siecią przedstawicieli nauk społecznych prowadzących badania nad skutkami zastosowania nowych mediów, w tym nad wspólną polityką europejską w tej dziedzinie. W 1983 roku Europejska Fundacja Kultury oraz Uniwersytet w Manchesterze powołały Europejski Instytut Badań nad Mediami. Od 1985 roku Instytut na zlecenie III i X Dyrektoriatu Wspólnoty Europejskiej prowadził badania nad zmianami technologicznymi, ekonomicznymi, kulturowymi i politycznymi w europejskim sektorze audiowizualnym, telekomunikacyjnym i komputerowym.

Wcześniej, bo już w 1978 roku Simon Nora i Alain Minc przedstawili raport na temat społecznych skutków i kosztów informatyzacji we Francji[1]. Raport został sporządzony na zlecenie prezydenta Francji Valéry'ego Giscarda d'Estaing i był podstawą pierwszej w Europie narodowej strategii budowania społeczeństwa informacyjnego. Autorzy m.in. wprowadzili termin „informatyzacja" dla zdefiniowania procesów zmian wiodących do powstania społeczeństwa informacyjnego. Termin

[1] S. Nora, A. Minc, *L'Informatisation de la société*, La Documentation française: Paris Janvier 1978, [online :] https://www.vie-publique.fr/rapport/34772-linformatisation-de-la-societe.

ten zawdzięcza jednak popularność Niemcowi Martinowi Bangemannowi, który jako komisarz ds. przemysłu oraz technologii informacyjnych i telekomunikacyjnych, przygotował w 1994 roku raport *Europa a społeczeństwo globalnej informacji – zalecenia dla Rady Europejskiej*[2], nazywany *Raportem Bangemanna*. W rzeczywistości pojęcie „społeczeństwo informacyjne" pojawiło się w politycznej doktrynie UE po raz pierwszy w grudniu 1993 r. wraz z publikacją *Białej Księgi*[3]. W dokumencie tym Komisja Europejska zwróciła uwagę na problematykę nowych technik informacyjno-komunikacyjnych oraz wyzwania i możliwości, jakie stwarzają one dla krajów europejskich.

W *Raporcie Bangemanna* opowiedziano się po stronie rynkowego i komercyjnego modelu rozwoju ICT, podkreślano wagę liberalizacji sektora telekomunikacyjnego i konkurencji. Zaproponowano dziesięć inicjatyw, które obejmowały m.in. takie obszary, jak telepraca, szkolenia na odległość, usługi teleinformatyczne dla małych i średnich przedsiębiorstw oraz komputeryzacja sektora zamówień publicznych. Sektor publiczny powinien podjąć konkretne kroki w celu opracowania odpowiednich regulacji prawnych, ochrony obywateli i konsumentów oraz podnoszenia świadomości społeczeństwa. W konsekwencji *Raportu* Komisja Europejska powołała dwa ciała doradcze: forum ds. społeczeństwa informacyjnego oraz grupę ekspertów najwyższego szczebla. Ich zadaniem była analiza społecznych, socjalnych i kulturowych aspektów społeczeństwa nowego typu. Postulaty zawarte w dokumencie wyznaczyły perspektywy i kierunki działań, w jakich powinny zmierzać kraje europejskie i polityka Unii Europejskiej.

---

[2] *Europe and the Global Information Society: Recommendation to the European Council*, Brussels, 26 May 1994, [online:] https://op.europa.eu/en/publication-detail/-/publication/31a0bebe-4bc6-4f31-a319-7b7799e45d86/language-en.

[3] *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century – White Paper*, COM(93) 700, [online:] https://op.europa.eu/en/publication-detail/-/publication/4e6ecfb6-471e-4108-9c7d-90cb1c3096af/language-en.

Działanie organów UE doprowadziło do uchwalenia trzech istotnych dokumentów – „zielonych ksiąg", które stały się podstawą tworzenia wiążących regulacji prawnych Unii Europejskiej[4].

Strategia Lizbońska[5] to jeden z podstawowych aktów planowania UE; przyjęta została na posiedzeniu Rady Europejskiej w marcu 2000 roku. Jej podstawowym założeniem było przyjęcie, że w ciągu dziesięciu lat uda się przekształcić gospodarkę europejską w najbardziej konkurencyjną na świecie. *Strategia* w punktach 8-11 (*An information society for all*) zawierała konkluzje inicjatywy *eEurope* i poleciła organom Unii opracowanie szczegółowego planu działania (*eEurope Action Plan*). Inicjatywa *eEurope* została przedstawiona Radzie Europejskiej przez Komisję Europejską 8 grudnia 1999 roku. Warto wspomnieć, że przewodniczący Komisji Romano Prodi był jednym z członków grupy, która opracowała *Raport Bangemanna*. Do realizacji celów *Strategii Lizbońskiej* Komisja przedstawiła wkrótce dwa programy do realizacji na lata 2000-2002 (*eEurope 2002*) i 2003-2005 (*eEurope 2005*), a także *eEurope+* dla państw kandydujących do członkostwa UE (w tym Polski).

W dokumencie *eEurope 2002* infrastruktura informacyjna została zdefiniowana jako podstawowe narzędzie komunikowania obywateli w UE oraz jako główny nośnik jej sukcesu gospodarczego. Ataki na systemy informacyjne uznano za zagrożenie dla społeczeństwa informacyjnego i zalecono wspólną prewencję na poziomie Unii. W agendzie

---

[4] *Green Paper. Living and Working in Information Society. People First*, COM(96) 389 Final, [online:] https://op.europa.eu/en/publication-detail/-/publication/8bcd9942-f9ef-4fe7-9637-936af5c0fd85/language-en; *Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for Regulation – Towards an information society approach,* COM(97) 623 Final, [online:] https://op.europa.eu/en/publication-detail/-/publication/3967c098-852d-4774-af8b-691e70b40395/language-en; *Public sector information: a key resource for Europe – Green Paper on public sector information in the information society*, COM(1998) 585 Final, [online:] https://op.europa.eu/en/publication-detail/-/publication/599834ce-7a43-44fe-8cd8-334b3c 19feba/language-en.

[5] *Lisbon European Council 23 and 24 March 2000 Presidency Conclusions*, [online:] https://www.europarl.europa.eu/summits/lis1_en.htm; https://www.europarl.europa.eu/bulletins/pdf/1s2000en.pdf.

eEurope 2005 zauważono m.in., że tworzenie warunków do realizacji transakcji online musi być skorelowane z działaniami na rzecz bezpieczeństwa informatycznego. Do zadań KE należało wspomaganie projektów podnoszących świadomość użytkowników w kwestii bezpieczeństwa transakcji i treści w internecie. Od 2002 roku w Unii toczyła się dyskusja nad koniecznością powołania zespołu ds. cyberbezpieczeństwa (*cyber security task force*), jako europejskiego centrum informacji o zagrożeniach w sieci i walki z przestępczością internetową. Ostatecznie centrum powstało w 2004 roku pod nazwą European Network and Information Security Agency (ENISA)[6].

Kolejna strategia UE ws. rozwoju społeczeństwa informacyjnego to *i2010 – Europejskie społeczeństwo informacyjne do 2010 r.*[7]. Napisano w niej, że – jako kluczowy element odnowionego partnerstwa lizbońskiego na rzecz wzrostu i zatrudnienia – strategia *i2010* będzie wspierać zintegrowane podejście w unijnej polityce dotyczącej społeczeństwa informacyjnego i mediów audiowizualnych. Komisja Europejska zaproponowała trzy priorytety strategiczne, w tym jako pierwszy ukończenie jednolitej europejskiej przestrzeni informacyjnej wspierającej otwarty i konkurencyjny rynek wewnętrzny w dziedzinie społeczeństwa informacyjnego i mediów. W tym obszarze zauważono cztery wyzwania: szybkość, zawartość multimedialna, interoperacyjność i bezpieczeństwo, rozumiane jako „lepsze zabezpieczenie internetu przed oszustwami, szkodliwą zawartością i awariami technologicznymi zwiększające zaufanie inwestorów i konsumentów do tego medium".

---

[6] Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz.Urz. UE, L 2002.077.

[7] Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów - „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia" {SEC(2005) 717} [COM/2005/0229 końcowy], [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52005DC0229.

Punktem zwrotnym w zintegrowanym podejściu do problematyki cyberbezpieczeństwa była *Europejska agenda cyfrowa (EAC)*[8], będąca elementem strategii *Europa 2020*[9]. Zauważono w tych dokumentach, że użytkownicy nie mają zaufania co do bezpieczeństwa nie tylko płatności internetowych, ale w ogóle związanych z ochroną życia prywatnego. Należało zatem przygotować swoisty kodeks, zawierający jasne i przystępne streszczenia praw jednostki w internecie. Zwrócono także uwagę na konieczność budowania systemów przeciwdziałających atakom cyberterrorystycznym.

Komunikaty Komisji i rezolucja Parlamentu z 20 maja 2010 roku przygotowały grunt pod *Akt o jednolitym rynku* (COM(2010)0608) wprowadzający szereg środków mających na celu pobudzenie gospodarki UE i tworzenie miejsc pracy. W październiku 2012 roku Komisja opublikowała *Akt o jednolitym rynku II* (COM(2012)0573) zawierający 12 działań podstawowych skoncentrowanych na czterech głównych czynnikach wzrostu gospodarczego, zwiększania zatrudnienia oraz pogłębiania zaufania: zintegrowanych sieciach, mobilności transgranicznej, gospodarce cyfrowej oraz działaniach sprzyjających spójności i przynoszących korzyści konsumentom.

6 maja 2015 r. Komisja przyjęła *Strategię jednolitego rynku cyfrowego*[10], która opiera się na trzech filarach: łatwiejszym dostępie do towarów i usług cyfrowych w całej UE; stworzeniu warunków dla sieci cyfrowych i innowacyjnych usług; oraz maksymalizacji potencjału wzrostu tkwiącego w gospodarce cyfrowej. Działania związane z cyberbezpieczeństwem są prowadzone w ramach drugiego filaru. W ślad za strategią przyjęto serię środków ustawodawczych, które miały doprowadzić do powstania jednolitego rynku cyfrowego. Dotyczyły one takich kwestii jak transgraniczne doręczanie paczek, transgraniczne przenoszenie usług online w zakresie treści, audiowizualne usługi medialne, cyfrowe prawo autorskie (dyrektywa (UE) 2019/790), umowy sprzedaży

[8] COM(2010) 245.

[9] COM(2010) 2020.

[10] COM(2015) 192 final.

towarów przez internet i w inny sposób na odległość oraz umowy o dostarczanie treści i usług cyfrowych (dyrektywa (UE) 2019/770). Następnie jednolity rynek cyfrowy wzmocniono m.in. uruchomienie jednolitego portalu cyfrowego (rozporządzenie (UE) 2018/1724); zmniejszenie kosztów wdrażania szybkich sieci łączności elektronicznej (dyrektywa 2014/61/UE); oraz wprowadzenie przepisów dotyczących identyfikacji elektronicznej (rozporządzenie (UE) nr 910/2014) i europejskiego cyberbezpieczeństwa (dyrektywa (UE) 2016/1148).

Aby przyspieszyć powstanie jednolitego rynku cyfrowego, 20 października 2020 r. Parlament Europejski przyjął rezolucję w sprawie aktu o usługach cyfrowych[11]. Zalecił w niej, by pakiet ten wzmocnił rynek wewnętrzny, zagwarantował ochronę konsumentów, zapewnił jednakowe traktowanie działalności w internecie i w tradycyjnej gospodarce, utrzymał przejrzystość, zagwarantował poszanowanie praw i objął swoim zakresem działalność podmiotów spoza UE, które mają wpływ na konsumentów w UE. 15 grudnia 2020 r. Komisja przedstawiła dwa wnioski ustawodawcze: akt o usługach cyfrowych i akt o rynkach cyfrowych. Ich główne cele to stworzenie bezpieczniejszej przestrzeni cyfrowej, w której podstawowe prawa użytkowników usług cyfrowych będą należycie respektowane, oraz stworzenie równych warunków działania, by wspierać innowacje, wzrost gospodarczy i konkurencyjność na jednolitym rynku europejskim i na świecie. Akt o usługach cyfrowych (rozporządzenie (UE) 2022/2065)[12] i akt o rynkach cyfrowych (rozporządzenie (UE) 2022/1925) weszły w życie w maju 2023 roku.

