CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski, Władysław Hydzik
Dariusz Jagiełło, Zuzanna Krauzowicz, Filip Krzyżankiewicz, Arwid Mednis
Włodzimierz Nowak, Marcin Rojszczak, Adam Szafrański, Ryszard Szpyra
Kazimierz Waćkowski, Paweł Widawski, Joanna Worona-Vlugt, Zofia Zawadzka

SERIA AKADEMICKA

WYDANIE 2

Wolters Kluwer

CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski, Władysław Hydzik
Dariusz Jagiełło, Zuzanna Krauzowicz, Filip Krzyżankiewicz, Arwid Mednis
Włodzimierz Nowak, Marcin Rojszczak, Adam Szafrański, Ryszard Szpyra
Kazimierz Waćkowski, Paweł Widawski, Joanna Worona-Vlugt, Zofia Zawadzka

SERIA AKADEMICKA

WYDANIE 2

Wolters Kluwer

WARSZAWA 2023

Stan prawny na 14 sierpnia 2023 r.

Recenzentka 1. wydania
Prof. dr hab. Hanna Gronkiewicz-Waltz

Wydawczyni
Agata Jędrasik

Redaktorka prowadząca
Joanna Ołówek

Opracowanie redakcyjne
Violet Design

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Poszczególne rozdziały napisali:
Cezary Banasiński – rozdz. I
Cezary Banasiński, Włodzimierz Nowak – rozdz. III
Cezary Błaszczyk – rozdz. VII
Jacek M. Chmielewski, Kazimierz Waćkowski – rozdz. II
Władysław Hydzik – rozdz. IX
Dariusz Jagiełło – rozdz. XIV, XV
Filip Krzyżankiewicz, Arwid Mednis – rozdz. XII
Włodzimierz Nowak – rozdz. IV
Marcin Rojszczak – rozdz. V, VIII
Adam Szafrański – rozdz. XIII
Ryszard Szpyra – rozdz. VI
Zuzanna Krauzowicz, Paweł Widawski – rozdz. X
Joanna Worona-Vlugt, Zofia Zawadzka – rozdz. XI

ISBN 978-83-8328-821-5 *ISBN PDF-a: 978-83-8358-136-1*
2. wydanie

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

CZĘŚĆ V
CYBERPRZESTĘPCZOŚĆ

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 97/66/WE – dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z 15.12.1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (Dz.Urz. UE L 24 z 1998 r., s. 1) – nie obowiązuje

dyrektywa 2008/114/WE – dyrektywa Rady 2008/114/WE z 8.12.2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. UE L 345, s. 75)

dyrektywa 2009/140/WE – dyrektywa 2009/140/WE z 25.11.2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (Dz.Urz. UE L 337, s. 37, ze sprost.)

dyrektywa 2011/83/UE – dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.Urz. UE L 304, s. 64, ze zm.)

dyrektywa 2011/93/UE – dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13.12.2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335, s. 1, ze sprost.)

dyrektywa 2013/40/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12.08.2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8)

dyrektywa 2016/680 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)

dyrektywa 2017/541	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z 15.03.2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L 88, s. 6)
dyrektywa EECC	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36, ze zm.)
dyrektywa NIS	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
dyrektywa NIS 2	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 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 333, s. 80)
dyrektywa o e-prywatności	– dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37, ze zm.)
dyrektywa o handlu elektronicznym	– dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178, s. 1, ze zm.).
dyrektywa o ochronie danych	– dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281, s. 31, ze zm.) – nie obowiązuje
dyrektywa PSD	– dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z 13.11.2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniającej dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającej dyrektywę 97/5/WE (Dz.Urz. UE L 319, s. 1, ze zm.) – nie obowiązuje
dyrektywa PSD2	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35, ze zm.)
dyrektywa ramowa	– dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.Urz. UE L 108, s. 33, ze zm.) – nie obowiązuje
k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2022 r. poz. 1138 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)

k.p.c.	– ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2023 r. poz. 1550 ze zm.)
k.p.k.	– ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2022 r. poz. 1375 ze zm.)
KPP	– Karta Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
k.s.h.	– ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2022 r. poz. 1467 ze zm.)
k.w.	– ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2022 r. poz. 2151 ze zm.)
pr. aut.	– ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509 ze zm.)
pr. kon.	– ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. z 2020 r. poz. 287 ze zm.)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 ze zm.)
p.w.p.	– ustawa z 30.06.2000 r. – Prawo własności przemysłowej (Dz.U. z 2023 r. poz. 1170)
RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)
rozporządzenie 2015/2120	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z 25.11.2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu i dotyczące opłat detalicznych za regulowane usługi łączności wewnątrzunijnej oraz zmieniające dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012 (Dz.Urz. UE L 310, s. 1, ze zm.)
rozporządzenie 2019/881	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15)
rozporządzenie DORA	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.Urz. UE L 333, s. 1)
rozporządzenie eIDAS	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 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 257, s. 73, ze zm.)
rozporządzenie dotyczące silnego uwierzytelnienia i bezpiecznej komunikacji	– rozporządzenie delegowane Komisji (UE) 2018/389 z 27.11.2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Dz.Urz. UE L 69 z 2018 r., s. 23, ze zm.)

TUE – Traktat o Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 13)
u.k.s.cyb. – ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913 ze zm.)
u.o.b.d. – ustawa z 27.07.2001 r. o ochronie baz danych (Dz.U. z 2021 r. poz. 386)
u.o.d.o. – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.ś.u.d.e. – ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.u.p. – ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2022 r. poz. 2360 ze zm.)
u.u.z.i.e. – ustawa z 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797 ze zm.)
u.z.k. – ustawa z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122)
u.z.n.k. – ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233)

Czasopisma

MoP – Monitor Prawniczy
OSA – Orzecznictwo Sądów Apelacyjnych
OSAWr – Orzecznictwo Sądu Apelacyjnego we Wrocławiu
OSG – Orzecznictwo Sądów Gospodarczych
OSNC – Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSN(K) – Zbiór Orzeczeń Sądu Najwyższego
OSNKW – Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNP – Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OSNwSK – Orzecznictwo Sądu Najwyższego w Sprawach Karnych
OTK-A – Orzecznictwo Trybunału Konstytucyjnego. Seria A
PPH – Przegląd Prawa Handlowego
Prok. i Pr. – Prokuratura i Prawo
PS – Przegląd Sądowy
ZNUJ PPWI – Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej
ZNUJ PWiOWI – Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej

Inne

ABW – Agencja Bezpieczeństwa Wewnętrznego
APT – złożony permanentny atak (ang. *advanced persistent threat*)
BHP – bezpieczeństwo i higiena pracy
CEN – Europejski Komitet Normalizacyjny
CENELEC – Europejski Komitet Normalizacyjny Elektrotechniki

COBIT – zbiór wskazówek i dobrych praktyk dotyczących zarządzania procesami IT w organizacji (ang. *Control Objectives for Information and related Technology*)
DNS – system nazw domenowych (ang. *domainname system*)
EBC – Europejski Bank Centralny
ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ang. *European Network and Information Security Agency*)
EOG – Europejski Obszar Gospodarczy
ETPC – Europejski Trybunał Praw Człowieka
ETSI – Europejski Instytut Norm Telekomunikacyjnych
EUN – Europejskie Urzędy Nadzoru
EUNB – Europejski Urząd Nadzoru Bankowego (ang. *European Banking Authority*)
GIODO – Generalny Inspektor Ochrony Danych Osobowych
HL7 – standard cyfrowej wymiany informacji w środowiskach medycznych (ang. *Health Level Seven*)
ICT – technologie informacyjne i komunikacyjne (ang. *information and communication technologies*)
IGF – Forum Zarządzania Internetem (ang. *Internet Governance Forum*)
IHE – *Integrating the Healthcare Enterprise*
ISACA – Information Systems Audit and Control Association
ISO – Międzynarodowa Organizacja Normalizacyjna (ang. *International Organization for Standardization*)
IT – technologia informacyjna (ang. *information technology*)
ITIL – wytyczne dotyczące najlepszych praktyk w zakresie zarządzania usługami IT (ang. *Information Technology Infrastructure Library*)
ITU – Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union*)
KNF – Komisja Nadzoru Finansowego
MŚP – małe i średnie przedsiębiorstwa
NASK – Naukowa i Akademicka Sieć Komputerowa
NATO – Organizacja Traktatu Północnoatlantyckiego (ang. *North Atlantic Treaty Organization*)
NIST – Narodowy Instytut Norm i Techniki (ang. *National Institute of Standards and Technology*)
ONZ – Organizacja Narodów Zjednoczonych
OTT – usługa świadczona ponad siecią (ang. *Over-the-Top*)
resp. – odnośnie, względnie (ang. *respective*)
RP – Rzeczpospolita Polska
SA – sąd apelacyjny
SCA – silne uwierzytelnianie klienta (ang. *strong customer authentication*)
SN – Sąd Najwyższy
SOA – koncepcja architektury zorientowanej na usługi (ang. *service-oriented architecture*)
SR – sąd rejonowy
SZBI – system zarządzania bezpieczeństwem informacji
TPP – podmioty trzecie (ang. *Third Party Providers*)