W marcu 2021 Rada przyjęła unijny program „Cyfrowa Europa", obejmujący lata 2021–2027 z mocą wsteczną od 1 stycznia 2021 roku[13]. Wśród kluczowych dziedzin nowej strategii cyfrowej UE znalazły się:

---

[11] Dz.Urz. UE, C2021.404/31.

[12] Dz.Urz. UE, L 2022.277/1.

[13] Stanowisko Rady w pierwszym czytaniu w sprawie przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" oraz uchylającego decyzję (UE) 2015/2240 - Przyjęte przez Radę w dniu 16 marca 2021 r. (nr 6789/1/20). https://data.consilium.europa.eu/doc/document/ST-6789-2020-REV-1/pl/pdf [10.09.2021].

1. Suwerenność cyfrowa;
2. Usługi cyfrowe, gwarantujące bezpieczeństwo użytkowników oraz tworzące wolną i konkurencyjną przestrzeń do funkcjonowania przedsiębiorstw, działających w sektorze cyfrowym;
3. Gospodarka oparta na danych;
4. Sztuczna inteligencja i jej znaczenie w tworzeniu innowacji głównie w sektorach bezpieczeństwa, edukacji i opieki zdrowotnej;
5. Technologie prorozwojowe w postaci chmury obliczeniowej, technologii kwantowych i obliczeń wielkiej skali;
6. Konektywność, której wyrazem ma stać się powszechna łączność, umożliwiająca dostęp do usług cyfrowych;
7. Europejska identyfikacja cyfrowa (e-ID);
8. e-Zdrowie oraz transformacja cyfrowa w sektorze opieki zdrowotnej;
9. Umiejętności cyfrowe i edukacja cyfrowa celem zarówno pozyskania wykwalifikowanych specjalistów cyfrowych, jak i podniesienia świadomości istnienia i ochrony przed cyberzagrożeniami;
10. Cyfryzacja wymiaru sprawiedliwości;
11. Cyberbezpieczeństwo, bez którego wszystkie wyżej wymienione aspekty nie będą w pełni funkcjonalne.

W programie „Cyfrowa Europa" cyberbezpieczeństwo odgrywa kluczową rolę. Powodem jest stale rosnąca skala cyberzagożeń i bezsprzeczne uzależnienie wzrostu wskaźników gospodarczych od efektywności wykorzystania infrastruktury cyfrowej. Bezpieczna, otwarta i powszechna cyberprzestrzeń, która dla UE jest fundamentem rozwoju gospodarczego, nie może funkcjonować bez mechanizmów zwiększających zaufanie do cyfrowych technologii. Dla unijnych przywódców oznaczało to podjęcie niezbędnych działań do uzyskania unijnej strategicznej samodzielności w zakresie cyberbezpieczeństwa.

2. Strategiczne dokumenty Unii Europejskiej w dziedzinie cyberbezpieczeństwa

W pierwotnym (traktatowym) prawie UE niewiele miejsca poświęcono cyberbezpieczeństwu. Traktaty sprzed Lizbony były podpisywane jeszcze w erze przedinternetowej. UE wpływa i kształtuje politykę cyberbezpieczeństwa państw członkowskich poprzez powiązanie jej z innymi politykami, poprzez ustalanie definicji, standardów, certyfikacji i innych procedur. Istotne są także mniej techniczne tematy, które obejmują kształtowanie świadomości społecznej w zakresie cyberzagrożeń, budowanie umiejętności i wiedzy poprzez edukację i wymianę doświadczeń. Fundamentem polityki UE jest rozwój oraz stabilne funkcjonowanie jednolitego rynku wewnętrznego.

Na poziomie prawa wtórnego uchwalono kilkadziesiąt dyrektyw, rozporządzeń i decyzji[14], które odnoszą się w różnym stopniu do bezpieczeństwa cybernetycznego. Najważniejsze z nich to:

1. Rozporządzenie 2004/460 Parlamentu Europejskiego i Rady z 10.03.2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA).
2. Decyzja ramowa 2005/222/WSiSW Rady z 24.02.2005 r. ws. ataków na systemy informatyczne;
3. Decyzja Parlamentu Europejskiego i Rady 2005/854/WE z 11.05.2005 r. ws. ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z internetu i nowych technologii sieciowych;
4. Dyrektywa 2008/11/WE ws, rozpoznania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony;
5. Komunikat Komisji z 28.03.2012 r. – Zwalczanie przestępczości w erze cyfrowej; ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością;

---

[14] Por. H. Wyrębek, *Cyberprzestrzeń. Zagrożenia, strategie bezpieczeństwa*, Siedlce 2021, s. 96-97.

6. Rezolucja Parlamentu Europejskiego z 12.06.2012 r. ws. ochrony krytycznej infrastruktury teleinformatycznej – Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni (2011/2284(INI));
7. Rezolucja Parlamentu Europejskiego z 22.11.2012 r. ws. bezpieczeństwa cybernetycznego i cyberobrony (2012/2096(INI));
8. Dyrektywa 2013/40/UE z 12.08.2013 r., której celem jest usprawnienie współpracy właściwych organów państw w dziedzinie ataków na systemy informatyczne oraz ustanowienie minimalnych norm dotyczących określenia przestępstw i kar w dziedzinie ataków na systemy informatyczne; zastąpiła Decyzję 2005/222/WSiSW;
9. Dyrektywa 2016/1148 z 6.07.2016 r. (NIS)– jest pierwszym aktem prawa Unii w zakresie cyberbezpieczeństwa.
10. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego, COM(2016) 410 final z 5.07.2016 r.

Przegląd dokumentów strategicznych w zakresie cyberbezpieczeństwa należy rozpocząć od *Strategii na rzecz bezpiecznego społeczeństwa informacyjnego* z 2006 roku[15]. W dokumencie stwierdzono, że mimo działań podejmowanych na poziomie międzynarodowym, europejskim i krajowym kwestia bezpieczeństwa nadal stanowi poważne wyzwanie. Naruszenie bezpieczeństwa sieci i informacji może mieć skutki wykraczające poza wymiar gospodarczy. W istocie, powszechne są obawy, że problemy bezpieczeństwa mogą zniechęcić użytkowników i zmniejszyć popyt na technologie teleinformatyczne, podczas gdy

[15] Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy" {SEC(2006) 656} /* COM/2006/0251 końcowy */, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX: 52006DC0251.

dostępność, niezawodność i bezpieczeństwo są niezbędnym warunkiem zapewnienia ochrony praw podstawowych w Internecie. Zarówno przedsiębiorcy, jak i obywatele w Europie nadal lekceważą ryzyko naruszeń bezpieczeństwa. Bezpieczne społeczeństwo informacyjne musi opierać się na zwiększonym bezpieczeństwie sieci i informacji oraz powszechnej kulturze bezpieczeństwa. W tym celu Komisja Europejska proponuje dynamiczne, zintegrowane podejście obejmujące wszystkie zainteresowane podmioty, oparte na dialogu, partnerstwie i przejmowaniu inicjatywy.

Strategia została wzmocniona Rezolucją Rady Europejskiej z marca 2007 roku[16], w której przypomniano m.in., że zaufanie jest zasadniczym elementem sukcesu nowego społeczeństwa informacyjnego; zaufanie związane jest także z doświadczeniami użytkowników oraz potrzebą poszanowania ich prywatności; dlatego też bezpieczeństwo sieci i informacji nie powinno być uważane jedynie za kwestię techniczną. Wiedza o bezpieczeństwie sieci i informacji oraz umiejętności z nim związane muszą stać się integralną częścią codziennego życia każdej osoby i zainteresowanej strony funkcjonującej w społeczeństwie. Dlatego zwrócono się do państwa członkowskich o wspieranie programów szkoleń oraz zwiększanie ogólnej wiedzy na temat kwestii bezpieczeństwa sieci i informacji oraz zwiększenie wkładu w związane z bezpieczeństwem badania i rozwój. Zaapelowano także do ENISA do dalszego działania w bliskiej współpracy z państwami członkowskimi, Komisją i innymi odpowiednimi zainteresowanymi stronami, a także do wspomagania podejmowanych przez Komisję i państwa członkowskie działań zmierzających do sprostania wymaganiom bezpieczeństwa sieci i informacji.

Po sześciu latach (7.02.2013 r.) Komisja Europejska zaproponowała *Strategię bezpieczeństwa cybernetycznego UE* [17] , która jest

[16] Rezolucja Rady z dnia 22 marca 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie, Dz.Urz. UE, C 2007.68/1.

[17] Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń

pierwszym dokumentem strategicznym UE w zakresie cyberbezpieczeństwa. W tym samym czasie KE przedstawiła również projekt *Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (tzw. Dyrektywa NIS). *Strategia* była poprzedzona m.in. dwiema rezolucjami Parlamentu Europejskiego z 2012 roku

Strategia podkreśliła, że technologie informacyjno-komunikacyjne stanowią fundament wzrostu gospodarczego i mają krytyczne znaczenie, ponieważ leżą u podstaw złożonych systemów, które napędzają gospodarkę w sektorach, takich jak finanse, opieka zdrowotna, energetyka i transport. Z tego powodu niezwykle istotne jest budowanie trwałej współpracy w zakresie cyberbezpieczeństwa pomiędzy administracją i kluczowymi sektorami gospodarki. Potrzebę tę miał zaadresować przede wszystkim projekt Dyrektywy NIS.

Wskazano następujące zasady bezpieczeństwa cybernetycznego:

1. Podstawowe wartości UE mają zastosowanie w świecie cyfrowym w taki sam sposób, jak w świecie fizycznym;
2. Ochrona praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności;
3. Dostęp dla wszystkich;
4. Demokratyczne i efektywne zarządzanie wielostronne;
5. Wspólna odpowiedzialność za zapewnienie bezpieczeństwa.

Strategia wyznaczyła pięć kierunków działań, które miały zapewnić większy poziom bezpieczeństwa cybernetycznego UE:

1. Osiągnięcie odporności na zagrożenia cybernetyczne;
2. Radykalne ograniczenie cyberprzestępczości;
3. Opracowanie polityki obronnej i rozbudowa zdolności bezpieczeństwa cybernetycznego w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony UE;
4. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cyberprzestrzeni;

/*JOIN/2013/01 final */, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52013JC0001.

5. Ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Strategia wskazuje na potrzebę wprowadzenia rygorystycznych i skutecznych przepisów w celu zwalczania cyberprzestępczości. W tym kontekście odnosi się do:

- Dyrektywy 2011/93/UE o zwalczaniu wykorzystywania seksualnego dzieci w Internecie, określającej normy przestępstw CSAM oraz ich karania, zapobiegania, wsparcia ofiar czy usuwania treści CSAM z Internetu;
- Dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne, a także określającej normy przestępstw komputerowych i ich karania;
- Powołania Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3) w ramach Europolu, które miało zwiększyć zdolność operacyjną działań zapobiegających i zwalczających przestępczość w cyberprzestrzeni.

Komisja podkreśla także, że zagrożenia, incydenty a także przestępstwa popełniane w cyberprzestrzeni nie mają granic. Dlatego wszystkie podmioty – począwszy od organów ds. bezpieczeństwa sieci i informacji, poprzez CERT-y, organy ścigania i przedstawicieli branży teleinformatycznej – muszą wziąć wspólną odpowiedzialność za zapewnienie bezpieczeństwa cybernetycznego, zarówno na poziomie krajowym, jak i Unii Europejskiej.

Celem działań opisanych w *Strategii* ma być uczynienie środowiska internetowego UE najbezpieczniejszym na świecie, w oparciu o silną ochronę i wspieranie praw obywateli.

13 września 2017 r. Komisja Europejska przedstawiła komunikat[18] będący aktualizacją *Strategii Cyberbezpieczeństwa UE*. Silniejszy nacisk położono na kwestię wspólnej odpowiedzi państw członkowskich na międzynarodowe incydenty oraz współpracę sektora cywilnego z militarnym.

---

[18] COM(2017)476 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0476.

W komunikacie Komisja podkreśliła, że w ciągu kilku ostatnich lat rozwój technologii cyfrowych osiągnął bardzo wysokie tempo, a jego oddziaływanie zaczęło mieć znaczący wpływ na właściwie każdy aspekt codziennego życia oraz globalnej gospodarki. Wraz z dynamicznym postępem transformacji cyfrowej zwiększyła się również skala występujących zagrożeń. Dlatego zapewnienie odpowiedniego poziomu cyberbezpieczeństwa stało się kluczowe dla sprawnego funkcjonowania państwa. KE zapowiedziała, że jej celem jest zwiększenie zdolności technologicznych i umiejętności w dziedzinie cyberbezpieczeństwa, a także budowa silnego Jednolitego Rynku Cyfrowego. Interesującą kwestią jest też silne zbliżenie wojskowych i cywilnych kwestii związanych z cyberbezpieczeństwem oraz zapowiedziane wzmocnienie ENISA.