TSUE – Trybunał Sprawiedliwości Unii Europejskiej
UE – Unia Europejska
UKE – Urząd Komunikacji Elektronicznej
UODO – Urząd Ochrony Danych Osobowych (obecnie: Prezes UODO)
UOKIK – Urząd Ochrony Konkurencji i Konsumentów
WPBiO – wspólna polityka bezpieczeństwa i obrony
WSA – wojewódzki sąd administracyjny
WSIS – Światowy Szczyt Społeczeństwa Informacyjnego (ang. *The World Summit on the Information Society*)
ZO ONZ – Zgromadzenie ogólne Organizacji Narodów Zjednoczonych

WSTĘP

Postępująca informatyzacja niemal wszystkich dziedzin współczesnego życia niesie za sobą nie tylko korzyści, lecz także zagrożenia, wzmacniane przy tym przez niezwykłą wręcz dynamikę i nieprzewidywalność rozwoju technologicznego ostatnich lat. Stąd też zainteresowanie tematyką zagrożeń w cyberprzestrzeni i ochrony przed nimi przestało być domeną wąskiej grupy specjalistów, stając się niebudzącym wątpliwości istotnym problemem współczesnego świata. Pytanie, na ile możliwość ziszczenia się ponurych wizji „cybernetycznego Pearl Harbor" jest realna, pozostaje w sposób oczywisty bez odpowiedzi. Niemniej zagwarantowanie bezpieczeństwa w cyberprzestrzeni jest wyjątkowo aktualnym wyzwaniem praktycznie dla każdego użytkownika systemów teleinformatycznych.

Mając świadomość powyższych wyzwań, autorzy przedstawili nie tylko najnowsze podstawy prawne szeroko rozumianego cyberbezpieczeństwa i zasadnicze instytucje, ale także najnowsze zagrożenia i odpowiadające im rozwiązania techniczne oraz prawne, chroniące wszystkie podmioty korzystające z systemów informatycznych. Podręcznik skierowany jest do osób, których przedmiotem zainteresowania jest problematyka cyberbezpieczeństwa, i to zarówno z zakresu nauk ścisłych, jak i nauk humanistycznych. Zagadnienie cyberbezpieczeństwa ma bowiem charakter interdyscyplinarny, podobnie jak nauki o bezpieczeństwie, których integralnym i niezwykle istotnym współcześnie fragmentem jest właśnie bezpieczeństwo w cyberprzestrzeni. Problem cyberbezpieczeństwa dotyczy przy tym różnych dziedzin aktywności ludzkiej. Podmiotami cyberbezpieczeństwa są przedsiębiorcy, państwa, organizacje międzynarodowe, wirtualne społeczności internetowe czy wreszcie poszczególni użytkownicy sieci. Dlatego każdy zainteresowany obszarem bezpieczeństwa sieci oraz systemów informatycznych Czytelnik tej książki – pomimo że formalnie jest ona podręcznikiem akademickim – znajdzie w niej zapewne coś interesującego dla siebie. Publikacja zawiera bowiem niezbędne informacje techniczne, prawne, organizacyjne dotyczące bezpieczeństwa systemów operacyjnych, sieci komputerowych oraz telekomunikacyjnych i zarazem bezpieczeństwa gromadzonych, przetwarzanych i wysyłanych danych. Zakres treściowy opracowania wychodzi naprzeciw także potrzebom praktyków uczestniczących w procesach zachowania bezpieczeństwa informatycznego, których zadaniem jest monitorowanie, detekcja oraz analiza ryzyk i zagrożeń dla sprawnego funkcjonowania systemów informatycznych.

W książce – będącej jak każdy podręcznik kompromisem między wymogiem zwięzłości wykładu a potrzebą jego wszechstronności – skupiono się na najważniejszych kwestiach z zakresu bezpieczeństwa w cyberprzestrzeni.

Część pierwsza jest wprowadzeniem do problematyki cyberbezpieczeństwa. Omówione zostały podstawy prawne bezpieczeństwa w cyberprzestrzeni. Przedstawiono również zasadnicze dylematy terminologiczne związane z prezentowaną w książce tematyką. Przybliżono kwestie technologii teleinformatycznych, ich rozwoju oraz bezpieczeństwa, zwłaszcza w kontekście zarządzania usługami IT, przeanalizowano rodzaje ataków sieciowych, w tym ataków ukierunkowanych, a także odniesiono się do problemu zapór sieciowych czy czynników wpływających na podatność infrastruktury na cyberataki. Część tę uzupełnia analiza podatności zastosowanych mechanizmów cyberbezpieczeństwa na zagrożenia wynikające z możliwości komputerów kwantowych, wykorzystania kryptografii kwantowej i postkwantowej, jak również łączności kwantowej.

Część druga odnosi się do cyberbezpieczeństwa z perspektywy państwa. Omówione zostały ustrojowe (organizacyjne) podstawy europejskiego i krajowego systemu cyberbezpieczeństwa. Przedstawiono także zasadnicze zasady ochrony infrastruktury krytycznej służące zapewnieniu sprawnego funkcjonowania administracji publicznej, instytucji i przedsiębiorców z punktu widzenia zagrożeń i ryzyk wykorzystywania tej infrastruktury; z uwagi na złożoność problemu kwestię tę ujęto z punktu widzenia norm technicznych oraz od strony nauk o zarządzaniu. Odniesiono się również do sektora łączności elektronicznej, którego znaczenie jest bezprecedensowe z perspektywy omawianej w podręczniku tematyki. Dopełnieniem tej części opracowania jest ukazanie problemu w płaszczyźnie militarnej, gdzie analiza podstawowych elementów cyberbezpieczeństwa skorelowana została ze współczesnymi militarnymi koncepcjami prowadzenia operacji wojskowych w cyberprzestrzeni.

Część trzecia jest analizą cyberbezpieczeństwa z punktu widzenia przedsiębiorcy. Przybliżone zostały zagadnienia cywilnoprawnego obrotu gospodarczego w cyberprzestrzeni. Odniesiono się także do modeli wdrażania cyberbezpieczeństwa przez przedsiębiorców, jak np. warstwowego modelu bezpieczeństwa informacyjnego, modeli zarządzania bezpieczeństwem IT według norm ISO/IEC oraz innych koncepcji, w tym m.in. opartych na zaleceniach i wytycznych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa. Kwestie te istotnie uzupełnia problematyka zarządzania ryzykiem przez przedsiębiorcę. Omówiono również zagadnienia cyberbezpieczeństwa w najbardziej wrażliwym z punktu widzenia przedmiotu opracowania sektorze gospodarki, a mianowicie sektorze bankowym. Tę część zamyka analiza cyberbezpieczeństwa od strony prawa własności intelektualnej.

Część czwarta dotyczy bezpieczeństwa obywateli w cyberprzestrzeni. Zwrócono tu uwagę, z jednej strony, na fundamentalną dla każdego obywatela ochronę prywatności i danych osobowych, z drugiej zaś – na wyjątkowo newralgiczną społecznie ochronę dzieci i młodzieży w cyberprzestrzeni przed szkodliwymi dla ich rozwoju treściami.

W części ostatniej, poświęconej cyberprzestępczości, przybliżono karnoprawne ramy odpowiedzialności za przestępstwa popełniane w cyberprzestrzeni, uzupełniając regulacje materialnoprawne także problematyką karnoprocesową i śledczą.

Idea podręcznika do cyberbezpieczeństwa powstała w ramach Pracowni Nowych Technologii Zakładu Prawa Administracyjnego Gospodarczego i Bankowego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego na potrzeby wykładu specjalizacyjnego. Stąd też książka została podzielona na pięć bloków tematycznych podporządkowanych 30-godzinnemu semestralnemu wykładowi akademickiemu, a zatem 15 półtoragodzinnym standardowym wykładom. Zagadnienia prezentowane w podręczniku uzupełnia obszerna bibliografia oraz liczne odniesienia do materiałów źródłowych dające Czytelnikowi szansę pogłębienia zagadnień zawartych w publikacji.