Założenia Komisji opierały się na trzech filarach:

Filar I – Budowanie odporności UE na ataki cybernetyczne

- Wzmocnienie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA);
- Rozwój w kierunku jednolitego rynku bezpieczeństwa cybernetycznego;
- Wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji (Dyrektywa NIS);
- Odporność dzięki szybkiemu reagowaniu w sytuacji kryzysowej;
- Stworzenie sieci ośrodków kompetencji w dziedzinie bezpieczeństwa cybernetycznego oraz Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego;
- Budowanie silnej unijnej bazy umiejętności cybernetycznych;
- Propagowanie cyberhigieny i świadomości zagrożeń.

Filar II – Kształtowanie skutecznej unijnej prewencji cybernetycznej

- Identyfikacja podmiotów działających w złych intencjach;
- Doskonalenie reagowania przez organy ściągania;
- Publiczno-prywatna współpraca w zwalczaniu cyberprzestępczości;
- Doskonalenie reagowania politycznego;

- Kształtowanie prewencji w zakresie bezpieczeństwa cybernetycznego za pomocą potencjału obronnego państw członkowskich.

Filar III – Wzmocnienie współpracy międzynarodowej w dziedzinie bezpieczeństwa cybernetycznego

- Bezpieczeństwo cybernetyczne w stosunkach zewnętrznych;
- Budowanie zdolności w obszarze bezpieczeństwa cybernetycznego;
- Współpraca UE-NATO.

Jak stwierdzono wyżej KE wraz ze *Strategią Cyberbezpieczeństwa UE* przedłożyła projekt Dyrektywy NIS. Negocjacje w sprawie jej przyjęcia trwały trzy lata i została ona uchwalona w 2016 roku. *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* [19] **Dyrektywa NIS jest pierwszym europejskim prawem w zakresie cyberbezpieczeństwa** wprowadzającym regulacje międzysektorowe[20].

Dyrektywa zobowiązuje państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Jej przepisy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty. *Dyrektywa NIS* nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie. Dokument stanowi jednak harmonizację minimalną, a zatem wyznacza pewne minimalne warunki, które należy spełniać. Nie ogranicza przy tym możliwości państw członkowskich do regulowania problematyki cyberbezpieczeństwa administracji publicznej.

Zapisy *Dyrektywy* ogniskują się na trzech filarach: (1) instytucjach, które powinny powstać we wszystkich państwach członkowskich; (2)

---

[19] Dz. Urz. UE, L 2016.194.

[20] I. Oleksiewicz, *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka, strategia, prawo*, Warszawa 2021, s. 166.

współpracy na poziomie europejskim; (3) zobowiązaniach w zakresie bezpieczeństwa sieci i informacji.

W pierwszym filarze każde państwo członkowskie zostało zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji. Funkcję tą mogą pełnić już istniejące instytucje. Zadaniem organu właściwego jest monitorowanie wdrożenia przepisów dyrektywy na poziomie krajowym we wszystkich sektorach objętych regulacją. Państwa mogą wyznaczyć jeden lub kilka organów. Organy właściwe ds. bezpieczeństwa sieci i informacji będą miały uprawnienia do:

- badania przypadków niewypełniania przez operatorów usług kluczowych zobowiązań z zakresu bezpieczeństwa sieci i informacji;
- oceny wyników audytów bezpieczeństwa teleinformatycznego;
- wydawania wytycznych w zakresie bezpieczeństwa teleinformatycznego;
- wprowadzenia sankcji za nieprzestrzeganie przepisów.

Ponadto każde państwo członkowskie musi ustanowić Pojedynczy Punkt Kontaktowy (PPK, Single Point of Contact). Jego zadaniem jest wzmacnianie współpracy między państwami członkowskimi. Będzie również gromadził informacje o incydentach w skali kraju, a także wymieniał się informacjami o znaczących, międzynarodowych incydentach ze swoimi odpowiednikami z zagranicy.

Ostatnią instytucją w dyrektywie jest CSIRT, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Państwa członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, bądź zbudować sieć CSIRT-ów sektorowych, obejmujących sektory rynkowe.

Drugi filar wprowadza mechanizmy współpracy na dwóch poziomach:

- technicznym – ma być zapewniona poprzez europejską sieć CSIRT oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych pomiędzy CSIRT-ami wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych;

– polityczno-strategicznym – ma być realizowana poprzez utworzenie Grupy Współpracy, która zajmie się wypracowaniem wspólnych koncepcji strategicznych oraz będzie przyjmowała m.in. roczne raporty od właściwych organów.

Trzeci filar– zobowiązania w zakresie bezpieczeństwa sieci i informacji są różne w zależności od aneksu. Operatorzy usług kluczowych (aneks II) są zobowiązani do oceny ryzyka cyberzagrożeń oraz do przyjęcia odpowiednich środków, zapewniających bezpieczeństwo sieci i informacji. Muszą też zgłaszać właściwym organom wszelkie incydenty poważnie zagrażające ich sieciom i systemom informatycznym. Obowiązkowemu raportowaniu podlegają incydenty o „znaczącym wpływie na ciągłość działania operatorów", co *de facto* oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji przepisów dyrektywy.

Dostawcy usług cyfrowych (aneks III) są objęci regulacją *light touch approach*. Polega ona na kontroli *ex post*, tzn. po zaistnieniu incydentu i tylko przez państwo, na terenie którego dostawca usługi ma swoją siedzibę.

Dyrektywa nakłada także na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której określone zostaną m.in.: narodowe cele i priorytety cyberbezpieczeństwa, role i obowiązki organów administracji publicznej, zasady współpracy sektora publicznego i prywatnego, krajowa analiza ryzyka oraz zadania w zakresie edukacji.

Dyrektywa NIS daje organom publicznym konkretne narzędzia do przeciwdziała i reakcji na incydenty w cyberprzestrzeni. Są to m.in. obowiązkowe raportowanie, przygotowanie krajowej strategii NIS, skoordynowanie przepływu informacji czy też zinstytucjonalizowanie współpracy CSIRT-ów.

30 stycznia 2018 r. Komisja Europejska opublikowała Rozporządzenie Wykonawcze 2018/151[21]. Dokument dotyczy trzeciego aneksu *Dyrektywy NIS*, czyli dostawców usług cyfrowych. Rozporządzenie

[21] Dz.Urz. UE, L 2018.26/48.

doprecyzowuje elementy bezpieczeństwa sieci i systemów informatycznych, które mają zostać uwzględnione przez dostawców usług cyfrowych przy oferowaniu usług. Dokument obowiązuje od 10 maja 2018 roku.

W Polsce zapisy *Dyrektywy NIS* realizuje Ustawa o krajowym systemie cyberbezpieczeństwa z 28 sierpnia 2018 roku.

Akt o cyberbezpieczeństwie (Cybersecurity Act)[22], to **druga** po *Dyrektywie NIS* ogólnoeuropejska **regulacja prawna w zakresie cyberbezpieczeństwa**. Dokument wszedł w życie 27 czerwca 2019 roku i reguluje m.in. obszar certyfikacji cyberbezpieczeństwa. Akt o cyberbezpieczeństwie tworzy europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT oraz nadaje nowe, stałe kompetencje Agencji UE ds. Cyberbezpieczeństwa (ENISA).

Europejskie ramy certyfikacji cyberbezpieczeństwa pozwolą stymulować rozwój jednolitego rynku. Utworzenie ram pozwoli także ograniczyć koszty związane z testami i badaniami, poprawiając tym samym funkcjonowanie mechanizmów bezpieczeństwa. Poszerzona oferta rynkowa pozytywnie przyczyni się do większej dostępności cenowej bezpiecznego oprogramowania, urządzeń i usług dla przedsiębiorców, a także dla obywateli. Lepszy dostęp do certyfikowanych produktów przyczyni się również do ogólnego wzrostu cyberbezpieczeństwa i pozwoli zmniejszyć straty jakie ponoszą przedsiębiorcy w związku z cyberprzestępczością. Za przygotowywanie poszczególnych programów certyfikacji odpowiada **ENISA** (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji), która we współpracy z nowym organem, Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa (**ECCG**), przygotowuje kompleksowy zbiór wymogów technicznych, norm i procedur w celu oceny produktów i usług pod kątem odpowiednich zabezpieczeń.

---

[22] Wniosek Rozporządzenie Paramentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") COM/2017/0477 final/3 – 2017/0225(COD), https://eur-lex.europa.eu/ legal-content/PL/TXT/?uri=CELEX:52017PC0477R(02).

ECCG to jeden z najważniejszych organów, który powołuje do życia *Akt o cyberbezpieczeństwie*. Ponadto na mocy rozporządzenia powołano także Grupę Interesariuszy do spraw Certyfikacji Cyberbezpieczeństwa. Głównymi zadaniami tej grupy jest doradzanie Komisji w sprawach strategicznych związanych z europejskimi ramami certyfikacji cyberbezpieczeństwa.

Akt o cyberbezpieczeństwie przekształcił Europejską Agencje Bezpieczeństwa Sieci i Informacji w Agencję UE ds. Cyberbezpieczeństwa (ENISA). Pierwsza część dokumentu określa charakter nowego mandatu Agencji, który został przekształcony z mandatu czasowego na mandat stały. Rola ENISA została znacznie wzmocniona nie tylko poprzez nadanie stałych uprawnień, ale także poprzez szereg nowych obowiązków związanych z wejściem w życie dyrektywy NIS oraz europejskich ram certyfikacji. Obecnie ENISA ma większy wpływ na ekosystem cyberbezpieczeństwa UE.

Nowym zadaniem jest m.in. udzielanie pomocy państwom członkowskim i instytucjom unijnym. Na wyraźną prośbę państwa członkowskiego, ENISA oferuje wsparcie przy organizacji zespołów CSIRT. Udziela również niezbędnej i fachowej wiedzy będącej istotnym elementem w budowie kompetencji CSIRT, jak również pozwalającym analizować i przeciwdziałać cyberzagrożeniom i incydentom. W tej dziedzinie ważną rolę odgrywa współpraca pomiędzy ENISA, a z CERT-EU, obsługującym incydenty bezpieczeństwa w instytucjach unijnych.

Akt o cyberberbezpieczeństwie został nowelizowany w 2023 roku[23]. Doprecyzowano wówczas zapisy dotyczące przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa oraz zmodyfikowano zakres obowiązków ENISA (m.in. ENISA propaguje korzystanie z

[23] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa, COM(2023) 208 final, 2023/0108(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52023PC0208.

europejskiej certyfikacji cyberbezpieczeństwa z myślą o unikaniu rozdrobnienia rynku wewnętrznego; sporządza i publikuje wytyczne oraz opracowuje dobre praktyki dotyczące wymogów cyberbezpieczeństwa; ułatwia ustanowienie i upowszechnianie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem oraz dotyczących bezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa).

Drugim dokumentem strategicznym jest *Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę* z 16.12.2020 roku [24]. W pierwszym akapicie dokumentu napisano: „Cyberbezpieczeństwo stanowi integralny element bezpieczeństwa Europejczyków. Obywatele muszą mieć pewność, że gdy korzystają z urządzeń podłączonych do internetu lub z sieci elektroenergetycznych, udają się do banku, lecą samolotem, korzystają z usług administracji publicznej czy leżą w szpitalu, są chronieni przed cyberzagrożeniami. Gospodarka, demokracja i społeczeństwo UE bardziej niż kiedykolwiek polegają na bezpiecznych i niezawodnych narzędziach cyfrowych i łączności. Cyberbezpieczeństwo ma zatem zasadnicze znaczenie dla budowania odpornej, ekologicznej i cyfrowej Europy". Poprawa cyberbezpieczeństwa jest niezbędna, aby ludzie ufali innowacjom, łączności i automatyzacji, używali ich i czerpali z nich korzyści, a także aby zapewnić ochronę podstawowych praw i wolności, w tym prawa do prywatności i ochrony danych osobowych oraz wolności wypowiedzi i informacji. Cyberbezpieczeństwo jest niezbędne dla łączności sieciowej oraz globalnego i otwartego internetu, które muszą stanowić podstawę transformacji gospodarki i społeczeństwa w latach 20. XXI wieku.