Przygotowując podręcznik, autorzy dążyli nie tylko do przekazania niezbędnej wiedzy teoretycznej, lecz także koniecznych informacji praktycznych, co przy wykładaniu problematyki cyberbezpieczeństwa jest warunkiem jej efektywnego nauczania. Proporcje w tym zakresie zostały podporządkowane treści poszczególnych obszarów tematycznych. Mając świadomość, że opracowanie siłą rzeczy nie obejmuje wszystkich zagadnień tej niezwykle szerokiej tematyki, jaką jest cyberbezpieczeństwo, autorzy będą wdzięczni za wszelkie uwagi dotyczące zawartości oddawanej do rąk Czytelników książki.

Autorzy

Część I

WPROWADZENIE DO PROBLEMATYKI CYBERBEZPIECZEŃSTWA

Rozdział I

PODSTAWOWE POJĘCIA I PODSTAWY PRAWNE BEZPIECZEŃSTWA W CYBERPRZESTRZENI

1. Pojęcia cyberbezpieczeństwa i cyberprzestrzeni

1.1. Wprowadzenie

Pojęcia cyberbezpieczeństwa i cyberprzestrzeni nieodłącznie wiążą się z ewolucją dostępu do informacji wskutek rewolucji informatycznej ostatnich lat; oba zjawiska są ze sobą ściśle związane.

W literaturze brak jest powszechnie akceptowanego pojęcia informacji; w pewnym sensie jest to termin złożony, interdyscyplinarny, definiowany odmiennie w różnych naukach, niemający jednoznacznej, powszechnej definicji. Często nie definiuje się w rozważaniach dotyczących informacji samego pojęcia informacji, „zadowalając się jego znaczeniem potocznym jako komunikatu – wiadomości, wyrażonych w dowolny sposób”[1].

Z punktu widzenia cybernetyki oraz teorii informacji[2] termin ten definiowany jest jako „zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne”[3]. W ujęciu tym informacja jest pojęciem ściśle związanym z człowiekiem i zdolnością jego celowego działania[4]. Ale już w ujęciu szerszym,

[1] T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 4.

[2] Szerzej o informacji J. Petzel, *Informatyka prawnicza. Zagadnienia teorii i praktyki*, Warszawa 1999, s. 35 i n.

[3] P. Sienkiewicz, *10 wykładów*, Warszawa 2005, s. 62, cyt. za M. Kłodawski, *Pojęcie informacji w naukach teoretycznoprawnych*, s. 5, https://depot.ceon.pl/bitstream/handle/123456789/316/Maciej_Klodawski_-_Pojecie_informacji_w_naukach_teoretycznoprawnych.pdf (dostęp: 1.07.2023 r.).

[4] L. Ciborowski cyt. za R. Kwećka, *Informacja w walce zbrojnej*, Warszawa 2001, s. 17.

pozwalającym połączyć podejście jakościowe do informacji z ilościowym ujęciem matematycznym (ITI), informacja to każdy czynnik, który ludzie, inne organizmy żywe, ale również i urządzenia automatyczne mogą spożytkować do celowego działania. Tak też traktuje informację – na potrzeby jej przetwarzania – Polska Norma PN-ISO/IEC 2382-1:1996-01.01.02, która utożsamia informację z wiedzą dotyczącą obiektów, takich jak: fakty, zdarzenia, przedmioty, procesy lub idee, zawierającą koncepcję, która w określonym kontekście ma określone znaczenie; pozwala to odróżnić informację od terminu „dane", który w tej samej normie traktowany jest jako „reprezentacja informacji mająca interpretację, właściwą do komunikowania się, interpretacji lub przetwarzania"[5].

Niezależnie jednak od różnych prób definiowania pojęcia informacji można przyjąć generalnie, że informacja jest przenaszalnym dobrem niematerialnym zmniejszającym niepewność[6]. Informacja zawarta w komunikacie umożliwia przy tym podjęcie określonej reakcji na treści w niej zawarte.