Strategia ma na celu zapewnienie globalnego i otwartego internetu, który posiada silne zabezpieczenia umożliwiające sprostanie zagrożeniom dla bezpieczeństwa i podstawowych praw i wolności Europejczyków. Opierając się na postępach osiągniętych w ramach poprzednich

---

[24] Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX: 52020JC0018.

strategii, zawiera ona konkretne propozycje dotyczące stosowania trzech głównych instrumentów – instrumentów regulacyjnych, inwestycyjnych i politycznych – w celu zajęcia się trzema obszarami działań UE:

1. Odpornością, suwerennością technologiczną i przywództwem;
2. Budowaniem zdolności operacyjnych na potrzeby zapobiegania, odstraszania i reagowania;
3. Rozwojem globalnej i otwartej cyberprzestrzeni.

Cyberbezpieczeństwo należy włączyć do wszystkich tych inwestycji cyfrowych, w szczególności dotyczących kluczowych technologii, takich jak sztuczna inteligencja (AI), szyfrowanie i kwantowe technologie obliczeniowe, stosując zachęty, nakładając obowiązki i stosując poziomy odniesienia. Także na poziomie organów UE dostrzeżono zagrożenia – instytucje, organy i agencje UE są regularnym celem cyberataków, a zwłaszcza cyberszpiegostwa. Poszczególne instytucje, organy i agencje UE różnią się jednak znacznie, jeśli chodzi o poziom ich cyberodporności i zdolności do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie oraz związaną z tym dojrzałość. Konieczne jest zatem zwiększenie ogólnego poziomu cyberbezpieczeństwa poprzez przyjęcie spójnych i jednolitych zasad.

We wnioskach zapisano, że spójne wdrożenie *Strategii* przyczyni się do zapewnienia UE cyberbezpiecznej cyfrowej dekady, realizacji unii bezpieczeństwa oraz wzmocnienia pozycji UE na świecie. UE powinna odgrywać wiodącą rolę w opracowywaniu standardów i norm na potrzeby światowej klasy rozwiązań oraz norm z zakresu cyberbezpieczeństwa na potrzeby podstawowych usług i infrastruktury krytycznej, jak również w rozwijaniu i stosowaniu nowych technologii. Każda organizacja i każda osoba korzystająca z internetu jest częścią rozwiązania zapewniającego cyberbezpieczną transformację cyfrową.

13 maja 2022 r. Rada i Parlament Europejski osiągnęły porozumienie w sprawie przepisów dotyczących środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby jeszcze bardziej zwiększyć odporność i zdolność reagowania na incydenty, zarówno w sektorze publicznym i prywatnym, jak i całej UE. Prace nad

nową dyrektywą, nazywaną roboczo NIS 2, rozpoczęto już w grudniu 2020 roku[25].

Przyjęta 14 grudnia 2022 roku ***Dyrektywa NIS 2***[26] doprecyzowała i rozszerzyła przepisy zwiększające bezpieczeństwo sieci i systemów informatycznych, wprowadzone *Dyrektywą NIS* z 2016 roku. Zmienił się zarówno zakres podmiotowy, jak i przedmiotowy regulacji. Jednym z nowych rodzajów podmiotów, których dotyczyć będą obowiązki wynikające z *Dyrektywy NIS 2*, są dostawcy usług zaufania (DUZ). Ich zakres działania do tej pory regulowany był przede wszystkim rozporządzeniem 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS)[27], które do prawa polskiego wdrożone zostało ustawą o usługach zaufania oraz identyfikacji elektronicznej (Ustawa o UZIE).

Dyrektywa NIS 2 ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego. Prawodawca uznał, że w celu zapewnienia odpowiedniego poziomu bezpieczeństwa i nadzoru wobec dostawców usług zaufania, należy ich również objąć zakresem stosowania *Dyrektywy NIS 2*. Definiując w niej kwestie związane z usługami zaufania i ich dostawcami, odwołano się do podstawowych definicji określonych w *Rozporządzeniu eIDAS*.

---

[25] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 – Podejście ogólne, ST 14337 2021 INIT, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CONSIL%3AST_14337_2021_INIT.

[26] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz.Urz. UE, L 2022.333.

[27] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Dz.Urz. UE, L 2014.257.

Niezależnie od tego, jaki status posiada dostawca usług zaufania (kwalifikowany czy niekwalifikowany), jest on zobowiązany do wypełniania wszystkich obowiązków określonych w dyrektywie. Kwalifikowani DUZ są podmiotami kluczowymi, natomiast niekwalifikowani DUZ – ważnymi. Pierwszym z obowiązków jest podjęcie przez dostawców usług zaufania wszelkich odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone są ich usługi oraz zapewnienia bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności lub świadczenia usług. Mają one również zapobiegać wpływowi incydentów na odbiorców usług lub minimalizować taki wpływ. Drugim ważnym obowiązkiem jest zgłaszanie incydentów poważnych do odpowiedniego CSIRT lub właściwego organu. Ponadto dostawcy usług zaufania zostali również zobowiązani do powiadomienia odbiorców swoich usług o poważnych incydentach, które mogą mieć wpływ na ich świadczenie, a także – w przypadku odbiorców, których potencjalnie dotyczy poważne cyberzagrożenie – o środkach zaradczych. Oprócz tego, do obowiązków należy prowadzenie szkoleń (obowiązkowych dla kadry kierowniczej oraz zalecanych dla pracowników), stosowanie własnych lub nabytych certyfikowanych produktów, usług i procesów oraz zawiadamianie o uczestnictwie w mechanizmach wymiany informacji.

* * *

Kwestia cyberbezpieczeństwa jest przedmiotem także kilku innych dokumentów o znaczeniu strategicznym, które zostały przyjęte w ciągu ostatnich lat, np. program „Horyzont Europa”[28], czy też Planu

[28] Implementation Strategy for Horizon Europe, [online:] https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_implementation-strategy_he.pdf. [08.11.2023]; Horizon Europe Strategic Plan (2021–2024). https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3c6ffd74-8ac3-11eb-b85c-01aa75ed71a1 [10.11.2023].

Odbudowy dla Europy[29]. „Horyzont Europa" to unijny program finansowania badań i innowacji na lata 2021–2027, zastępujący wcześniejszy „Horyzont 2020". Zakłada przeznaczenie 49 mln EUR na badania nad innowacjami w systemach cyberbezpieczeństwa, tak aby zwiększyć ochronę przed zaawansowanymi cyberzagrożeniami. W 2016 roku zawarto partnerstwo publiczno-prywatne w zakresie cyberbezpieczeństwa w ramach programu „Horyzont 2020" między Komisją Europejską a Europejską Organizacją ds. Bezpieczeństwa Cybernetycznego (ECSO), stowarzyszeniem składającym się z członków z branży cyberbezpieczeństwa, środowisk akademickich, administracji publicznych i innych.Przyjęcie przez unijnych przywódców w lipcu 2020 roku nadzwyczajnego instrumentu odbudowy *Next Generation EU* oraz wieloletnich ram finansowych oznaczało przeznaczenie łącznie ponad 1,8 mld EUR na zniwelowanie społeczno-gospodarczych skutków pandemii COVID-19, w tym cyberataków, których liczba i siła wzrosła w okresie tzw. *lockdawnów*. Cel ten został połączony ze wcześniejszymi, „przedcovidowymi" założeniami cyfrowej transformacji UE oraz realizacją założeń europejskiego zielonego ładu.

3. Polityka cyberobrony Unii Europejskiej

Jak stwierdzono wyżej *Strategia bezpieczeństwa UE* z 2013 roku przyjęła kilka kierunków działania, w tym opracowanie polityki obronnej i rozbudowa zdolności bezpieczeństwa cybernetycznego w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony UE. Obszar ten wskazuje na unijne ambicje skierowane ku budowie zdolności obronnych, obejmujących działania zapobiegawcze, odstraszanie oraz zintegrowane reagowanie na incydenty w cyberprzestrzeni. W ramach działań z zakresu cyberobrony Unia zapowiedziała powołanie Wspólnej Jednostki Cyberbezpieczeństwa (*Joint Cyber Unit*), powierzając jej zadanie koordynowania

[29] Plan odbudowy dla Europy. https://ec.europa.eu/info/strategy/recovery-planeurope_en [05.11.2023].

współpracy między unijnymi a krajowymi organami i instytucjami odpowiedzialnymi za cyberbezpieczeństwo oraz wzmocnienie funkcjonowania tzw. *Diplomacy Toolbox* – unijnego zestawu narzędzi i metod cyberdyplomacji.

Unijna cyberobrona zostałaby skierowana na zapobieganie i reagowanie oraz rozwijanie nowoczesnych zdolności odpowiedzi na cyberataki (w ramach prac Europejskiej Agencji Obrony i możliwości Europejskiego Funduszu Obrony). Do pozostałych inicjatyw z zakresu cyberobronności, zapisanych w *Strategii*, należy zaliczyć m.in.: wzbogacenie europejskich ram zarządzania kryzysowego o dziedzinę cyberbezpieczeństwa, realizację programu walki z cyberprzestępczością, wzmocnienie Centrum Analiz Wywiadowczych UE poprzez zachęcenie państw członkowskich do wymiany danych i informacji, działania na rzecz wzmocnienia pozycji UE w celu efektywnej realizacji strategii zniechęcania, odstraszania i reagowania na cyberzagrożenia, przegląd ram unijnej polityki cyberbezpieczeństwa, stworzenie wspólnej strategii wojskowej w ramach cyberbezpieczeństwa, budowę powiązań między przemysłem cywilnym, obronnym i kosmicznym oraz umacnianie bezpieczeństwa infrastruktury krytycznej w przestrzeni kosmicznej[30]. Całości dopełnia, zapisana w unijnej *Strategii*, w postaci trzeciego obszaru działań i inicjatyw, konieczność zacieśnienia współpracy międzynarodowej na rzecz otwartej i bezpiecznej cyberprzestrzeni w zakresie promowania wartości, na których Unia powstała. Stąd postulaty współpracy m.in. z ONZ, Radą Europy oraz podmiotami trzecimi, dotyczące stosowania podstawowych wolności i praw człowieka w sieci, czy też ochrona dzieci przed wykorzystywaniem seksualnym i niegodziwym traktowaniem w cyberprzestrzeni.

We wrześniu 2017 roku Komisja Europejska wydała *Zalecenie ws. skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na*

[30] Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final. [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX: 52020JC0018. [dostęp: 06.11.2023].

dużą skalę[31]. Incydent cybernetyczny może zostać uznany za sytuację kryzysową na szczeblu Unii, jeżeli wywołane nim zakłócenia mają zbyt duży zakres, by państwo członkowskie, w którym doszło do tego incydentu, poradziło sobie z nim w pojedynkę, albo jeżeli dla dwóch lub większej liczby państw członkowskich ma on skutki o tak szerokim zakresie i o tak dużym znaczeniu technicznym lub politycznym, że wymaga on szybkiej koordynacji i reakcji na szczeblu politycznym Unii. Skuteczne reagowanie na szczeblu UE na incydenty i kryzysy cybernetyczne na dużą skalę wymaga szybkiej i skutecznej współpracy między wszystkimi odpowiednimi zainteresowanymi stronami, a podstawowym warunkiem skutecznej reakcji jest gotowość i zdolności poszczególnych państw członkowskich do podejmowania określonych działań, a także skoordynowane wspólne działanie wspierane zdolnościami na szczeblu unijnym. Odpowiedzialność za reagowanie na incydenty spoczywa w pierwszej kolejności na państwach. Natomiast na szczeblu UE do głównych podmiotów zaangażowanych w reagowanie na kryzysy cybernetyczne należą nowe struktury i mechanizmy ustanowione na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, a mianowicie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz stosowne agencje i jednostki organizacyjne, tj. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością w Europolu (Europol/EC3), Centrum Analiz Wywiadowczych UE (INTCEN), Dyrekcja ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT) oraz Centrum Sytuacyjne (SITROOM), działające wspólnie jako SIAC (pojedyncza komórka analiz wywiadowczych), a ponadto komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (działająca przy INTCEN), zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE (CERT-UE) oraz Centrum Koordynacji Reagowania Kryzysowego działające w Komisji Europejskiej.

---

[31] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę, Dz.Urz. UE, L 2017.239/36.