Istotny jest jednak nie tyle spór definicyjny o istotę tego pojęcia[7], ile fakt, że rozwój technologii informacyjnych i komunikacyjnych (ICT, ang. *information and communication technologies*[8]) i ich współczesna powszechność[9] spowodował natomiast wyjątkową łatwość (swobodę) dystrybucji, dostępu i wymiany informacji. Ta będąca wynikiem rewolucji informatycznej dostępność informacji stworzyła podstawę dla integracji wiedzy, technologii, gospodarki i kultury[10], ewoluując w efekcie w kierunku społeczeństwa informacyjnego z jego informacyjną, nierzadko globalną, gospodarką, pozbawionego organizacyjnych czy administracyjnych granic terytorialnych[11]. Informacja stała się zasadniczym dobrem ekonomicznym, warunkując rozwój społeczny, ale także niosąc dla tego rozwoju istotne zagrożenia społeczne, gospodarcze czy kulturowe. Najczęściej wyróżnianymi formami zagrożeń teleinformatycznych są: hacking, haktywizm, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, wykorzystanie cyberprzestrzeni

[5] Szeroko D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 25 i n.

[6] G. Szpor, *Bezpieczeństwo danych osobowych a ochrona informacji niejawnych i biznesowych* [w:] *Ochrona informacji niejawnych i biznesowych*, red. M. Gajos, S. Zalewski, Katowice 2005, s. 34.

[7] Szeroko M.J. Schroeder, *Spór o pojęcie informacji*, „Studia Metodologiczne" 2015/34, s. 11.

[8] Przez pojęcie to należy rozumieć grupę technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej. Węższym pojęciem są technologie informatyczne (IT), które odnoszą się do technologii związanych z komputerami i oprogramowaniem, niezwiązanych jednak z technologiami komunikacyjnymi i dotyczącymi sieci. Rozwój tych technologii sprawia, że oba pojęcia stają się coraz bardziej zbliżone treściowo.

[9] M. Leszczyńska, *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej* [w:] *Społeczeństwo informacyjne – regionalne aspekty rozwoju*, red. M. Woźniak, „Nierówności społeczne a wzrost gospodarczy" 2011/23, s. 129.

[10] M. Niezgoda, *Społeczeństwo informacyjne w perspektywie socjologicznej: idea czy rzeczywistość?* [w:] *Społeczeństwo informacyjne – wizja czy rzeczywistość*, t. I, red. L. Haber, Kraków 2003, s. 122 i n.

[11] Szeroko T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Kraków 1999, s. 78.

jako piątego teatru działań zbrojnych[12] czy wreszcie skutki niekontrolowanego użycia internetu w sferze społecznej i psychicznej[13].

1.2. Pojęcie cyberprzestrzeni

Pojęcie cyberprzestrzeni należy do kategorii pojęć niedookreślonych. Od strony semantycznej cyberprzestrzeń jest hybrydą pojęciową będącą skrótem od sformułowania ang. *cybernetics space*, czyli przestrzeni cybernetycznej.

Termin „cyberprzestrzeń" został wykreowany na potrzeby literatury science fiction i spopularyzowany przez Williama Gibsona, który określił cyberprzestrzeń jako niewyobrażalną złożoność będącą niczym „konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach (…)"[14]. To literackie określenie cyberprzestrzeni z trudnością poddaje się naukowemu zdefiniowaniu, które odpowiadałoby wymogom teorii zastosowania reguł semiotycznych i praw logiki formalnej do działalności naukowej, czyli ogólnej metodologii nauk. Stąd też pojęcie cyberprzestrzeni traktowane jest czasami jako nic nie znaczące hasło, całkowicie nieprzydatne w badaniach naukowych, co dotyczy zwłaszcza nauk technicznych, czasem jako dość ogólne sformułowanie odnoszące się do środowiska społecznego komunikującego się przy pomocy technik stosowanych z użyciem komputera (cybertechnologie), czy też jako zjawisko, którego skutki występowania są analizowane w ramach stosowania cybernetyki społecznej do komunikacji komputerowej (cyberkomunikacji)[15]. Nie jest nawet jasny źródłosłów pojęcia cyberprzestrzeni; jedynie ogólnie można stwierdzić, że jest to zbitka słowna (hybryda) dwóch słów – *kybernets*, co w języku greckim oznacza sternik, zarządca, kontrolować, oraz *space*, czyli – w dosłownym tłumaczeniu z języka angielskiego – przestrzeń. Niejednoznaczne są zwłaszcza związki pojęcia cyberprzestrzeni z cybernetyką, z której bez wątpienia zapożyczono pojęcie cyberprzestrzeni w literaturze science fiction. Związki te są krytykowane w literaturze[16], aczkolwiek z drugiej strony zwraca się również uwagę, że z punktu widzenia etymologicznego pojęcie cyberprzestrzeni wywodzi się z cybernetyki[17], ukształtowanej przez Norberta Wienera, jako nauki o sterowaniu

[12] Szeroko *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.