KE przypomniała, że ćwiczenia w dziedzinie bezpieczeństwa cybernetycznego na szczeblu UE są niezbędne do stymulowania i poprawy współpracy między państwami członkowskimi a sektorem prywatnym. W tym celu od 2010 r. ENISA organizuje regularnie ćwiczenia w zakresie incydentów cybernetycznych na skalę ogólnoeuropejską („Cyber Europe"). Ponadto, w ramach współpracy z NATO, KE przewiduje wzajemny udział pracowników w odpowiednich ćwiczeniach, w tym w szczególności ćwiczeniach „Cyber Coalition" i „Cyber Europe".

Komisja Europejska w zaleceniu 2021/1086 z dnia 23 czerwca 2021 r. zaproponowała utworzenia wspólnej jednostki ds. cyberprzestrzeni (Joint Cyber Unit)[32]. Pomimo znacznych postępów osiągniętych dzięki współpracy między państwami członkowskimi w dziedzinie cyberbezpieczeństwa, w szczególności w ramach grupy współpracy („grupa współpracy NIS") oraz sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), nadal nie istnieje wspólna platforma UE, na której można by skutecznie i bezpiecznie wymieniać informacje zgromadzone w różnych społecznościach zajmujących się cyberbezpieczeństwem oraz na której odpowiednie podmioty mogłyby koordynować i mobilizować zdolności operacyjne. Powstaje zatem ryzyko, że cyberzagrożenia i cyberincydenty będą zwalczane w ramach silosów o ograniczonej skuteczności i większej podatności. Ponadto brakuje unijnego kanału współpracy technicznej i operacyjnej z sektorem prywatnym, zarówno w zakresie wymiany informacji, jak i wsparcia reagowania na incydenty.

Wspólna jednostka ds. cyberprzestrzeni zapewniać powinna wirtualną i fizyczną platformę i nie wymaga utworzenia dodatkowego, samodzielnego organu. Jej ustanowienie nie powinno mieć wpływu na kompetencje i uprawnienia krajowych organów ds. cyberbezpieczeństwa i odpowiednich podmiotów unijnych. Wspólna jednostka do spraw cyberprzestrzeni powinna zostać umocowana na podstawie protokołów ustaleń między jej uczestnikami. Powinna ona opierać się na

[32] Zalecenie Komisji (UE) 2021/1086 z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni, Dz.Urz. UE, L.2021.237.1.

istniejących strukturach, zasobach i zdolnościach i wnosić w nie wkład jako platforma bezpiecznej i szybkiej współpracy operacyjnej i technicznej między podmiotami UE a organami państw członkowskich. Powinna ona również skupiać wszystkie społeczności zajmujące się cyberbezpieczeństwem, tj. społeczność cywilną, organy ścigania, dyplomację i obronę. Uczestnicy platformy powinni pełnić rolę operacyjną lub wspierającą. Uczestnikami operacyjnymi powinny być: ENISA, Europol, zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE), Komisja, Europejska Służba Działań Zewnętrznych (w tym INTCEN), sieć CSIRT i EU-CyC-LONe. Uczestnikami wspierającymi powinny być: Europejska Agencja Obrony (EDA), przewodniczący grupy współpracy NIS, przewodniczący Horyzontalnej Grupy Roboczej Rady ds. Cyberprzestrzeni oraz jeden przedstawiciel odpowiednich projektów PESCO. Organizowanie wspólnej jednostki miało zakończyć się do czerwca 2023 roku.

Wspólna polityka bezpieczeństwa i obrony (WPBiO) została opisana w Traktacie z Lizbony, czyli Traktacie o Unii Europejskiej (TUE), który wszedł w życie w 2009 roku. W czerwcu 2016 r. wiceprzewodnicząca/wysoka przedstawiciel Federica Mogherini przedstawiła Radzie Europejskiej *Globalną strategię UE w dziedzinie bezpieczeństwa i obrony*[33], która determinuje strategię WPBiO. Wyznaczono w niej pięć priorytetów:

1. Bezpieczeństwo naszej Unii;
2. Odporność państw i społeczeństw na wschodzie i południu UE;
3. Zintegrowane podejścia do konfliktów i kryzysów;
4. Ład regionalny oparte na współpracy;
5. Globalne współzarządzanie w XXI wieku.

Odnośnie do bezpieczeństwa Unii stwierdzono, że musi ona wziąć większą odpowiedzialność za swoje bezpieczeństwo i obronę. Większy wkład do europejskiego bezpieczeństwa wyrażać się powinien w pięciu

[33] Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy, June 2016, [online:] https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

rodzajach działań: bezpieczeństwo i obrona, antyterroryzm, cyberbezpieczeństwo, bezpieczeństwo energetyczne oraz komunikacja strategiczna (bezpieczeństwo informacyjne). W kwestii obrony kolektywnej to dla większości krajów główną instytucją pozostaje NATO. Jednocześnie UE musi pogłębiać swoją współpracę z NATO, z zachowaniem autonomii decyzyjnej obu organizacji. Co do pozostałych dziedzin to wszystkie pozostają istotne: w krótszej perspektywie najpilniejsze są działania antyterrorystyczne, w dłuższej – cyberbezpieczeństwo. Odnośnie do cyberbezpieczeństwa UE chce utrzymać otwartą, wolną i bezpieczną cyberprzestrzeń. Planuje pomagać państwom członkowskim w ochronie przed zagrożeniami cybernetycznymi. Wiąże się to ze wzmocnieniem zdolności technologicznych mających na celu łagodzenie zagrożeń i odporność krytycznej infrastruktury, sieci i usług oraz ograniczenie cyberprzestępczości. Oznacza to wspieranie innowacyjnych systemów technologii informacyjno-komunikacyjnych (ICT), które gwarantują dostępność i integralność danych, przy jednoczesnym zapewnieniu bezpieczeństwa w europejskiej przestrzeni cyfrowej poprzez odpowiednie polityki dotyczące lokalizacji przechowywania danych i certyfikacji produktów i usług cyfrowych. Wymaga to wplatania kwestii bezpieczeństwa cybernetycznego we wszystkie obszary polityki, wzmacniania elementów cybernetycznych w misjach i operacjach WPBiO oraz dalszego rozwijania platform współpracy. UE będzie wspierać polityczną, operacyjną i techniczną współpracę cybernetyczną między państwami członkowskimi, w szczególności w zakresie analizy i zarządzania skutkami, oraz wspierać wspólne oceny między strukturami UE a odpowiednimi instytucjami w państwach członkowskich. Wzmocni współpracę w zakresie cyberbezpieczeństwa z głównymi partnerami, takimi jak USA i NATO. Odpowiedź UE będzie również osadzona w silnych partnerstwach publiczno-prywatnych. Współpraca i wymiana informacji między państwami członkowskimi, instytucjami, sektorem prywatnym i społeczeństwem obywatelskim może sprzyjać tworzeniu wspólnej kultury cyberbezpieczeństwa i zwiększać gotowość na możliwe zakłócenia i ataki cybernetyczne.

W listopadzie 2016 r. Mogherini przedstawiła Radzie *Europejski plan działań w sektorze obrony*[34], mający na celu urzeczywistnienie wizji zawartej w *Globalnej strategii UE*. Plan zawiera 13 wniosków, w tym skoordynowany roczny przegląd w zakresie obronności (CARD) oraz nowe porozumienie w sprawie stałej współpracy strukturalnej (PESCO) dla państw członkowskich, które chcą pogłębiać współpracę w dziedzinie bezpieczeństwa i obrony.

W *Strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę* z 2020 roku podkreślono potrzebę przeglądu unijnych ram polityki cybernetycznej. Ponadto przewodnicząca Ursula von der Leyen wezwała do opracowania europejskiej polityki cyberobrony w swoim orędziu o stanie Unii w 2021 r. W czerwcu 2021 r. rozpoczęto zastanawiać się nad przyszłością europejskiej polityki bezpieczeństwa i obrony. Doprowadziło to do powstania *Strategicznego kompasu na rzecz bezpieczeństwa i obrony*, dokumentu politycznego, w którym zdefiniowano unijną strategię bezpieczeństwa i obrony na najbliższe 5-10 lat. *Strategiczny kompas* to ramy działania na rzecz wspólnej wizji w dziedzinie bezpieczeństwa i obrony. Dokument opracowano w trzech etapach: analiza zagrożeń, zorganizowany dialog strategiczny oraz dalszy rozwój i przegląd przed przyjęciem. Głównym celem jest zapewnienie wytycznych politycznych dotyczących osiągnięcia przez UE autonomii strategicznej w czterech istotnych obszarach: zarządzanie kryzysowe, odporność, potencjał i partnerstwa. Proces ten ma na celu zrealizowanie coraz pilniejszej wizji UE jako podmiotu, którzy posiada zdolność do zapewniania bezpieczeństwa. Wiceprzewodniczący i wysoki przedstawiciel Josep Borrell przedstawił wstępną wersję dokumentu na wspólnej sesji ministrów spraw zagranicznych i ministrów obrony UE w listopadzie 2021 roku. W kontekście rosyjskiej agresji na Ukrainę (rozpoczętej 24 lutego 2022 r.) dokument musiał ulec dużym zmianom, aby uwzględnić

[34] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejski plan działań w sektorze obrony, COM(2016) 950 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0950.

destabilizację europejskiego porządku bezpieczeństwa i dostosować stanowisko, ambicje i narzędzie UE w dziedzinie obrony do nowej sytuacji. W dniach 24-25 marca 2022 r. podczas francuskiej prezydencji Rada Europejska zatwierdziła ostateczną wersję *Strategicznego kompasu*.

10 listopada 2022 roku Komisja i Wysoki Przedstawiciel ds. zagranicznych i polityki bezpieczeństwa przedstawili wspólny komunikat *Polityka UE w zakresie cyberobrony*[35], aby zaradzić pogarszającemu się środowisku bezpieczeństwa w następstwie rosyjskiej agresji na Ukrainę oraz zwiększyć zdolność UE do ochrony swoich obywateli i infrastruktury.

W nowej *Polityce* stwierdzono, że w ostatnich latach nasiliły się szkodliwe zachowania w cyberprzestrzeni, których źródłem są zarówno podmioty państwowe, jak i niepaństwowe; rośnie liczba cyberataków wymierzonych w wojskową i cywilną infrastrukturę krytyczną w UE, a także w prowadzone aktualnie misje i operacje; zacierają się granice między cywilnym i wojskowym wymiarem cyberprzestrzeni. UE musi wziąć na siebie większą odpowiedzialność za własne bezpieczeństwo. W tym celu UE musi zapewnić sobie suwerenność technologiczną i cyfrową w cyberprzestrzeni.

Polityka UE w zakresie cyberobrony opiera się na czterech filarach obejmujących szeroki zakres inicjatyw, które pomogą UE i państwom członkowskim lepiej wykrywać cyberataki, powstrzymywać je i bronić się przed nimi:

1. Wspólne działania na rzecz silniejszej unijnej cyberobrony: UE wzmocni swoje mechanizmy koordynacyjne między krajowymi i unijnymi podmiotami zajmującymi się cyberobroną, aby zwiększyć wymianę informacji i współpracę między wojskowymi i cywilnymi społecznościami cyberbezpieczeństwa oraz dalej wspierać wojskowe misje i operacje w ramach WPBiO.

---

[35] Wspólny komunikat do Parlamentu Europejskiego i Rady – Polityka UE w zakresie cyberobrony, JOIN(2022) 49 final, [online:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022JC0049.

2. Zabezpieczenie ekosystemu obronnego UE: Nawet niekrytyczne komponenty oprogramowania mogą być wykorzystywane do przeprowadzania cyberataków na firmy lub rządy, w tym w sektorze obronnym. Wymaga to dalszych prac nad normalizacją i certyfikacją cyberbezpieczeństwa w celu zabezpieczenia zarówno domen wojskowych, jak i cywilnych.
3. Inwestowanie w zdolności cyberobronne: państwa członkowskie muszą znacznie zwiększyć inwestycje w nowoczesne zdolności w zakresie obrony cybernetycznej w sposób oparty na współpracy, wykorzystując platformy współpracy i mechanizmy finansowania dostępne na szczeblu UE, takie jak PESCO, Europejski Fundusz Obronny, a także program „Horyzont Europa" i program „Cyfrowa Europa".
4. Zawiązywanie partnerstw w celu przezwyciężania wspólnych wyzwań: opierając się na istniejącym bezpieczeństwie i obronności, a także dialogu cybernetycznym z krajami partnerskimi, UE będzie dążyć do ustanowienia dostosowanych partnerstw w dziedzinie cyberobrony. Nowa polityka wymaga inwestycji w zdolności cyberobrony o pełnym spektrum i wzmocni koordynację i współpracę między wojskowymi i cywilnymi społecznościami cybernetycznymi UE. Wzmocni on współpracę z sektorem prywatnym i skuteczne zarządzanie kryzysowe w cyberprzestrzeni w Unii. Nowa polityka pomoże również zmniejszyć nasze strategiczne zależności w zakresie krytycznych technologii cybernetycznych oraz wzmocnić europejską bazę technologiczno-przemysłową sektora obronnego (EDTIB). Będzie stymulować szkolenia, przyciąganie i zatrzymywanie talentów cybernetycznych.

Główny cel polityki – budowa wspólnych zdolności do odpierania cyberataków – miał zostać zrealizowany dzięki powołaniu nowych jednostek odpowiedzialnych za cyberobronę i włączeniu ich w istniejący cywilny system cyberbezpieczeństwa. Kluczową rolę w nowym systemie cyberobrony przypisano Centrum Koordynacji UE ds. Cyberobrony (EUCDCC), aby zapewnić świadomość sytuacyjną państwom członkowskim oraz misjom i operacjom zagranicznym UE. Przy wsparciu

Europejskiej Agencji Obrony (EDA) miały działać ponadto sieć dla wojskowych zespołów reagowania na incydenty komputerowe (MICNET) oraz unijna konferencja dowódców ds. obrony cyberprzestrzeni – platforma dyskusji na temat cyberincydentów w siłach zbrojnych. Podnoszeniu praktycznych zdolności do cyberobrony miał służyć projekt wspólnych ćwiczeń CyDef-X oraz rezerwa ds. cyberbezpieczeństwa działająca na bazie usług świadczonych przez dostawców prywatnych. W praktyce utworzenie tak wielu nowych jednostek i sprecyzowanie ich kompetencji okazało się trudne. W lutym 2023 roku EDA z opóźnieniem utworzyła zaproponowany w *Polityce cyberobrony* MICNET, a w jego skład weszło tylko 18 z 27 państw UE.

Pozostałe założenia polityki, które m.in. za pośrednictwem stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obronnego (EDF) mają przyczynić się do poprawy stanu europejskiego przemysłu, wymagają natomiast szybkiego przeprowadzenia strategicznej oceny nowych i przełomowych technologii z uwzględnieniem sektora cyfrowego. W *Polityce* nie zidentyfikowano pożądanych inwestycji dla państw członkowskich, tymczasem np. uniezależnienie od krytycznych cybertechnologii z państw trzecich i podniesienie atrakcyjności sektora cyberobrony dla wykwalifikowanych ekspertów, których brakuje na europejskim rynku, są niezbędne do wzmacniania międzynarodowej pozycji UE.

Wskazówki bibliograficzne

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2 /10.

Czachór Z., *Europejska Strategia Bezpieczeństwa 2003-2008. Analiza politologiczna*, „Przegląd Politologiczny" 2010, nr 2.

Gawkowski K., *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka Komisji Politologii i Stosunków Międzynarodowych" 2018, nr 13/2.

Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Business Law Journal" 2019, nr 3.
Kańczak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8.
Małecka A., *Polityka cyberbezpieczeństwa Unii Europejskiej na początku trzeciej dekady XXI wieku*, „Rocznik Bezpieczeństwa Międzynarodowego" 2021, nr 2/15.
Szczygieł M., *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 2/71.

Rozdział 4

Cyberbezpieczeństwo Rzeczypospolitej Polskiej

Cyberbezpieczeństwo RP jest zapewniane dwutorowo. W sferze cywilnej, Polska jako członek ONZ, Rady Europy oraz Unii Europejskiej, zobligowana jest do realizowania postanowień prawa międzynarodowego, którego przestrzegania dobrowolnie podjęła się. I tak zapisy *Konwencji Budapeszteńskiej* zostały wprowadzone na grunt polskiego prawa karnego już w 2004 roku. Podobnie postanowienia *Dyrektywy NIS* realizuje polska *Ustawa o krajowym systemie cyberbezpieczeństwa* z 28 sierpnia 2018 roku. Natomiast w sferze obronności (wojskowej i zarządzania kryzysowego) Polska zasadniczo opracowuje i wdraża własne koncepcje. W niniejszym rozdziale zostaną poddane analizie dokumenty o charakterze strategicznym w obu obszarach. W obszarze bezpieczeństwa narodowego przedstawiono dwie ostatnie strategie bezpieczeństwa i jedną doktrynę cyberbezpieczeństwa.

1. Krajowy system cyberbezpieczeństwa

Polityka Ochrony Cyberprzestrzeni RP[1] z 2013 roku to chronologicznie pierwszy wprowadzony w życie dokument o charakterze strategicznym w zakresie cyberbezpieczeństwa w Polsce. Jej celem strategicznym było

[1] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013; [archiwum online:] https://web.archive.org/web/20150707164127/ https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf [dostęp 10.01.2024].

osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa.

Dokument wyznaczył następujące cele szczegółowe:

1. Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa.
2. Zwiększenie zdolności do zapobiegania cyberzagrożeniom oraz ich zwalczania.
3. Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne.
4. Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.
5. Stworzenie spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.
6. Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz jej użytkownikami.
7. Zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

Polityka miała być realizowana przez działania według wskazanej listy priorytetowej:

1. Szacowanie ryzyka.
2. Bezpieczeństwo portali administracji rządowej.
3. Działania legislacyjne.
4. Działania proceduralno-organizacyjne.
5. Kształcenie, szkolenia i uświadamianie w dziedzinie bezpieczeństwa.
6. Działania techniczne.

Jednym z ważniejszych elementów było szacowanie ryzyka przez każdą jednostkę administracji rządowej, która miała co roku przekazywać sprawozdanie ministrowi właściwemu do spraw informatyzacji. Dodatkowo każda jednostka organizacyjna administracji rządowej miała ustanowić system zarządzania bezpieczeństwem informacji oraz

wyznaczyć pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni, którego zadaniem było:

1. Realizacja obowiązków, które wynikały z aktów prawnych zapewniających cyberbezpieczeństwo.
2. Opracowanie i wdrożenie procedur reagowania na incydenty komputerowe w organizacji.
3. Prowadzenie cyklicznych analiz ryzyka.
4. Przygotowanie planów awaryjnych oraz ich testowanie.
5. Opracowanie procedur zapewniających poinformowanie właściwych zespołów reagowania na incydenty komputerowe CERT (ang. *Computer Emergency Response Team*) o:

- wystąpieniu incydentów komputerowych;
- zmianie lokalizacji jednostki organizacyjnej lub danych kontaktowych.

Polityka ustanowiła także trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe:

- Poziom I: koordynacja – minister właściwy ds. informatyzacji.
- Poziom II: reagowanie na incydenty komputerowe:
  - Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL – realizujący jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację obsługi incydentów komputerowych w obszarze cyberprzestrzeni RP.
  - Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej.
- Poziom III: realizacja – administratorzy odpowiadający za poszczególne systemy teleinformatyczne w cyberprzestrzeni.

Dokument opracowało Ministerstwo Administracji i Cyfryzacji przy współpracy z Agencją Bezpieczeństwa Wewnętrznego. Polityka została przyjęta uchwałą Rady Ministrów 25 czerwca 2013 roku i obowiązywała tylko administrację rządową. Nie obejmowała również niejawnych systemów teleinformatycznych.

9 maja 2017 roku Prezes Rady Ministrów Beata Szydło podpisała uchwałę nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 roku

w sprawie ***Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022***. Dokument zastąpił *Politykę Ochrony Cyberprzestrzeni RP* z 2013 roku. *Krajowe Ramy* stanowią zbiór założeń, którymi kierował się rząd przy tworzeniu *Ustawy o krajowym systemie cyberbezpieczeństwa*. Ponieważ *Krajowe Ramy* przyjęte zostały jako uchwała Rady Ministrów, obowiązują tylko administrację rządową, podobnie do poprzedniej *Polityki*.

W dokumencie określono cztery cele, które wskazują na potrzeby wynikające z rozbudowy krajowego systemu cyberbezpieczeństwa:

1. Osiągnięcie zdolności do skoordynowanego działania w skali kraju, które pozwoli zapobiegać, wykrywać, zwalczać oraz minimalizować skutki incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.
2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.
3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa.

Głównym celem tej strategii jest zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych. *Krajowe Ramy* zostały ustanowione na pięć lat. Funkcję koordynatora ich wdrażania sprawuje minister właściwy do spraw informatyzacji.

22 października 2019 roku Rada Ministrów przyjęła uchwałę w sprawie ***Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024***[2]. Dokument obowiązuje od 31 października 2019 roku i zastępuje *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*. Przyjęcie *Strategii* wynika z *Ustawy o krajowym systemie cyberbezpieczeństwa* z 5 lipca 2018 roku (art. 68).

[2] M.P. 2019.1037.

Strategia jest bardzo podobna do *Krajowych Ram* z 2017 roku. O ile jednak *Ramy* stanowiły zbiór założeń, którymi kierował się rząd przy opracowywaniu *Ustawy o krajowym systemie cyberbezpieczeństwa*, o tyle po jej przyjęciu, wizja zakłada „systematyczne wzmacnianie i rozwój krajowego systemu cyberbezpieczeństwa". Głównym celem przyjęcia i wdrożenia *Strategii* jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

W *Strategii* zapisano pięć celów szczegółowych polityki rządu:

1. Rozwój krajowego systemu cyberbezpieczeństwa.
2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
3. Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W obrębie każdego celu szczegółowego wyznaczone zostały priorytety działania administracji. Odnośnie do celu drugiego zaplanowano opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa (NSC) oraz promowanie dobrych praktyk i zaleceń; bezpieczeństwo łańcucha dostaw; testy i audyty cyberbezpieczeństwa. Opracowanie NSC ma wpłynąć przede wszystkim na zwiększenie odporności systemów teleinformatycznych administracji publicznej. W tym aspekcie istotne jest także wdrożenie unijnego *Aktu o Cyberbezpieczeństwie*, wprowadzającego certyfikację produktów i usług ICT. W Polsce musi zostać utworzony krajowy system oceny i certyfikacji w zakresie cyberbezpieczeństwa (m.in. powołanie lub ustanowienie Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC), Krajowej jednostki akredytującej oraz jednostek oceniających zgodność).

Strategia jest uchwalona była na pięć lat, a koordynatorem jej wdrażania jest minister właściwy ds. informatyzacji.

Jak wskazano wyżej, *Strategia* wynika z ***Ustawy o krajowym systemie cyberbezpieczeństwa***[3], która jest pierwszym aktem prawnym w tym zakresie w Polsce. Jest to implementacja do porządku krajowego unijnej *Dyrektywy NIS*. Ponieważ *Dyrektywa NIS* jest harmonizacją minimalną, polski ustawodawca częściowo włączył w zakres ustawy również administrację publiczną oraz sektor telekomunikacyjny. Ustawa obowiązuje od 28 sierpnia 2018 roku.

Ustawa wprowadziła definicję operatorów usług kluczowych (firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej). Wskazuje sektory, w których identyfikowani są operatorzy usług kluczowych – sektor energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej. Dokładna lista usług kluczowych została zawarta w rozporządzeniu wykonawczym do ustawy.

Operatorzy usług kluczowych zobowiązani są wdrożyć system zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej. W ramach zarządzania wymagane jest systematyczne szacowanie ryzyka i dostosowanie do niego środków bezpieczeństwa, takich jak bezpieczna eksploatacja systemu, bezpieczeństwo fizyczne systemu (w tym kontrola dostępu), bezpieczeństwo i ciągłość dostaw usług, które mają wpływ na świadczenie usługi kluczowej, utrzymanie planów działania umożliwiających ciągłość świadczenia usługi, ciągłe monitorowanie systemu zapewniającego świadczenie usługi. Ponadto operator jest zobowiązany do stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, w tym zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatności systemu. Operator jest także odpowiedzialny za opracowanie dokumentacji dotyczącej

[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018.1560.

cyberbezpieczeństwa systemu informacyjnego, uaktualnianie jej i przechowywanie przez okres co najmniej 2 lat.

Z kolei do usług cyfrowych zaliczane są: internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Z zakresu ustawy zostały wyjęte małe i mikroprzedsiębiorstwa.

W skład krajowego systemu cyberbezpieczeństwa (oprócz wskazanych wyżej operatorów) wchodzą również podmioty publiczne takie jak: Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej (wraz z wojewódzkimi funduszami), a także instytuty badawcze i spółki prawa handlowego, wykonujące zadania o charakterze użyteczności publicznej. Każdy z powyższych podmiotów ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych. Dodatkowo na każdym z podmiotów publicznych spoczywa obowiązek zarządzania incydentem, w tym zapewnienia jego obsługi. Czas na zgłoszenie incydentu do właściwego CSIRT nie może przekroczyć 24 godzin od momentu wykrycia.

Dyrektywa NIS dała państwom członkowskim dowolność w zakresie liczby powołanych CSIRT. Polski ustawodawca wyznaczył trzy CSIRT-y poziomu krajowego:

- CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK;
- CSIRT GOV w strukturach Agencji Bezpieczeństwa Wewnętrznego;
- CSIRT MON w strukturach resortu obrony narodowej.

Każdy CSIRT ma jasno określony zakres podmiotów, które zobowiązane są mu raportować i którym świadczy on wsparcie. CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym. CSIRT GOV koordynuje incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank

Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej. Natomiast CSIRT NASK koordynuje incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych, dostawców usług cyfrowych i samorząd terytorialny, a także osoby fizyczne – zwykli obywatele. Dodatkowo w przypadku incydentów o charakterze terrorystycznym właściwe są CSIRT MON i CSIRT GOV. W przypadku incydentów związanych z obronnością kraju zawsze właściwy jest CSIRT MON.

Ustawa wskazuje „organ właściwy", czyli taki, który odpowiada „swój" sektor cyberbezpieczeństwa. Organami właściwymi są:

- Minister właściwy ds. energii i gospodarki wodnej – dla sektora energii i gospodarki wodnej,
- Minister właściwy ds. transportu – dla sektora transportu (włącznie z podsektorem transport wodny),
- Komisja Nadzoru Finansowego – dla sektora bankowego i infrastruktury rynków finansowych,
- Minister właściwy ds. zdrowia – dla sektora ochrony zdrowia,
- Minister właściwy ds. informatyzacji – dla sektora infrastruktury cyfrowej,
- Minister obrony narodowej – dla sektora zdrowia i infrastruktury cyfrowej w zakresie podmiotów podległych ministrowi obrony narodowej.

Ustawa powołuje także organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych i usług cyfrowych.

W grudniu 2022 roku Unia Europejska przyjęła *Dyrektywę NIS 2*, a czas na jej wdrożenie mija 17 października 2024 roku. W Polsce dopiero 23 kwietnia 2024 roku udostępniono projekt nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[4], która ma implementować do polskiego porządku prawnego dyrektywę. Do czasu złożenia do druku niniejszej publikacji ustawy nie uchwalono.

[4] https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055217#13055217.

2. Strategie obrony cyberprzestrzeni RP

Prezydent Bronisław Komorowski 5 listopada **2014** r. zatwierdził ***Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej***[5]**.** *Strategia* jest najważniejszym dokumentem dotyczącym bezpieczeństwa i obronności państwa. Opisuje interesy narodowe i definiuje główne cele RP w dziedzinie bezpieczeństwa. Zawarte są w niej również najważniejsze kierunki działań prowadzących do osiągania tych celów. *Strategia* w sposób całościowy ujmuje zagadnienia bezpieczeństwa narodowego oraz wskazuje optymalne sposoby wykorzystania na potrzeby bezpieczeństwa wszystkich zasobów pozostających w dyspozycji państwa w sferze obronnej, ochronnej, społecznej i gospodarczej. Za realizację jej postanowień odpowiadać będą ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, organy samorządu terytorialnego oraz inne podmioty, we właściwościach których pozostają sprawy z zakresu bezpieczeństwa państwa. Dokument z 2014 roku zastępuje poprzednią *Strategię* wydaną w 2007 r.

Rozdział I „Polska jako podmiot bezpieczeństwa" m.in. wskazuje pięć interesów narodowych w dziedzinie bezpieczeństwa i szesnaście odpowiadających im celów strategicznych. Jako cel jedenasty wskazano: zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni.

W kolejnej części opisane jest środowisko bezpieczeństwa Polski na różnych poziomach. W wymiarze globalnym (pkt 31) dostrzeżono zagrożenia cybernetyczne – „Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak **cyberprzestępczość**, **cyberterroryzm**, **cyberszpiegostwo**, **cyberkonflikty** z udziałem podmiotów niepaństwowych i **cyberwojna**, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym

[5] https://www.bbn.gov.pl/ftp/SBN%20RP.pdf [dostęp: 10.12.2023].

uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw [wyróżnienia w oryginale]". Z kolei na poziomie regionalnym *Strategia* zauważa, że „znaczenie bezpieczeństwa w cyberprzestrzeni będzie rosło, podobnie jak odpowiedzialność państw za jej ochronę i obronę". Istotne znaczenie dla zwiększenia poziomu bezpieczeństwa RP w cyberprzestrzeni ma polityka organizacji i struktur współpracy międzynarodowej (szczególnie UE i NATO). W wymiarze krajowym – „bezpieczne funkcjonowanie systemu teleinformatycznego RP jest warunkiem niezakłóconego działania całego państwa".

W dalszej części stwierdzono, że cyberprzestrzeń stała się kolejnym środowiskiem walki zbrojnej. Siły Zbrojne RP muszą dysponować zdolnościami defensywnymi i ofensywnymi w tej sferze, tak aby realizować funkcję odstraszania potencjalnego przeciwnika, w szczególności muszą być gotowe do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny (pkt 77). Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni RP, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Z powyższego wynika, że konieczne będzie rozwijanie w Siłach Zbrojnych RP zdolności do działań w cyberprzestrzeni, w tym stworzenie mechanizmów cyberobrony i wzmocnienie dedykowanych jej jednostek (pkt 117).

Doktryna cyberbezpieczeństwa RP [6] z 2015 roku została przygotowana w Biurze Bezpieczeństwa Narodowego w wyniku analiz prowadzonych z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. *Doktryna* jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do *Strategii Bezpieczeństwa Narodowego RP*. Określa ona cele w dziedzinie cyberbezpieczeństwa, opisuje środowisko, wskazując

[6] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 10.12.2023].

na zagrożenia, ryzyka i szanse, a także rekomenduje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa. Rekomendacje *Doktryny* przeznaczone są do odpowiedniego wykorzystania przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie cyberbezpieczeństwa.

W preambule napisano, że cyberprzestrzeń jest polem konfliktu, na którym przychodzi zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami (grupami ekstremistycznymi, terrorystycznymi, czy zorganizowanymi grupami przestępczymi). Dlatego jednym z istotnych priorytetów polskiej strategii stało się bezpieczeństwo tego nowego środowiska. Należy zauważyć, że żadne inne „pole konfliktu" nie doczekało się rozwinięcia w formie dedykowanej doktryny.

Strategia z 2014 r. posługuje się terminami „cyberprzestrzeń" i „cyberprzestrzeń RP" jednak ich nie definiuje. Definicje podaje *Doktryna*, w ślad za ustawami z 2011 r. (patrz Rozdział I):

- **cyberprzestrzeń** – przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami;
- **cyberprzestrzeń RP** – cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji);
- **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;

Strategicznym celem w obszarze cyberbezpieczeństwa RP jest zapewnienie bezpiecznego funkcjonowania RP w cyberprzestrzeni. Cel strategiczny ma być osiągnięty przez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Główne cele operacyjne to:

- ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans;
- zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans;
- obrona i ochrona własnych systemów i zgromadzonych w nich zasobów;
- zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne);
- po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

Do osiągnięcia powyższych celów operacyjnych potrzebne jest, w wymiarze preparacyjnym, zbudowanie, utrzymywanie i systematyczne doskonalenie zintegrowanego, zarządzanego ponadresortowo, systemu cyberbezpieczeństwa RP obejmującego podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa oraz podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji.

Główne ryzyka w obszarze cyberbezpieczeństwa RP wiążą się z lukami i słabościami istniejącymi w systemie cyberbezpieczeństwa, np. nieuregulowane lub niewłaściwie uregulowane relacje między poszczególnymi podmiotami w tym systemie czy luki prawne. Jednymi ze wskazywanych źródeł zagrożeń jest działalność grup terrorystycznych i ekstremistycznych w cyberprzestrzeni.

Aktualna ***Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*** został zatwierdzona 12 maja **2020 roku** przez prezydenta Andrzeja Dudę. Dokument zawiera podstawowe interesy i cele państwa polskiego w zakresie bezpieczeństwa narodowego. Koncepcja bezpieczeństwa prezentuje podejście do problematyki zagrożeń i obejmuje nie tylko zagrożenia czysto militarne. Jest zgodna z celami NATO oraz Unii Europejskiej, a także z Konstytucją RP. Poszczególnymi wymiarami dotyczącymi bezpieczeństwa narodowego są bezpieczeństwo zewnętrzne, militarne, wewnętrzne, obywatelskie, społeczne, ekonomiczne, ekologiczne, informacyjne i telekomunikacyjne.

Strategia z 2020 r., w odróżnieniu od dotychczasowych dokumentów, cyberprzestrzeń wiąże z przestrzenią informacyjną. Już w pierwszej części, opisującej środowisko bezpieczeństwa, jako główne źródło zagrożenia polskiego bezpieczeństwa wskazuje się Federację Rosyjską, która podejmuje działania za pomocą środków pozamilitarnych, takich jak cyberataki i dezinformacja. Podkreślono, że w kontekście rewolucji cyfrowej należy uwzględnić szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej, które mogą stanowić pole do dezinformacji i manipulacji informacją, co wymaga prowadzenia skutecznych działań z zakresu komunikacji strategicznej.

Strategia wskazuje cztery interesy narodowe, które tworzą filary bezpieczeństwa narodowego Polski. Filar I – bezpieczeństwo państwa i obywateli – obejmuje pięć obszarów strategicznych, w tym cyberbezpieczeństwo i przestrzeń informacyjną. Kwestie dotyczące cyberprzestrzeni znajdują są także w pozostałych obszarach, jednak główny ciężar skupia się w obszarze czwartym (cyberbezpieczeństwo). Celem strategicznym w tym obszarze jest podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze

publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Cel można osiągnąć poprzez następujące działania:

1. Zwiększanie poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnięcie zdolności do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia.
2. Wzmacnianie defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa.
3. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni.
4. Rozwijanie krajowych zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa.
5. Rozwijanie kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa.
6. Wzmacnianie i rozbudowywanie potencjału państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii.

Natomiast kolejny obszar (przestrzeń informacyjna) formułuje cel: zapewnienie bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej. W tym m.in. zbudowanie zdolności do ochrony przestrzeni informacyjnej, rozumianej jako przenikające się warstwy przestrzeni: wirtualnej (warstwa systemów, oprogramowania i aplikacji), fizycznej (infrastruktury i sprzętu) i poznawczej (kognitywnej).

Wskazówki bibliograficzne

Kuś B., *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne*, „Cybersecutity and Law" 2023, nr 10/2.

Oleksiewicz I., *Bezpieczeństwo informacyjne w cyberprzestrzeni dy stany nadzwyczajne Rzeczypospolitej Polskiej*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2019, nr 33.

Rzucidło J., Węgrzyn J., *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego" 2015, nr 5/27.

Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023.

Skrzypczak J., *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7/4.

Strzępek K., *Cyberbezpieczeństwo Rzeczypospolitej Polskiej – podstawy prawne (międzynarodowe i krajowe)*, „Prokuratura i Prawo" 2023, nr 12.

Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 14/27.

Zakończenie

Cyberprzestrzeń jest tworem bez granic. Zapewnienie bezpieczeństwa wszystkim użytkownikom cyberprzestrzeni jest wspólną powinnością państw i organizacji międzynarodowych. Podmioty te uznają cyberprzestrzeń za kolejny obszar działalności, w tym także politycznej, prawnej i gospodarczej.

W wyniku dokonanej analizy dokumentów strategicznych ONZ, Rady Europy, Unii Europejskiej i RP można stwierdzić, że na wszystkich poziomach władzy, zarządzania i współpracy międzynarodowej dostrzegalny jest problem cyberbezpieczeństwa. Co prawda nie ma zgodności odnośnie do definiowania terminów cyberprzestrzeń i cyberbezpieczeństwo, jednak nie można zaprzeczyć, że przestrzeń taka istnieje i że należy dbać bezpieczeństwo jej i użytkowników.

Współpraca międzynarodowa w kontekście bezpieczeństwa międzynarodowego nie jest prosta. ONZ skupia wiele państw, które mają często przeciwstawne interesy, nie tylko w dziedzinie cyberbezpieczeństwa. Analiza dokumentów ONZ nie napawa optymizmem – wieloletnie dyskusje na forum Organizacji skutkują co najwyżej niewiążącymi i ogólnymi rezolucjami. Być może nadzieją jest dyskutowana konwencja przeciwko cyberprzestępczości.

Także współpraca między organami UE a państwami członkowskimi nie należy do najłatwiejszych. Główną przeszkodą jest znaczna liczba systemów prawnych i różnorodnych inicjatyw podejmowanych w tym obszarze. Próbą zmiany tej sytuacji były dwie dyrektywy – NIS i NIS2. Ta ostatnia jest w Polsce na etapie implementowania.

Bibliografia

1. Źródła Organizacji Narodów Zjednoczonych

Combating the criminal misuse of information technologies: resolution, A/RES/55/63, https://digitallibrary.un.org/record/428861?v=pdf.

Combating the criminal misuse of information technologies: resolution, A/RES/56/121, https://digitallibrary.un.org/record/454952?v=pdf.

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures: resolution, A/RES/64/211, https://digitallibrary.un.org/record/673712?v=pdf.

Creation of a global culture of cybersecurity and the protection of critical information infrastructures: resolution, A/RES/58/199, https://digitallibrary.un.org/record/509571?v=pdf.

Creation of a global culture of cybersecurity: resolution, A/RES/57/239, https://digitallibrary.un.org/record/482184?v=pdf.

Developments in the field of information and telecommunications in the context of international security: resolution, A/RES/73/27, https://digitallibrary.un.org/record/1655670?v=pdf.

Developments in the field of information and telecommunications in the context of international security: resolution, A/RES/53/70, https://digitallibrary.un.org/record/265311?v=pdf.

Developments in the field of information and telecommunications in the context of international security: resolution A/RES/75/240, https://digitallibrary.un.org/record/3896458?v=pdf.

Developments in the field of information and telecommunications in the context of international security: note, A/75/816, https://digitallibrary.un.org/record/3908015?v=pdf.

Draft United Nations convention against cybercrime: strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, A/AC.291/L.15, https://digitallibrary.un.org/record/4066282?v=pdf.

Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders: resolution, A/RES/45/121, https://digitallibrary.un.org/record/105578?v=pdf.

Follow-up to the 11th United Nations Congress on Crime Prevention and Criminal Justice: resolution, A/RES/60/177, https://digitallibrary.un.org/record/563311?v=pdf.

Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society: resolution, A/RES/70/125, https://digitallibrary.un.org/record/819076?v=pdf.

Programme of action to advance responsible – State behaviour in the use of information and communications technologies in the context of international security: resolution, A/RES/77/37, https://digitallibrary.un.org/record/3997617?v=pdf.

Recommendation X.1205 (04/08), International Telecommunication Union, https://www.itu.int/rec/T-REC-X.1205-200804-I/en.

Revised draft text of the convention : note : Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Concluding session, New York, 29 January – 9 February 2024, A/AC.291/22/Rev.1, https://digitallibrary.un.org/record/4067171?v=pdf.

The right to privacy in the digital age: resolution, A/RES/77/211, https://digitallibrary.un.org/record/3999709?v=pdf.

Twelfth United Nations Congress on Crime Prevention and Criminal Justice: resolution, A/RES/65/230, https://digitallibrary.un.org/record/700722?v=pdf.

2. Źródła Rady Europy

Convention on cybercrime. Special edition dedicated to the drafters of the Convention (1997-2001), Council of Europe 2022, https://rm.coe.int/special-edition-budapest-convention-en-2022/ 1680a6992e.

Drugi protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego, Dz.Urz. UE, L 2023.63.28.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015.728.

Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzona w Lanzarote dnia 25 października 2007 r., Dz.U. 2015.608.

Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r., Dz.U. 2015.730.

Recommandation n° (95)13 du comité des ministres aux états membres relative aux problémes de procédure pénale liés à la technologie de l'information, https://search.coe.int/archives?i=0900001680910c9c.

Recommendation No. R(89)9 of committee of ministers to member states on computer-related crime, https://search.coe.int/archives?i=0900001680910c99.

3. Źródła Unii Europejskiej

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 2016.194.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz.Urz. UE, L 2022.333.

Europa 2020 Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu /* COM/2010/2020 końcowy */, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52010DC2020.

Europe and the Global Information Society: Recommendation to the European Council, Brussels, 26 May 1994 (Raport Bangemann), https://op.europa.eu/en/publication-detail/-/publication/31a0bebe-4bc6-4f31-a319-7b7799e45d86/language-en.

Green Paper on the convergence of the telecommunications, media and information technology sectors, and the implications for Regulation – Towards an information society approach, COM(97) 623 final,

https://op.europa.eu/en/publication-detail/-/publication/3967c098-852d-4774-af8b-691e70b40395/language-en.

Green Paper. Living and Working in Information Society. People First, COM(96) 389 Final, https://op.europa.eu/en/publication-detail/-/publication/8bcd9942-f9ef-4fe7-9637-936af5c0fd85/language-en.

Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century – White Paper, COM(93) 700, https://op.europa.eu/en/publication-detail/-/publication/4e6ecfb6-471e-4108-9c7d-90cb1c3096af/language-en.

Horizon Europe Strategic Plan (2021–2024). https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3c6ffd74-8ac3-11eb-b85c-01aa75ed71a1.

Implementation Strategy for Horizon Europe. https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_implementation-strategy_he.pdf.

Komunikat Komisji do Parlamentu Europejskiego i Rady, – Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji - zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, COM(2017)476 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0476.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Europejska agenda cyfrowa /* COM/2010/0245 końcowy */COM(2010) 245. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52010DC0245.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia jednolitego rynku cyfrowego dla Europy, COM(2015) 192 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52015DC0192.

Komunikat Komisji do Parlamentu Europeskiego, Rady Europejskiej, Rady, Europejskiego komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejski plan działań w sektorze obrony, COM(2016) 950 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0950.

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów: „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia"

{SEC(2005) 717} /COM/2005/0229 final/, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52005DC0229.

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy" {SEC(2006) 656} /*COM/2006/0251 final*/, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52006DC0251.

Lisbon European Council 23 and 24 March 2000 Presidency Conclusions, https://www.europarl.europa.eu/summits/lis1_en.htm.

Plan odbudowy dla Europy, https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

Public sector information: a key resource for Europe – Green Paper on public sector information in the information society, COM(1998) 585 Final, https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:51998DC0585.

Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierające zalecenia dla Komisji w sprawie aktu prawnego o usługach cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego w odniesieniu do podmiotów gospodarczych prowadzących działalność internetową (2020/2019(INL)), Dz.Urz. UE, C2021.404/31.

Rezolucja Rady z dnia 22 marca 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie, Dz.Urz. UE, C 2007.68/1.

Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz.Urz. UE, L 2004.077.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), Dz.Urz. UE, L 2022.277/1.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Dz.Urz. UE, L 2014.257.

Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług

cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ, Dz.Urz. UE, L 2018.26.48.

Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy, June 2016, https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

Stanowisko Rady w pierwszym czytaniu w sprawie przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" oraz uchylającego decyzję (UE) 2015/2240 – Przyjęte przez Radę w dniu 16 marca 2021 r. (nr 6789/1/20). https://data.consilium.europa.eu/doc/document/ST-6789-2020-REV-1/pl/pdf.

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 – Podejście ogólne, ST 14337 2021 INIT, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CONSIL%3AST_14337_2021_INIT

Wniosek Rozporządzenie Paramentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") COM/2017/0477 final/3 – 2017/0225(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017PC0477R(02).

Wniosek Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa, COM(2023) 208 final, 2023/0108(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52023PC0208.

Wspólny komunikat do Parlamentu Europejskiego i Rady – Polityka UE w zakresie cyberobrony, JOIN(2022) 49 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022JC0049.

Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX: 52020JC0018.

Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Społeczno-Ekonomicznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP)), https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex:52013JC0001.

Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń /*JOIN/2013/01 final */, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52013JC0001.

Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę, Dz.Urz. UE, L 2017.239/36.

Zalecenie Komisji (UE) 2021/1086 z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni, Dz.Urz. UE, L.2021.237.1.

4. Źródła Rzeczypospolitej Polskiej

Doktryna cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015; https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html.

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 września 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo telekomunikacyjne, Dz.U. 2017.1907.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, https://web.archive.org/web/20150707164127/https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055217#13055217.

Przedstawiony przez Prezydenta Rzeczypospolitej Polskiej projekt ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Druk nr 4355. Uzasadnienie, https://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/$file/4355-uzasadnienie.doc.

Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP – Informacja o wynikach kontroli P/14/043, Najwyższa Izba Kontroli: Warszawa 2015, https://www.nik.gov.pl/kontrole/P/14/043/

Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia, https://archiwum.mswia.gov.pl/pl/aktualnosci/6966,Zalozenia-do-Rzadowego-programu-ochrony-cyberprzestrzeni-RP-na-lata-2009-2011.html.

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Ministerstwo Spraw Wewnętrznych i Administracji: Warszawa czerwiec 2010, wersja 1.1.

Społeczeństwo informacyjne w Polsce w 2023 r., Główny Urząd Statystyczny, Urząd Statystyczny w Szczecinie, Warszawa-Szczecin 2023; https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2023-roku,1,17.html.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022; https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.

Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, M.P. 2019.1037.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005.64.565.

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, Dz.U. 2002.62.558, z późn. zm.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002.144.1204.

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002.113.985 z późn. zm.

Ustawa z dnia 21 lipca 2000 r. Prawo telekomunikacyjne, Dz.U. 2000.73.852.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002.156.1301 z późn. zm.

Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz.U. 2011.222.1323.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018.1560.

5. Opracowania

Brave New Words. The Oxford Dictionary of Science Fiction, [ed. by] J. Prucher, New York 2007, s. 31.

Cyberbezpieczeństwo. Zarys wykładu, [red. nauk.] C. Banasiński, Warszawa 2018, s. 23.

Gołąb P., *Traktat ONZ o cyberprzestępczości może stać się „globalnym paktem nadzoru" ostrzegają obrońcy praw człowieka*, ITReseller, 28.08.2023, https://itreseller.pl/traktat-onz-o-cyberprzestepczosci-moze-stac-sie-globalnym-paktem-nadzoru-ostrzegaja-obroncy-praw-czlowieka/

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 129-130.

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

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

Ławniczak K., *Konwencja ONZ przeciwko cyberprzestępczości w ogniu krytyki. Może zwiększyć inwigilację rządową*, ITHARDWARE.PL, 22.08.2024, https://ithardware.pl/aktualnosci/konwencja_onz_cyberprzestepczosc_krytyka_inwigilacja-34638.html.

Nora S., Minc A., *L'Informatisation de la société*, Paris 1978, https://www.vie-publique.fr/rapport/34772-linformatisation-de-la-societe.

Oleksiewicz I., *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka, strategia, prawo,* Warszawa 2021.

Ottis R., Lorents P., *Cyberspace: Definition and Implications*, [w:] *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April 2010*, Wright-Patterson AFB 2010.

Plumb C., *Understanding the UN's new international treaty to fight cybercrime,* UNU-CPR, 30.07.2024, https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

Podstawowe kategorie bezpieczeństwa narodowego, [red.] A. Żukowski, M. Hartliński, W.T. Modzelewski, J. Więcławski, Olsztyn 2015.

Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9.

Wyrębek H., *Cyberprzestrzeń. Zagrożenia, strategie bezpieczeństwa*, Siedlce 2021.

6. Strony internetowe

UNODA
https://disarmament.unoda.org/group-of-governmental-experts/
https://disarmament.unoda.org/open-ended-working-group/
https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.
IGF
https://www.intgovforum.org/en.
https://www.intgovforum.org/en/content/trust-security-and-stability.
ITU
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx.
https://www.itu.int/itu-d/sites/cybersecurity/
https://www.itu.int/net/wsis/
NASK
https://archiwum.nask.pl/pl/aktualnosci/4271,Internet-w-Polsce-ma-30-lat.html.
https://cyberpolicy.nask.pl/
NIST
https://csrc.nist.gov/glossary/term/cyberspace.