[13] Szeroko *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, red. D. Morańska, Dąbrowa Górnicza 2015.

[14] Za J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013/9, s. 226.

[15] Zob. m.in. J. Janowski, *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, Warszawa 2012; J. Janowski, *Globalna cyberkultura polityki i prawa*, s. 311 i n., http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf (dostęp: 1.07.2023 r.).

[16] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 60 i n.

[17] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 74.

i komunikowaniu w systemach o różnej naturze[18], czyli wywieraniu pożądanego wpływu na określone zjawiska[19].

Odkrywając analogie między zasadami działania żywych organizmów, układów społecznych, ale i maszyn, cybernetyka ma wskazywać wspólne reguły dla różnych nauk, umożliwiając tym samym przenoszenie tych praw z jednej dziedziny na drugą. Współcześnie cybernetykę traktuje się wyjątkowo szeroko, jako naukę ogólną i abstrakcyjną, skierowaną na modelowanie zachowań systemów, ze szczególnym uwzględnieniem systemów, które można określić mianem inteligentnych[20]. Cybernetyka teoretyczna bada przy tym ogólne zasady działania systemów bez odwoływania się do konkretnych obiektów fizycznych. Zasadniczą funkcją cybernetyki jest jej zastosowanie w systemach opartych na zamkniętych zwrotnych relacjach przyczynowo-skutkowych (sprzężeniu zwrotnym), tzn. systemach, gdzie określone działanie systemu kształtuje zmiany w jego środowisku, te zaś zwrotnie oddziałują na ten system. Poszukiwanie w efekcie związków między cybernetyką a cyberprzestrzenią nie jest pozbawione racjonalności[21], aczkolwiek w literaturze podnosi się także odrębność zakresów treściowych cybernetyki i informatyki, jak również podważa możliwość wyodrębnienia z technicznego punktu widzenia przestrzeni cybernetycznej (czy nawet informatycznej)[22].

Brak jest również powszechnie akceptowanej definicji cyberprzestrzeni. Próby definicji tego pojęcia mają mniej lub bardziej ogólny charakter. W ujęciu szerokim, i zarazem abstrakcyjnym, cyberprzestrzeń to globalna infrastruktura informacyjna, wzajemna łączność między ludźmi za pomocą komputerów i telekomunikacji, przestrzeń komunikacyjna tworzona przez system powiązań internetowych ułatwiająca użytkownikowi sieci kontakty w czasie rzeczywistym i obejmująca wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych[23] czy też „wszechogarniająca świat domena informacyjna, gdzie nośnikiem danych jest spektrum elektromagnetyczne”[24], a także „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie”[25]. Tego rodzaju ujęcie zwraca uwagę na podstawowe elementy środo-

[18] P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni*, „Automatyka” 2009/2(13), s. 584.

[19] Szeroko M. Mazur, *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966, s. 11 i n.

[20] T. Marzec, *Co może dać nauce prawa cybernetyka, a czego dać nie może?*, „Studia Iuridica Toruniensia” 2015/17, s. 126.

[21] Tak m.in. P. Sienkiewicz, *Analiza systemowa zagrożeń dla bezpieczeństwa…*, s. 584–585.

[22] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji…*, s. 48–49.

[23] Zob. szeroki wybór poglądów literatury M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji…*, s. 76 i n.

[24] J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, https://www.researchgate.net/profile/Jerzy_Deren2/publication/272818724_NATO_a_aspekty_bezpieczenstwa_w_cyberprzestrzeni/links/56b48d5b08ae8cf9c25b67c0/NATO-a-aspekty-bezpieczenstwa-w-cyberprzestrzeni.pdf (dostęp: 1.07.2023 r.).

[25] P. Levy, *Drugi potop* [w:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, red. M. Hopfinger, Warszawa 2002, s. 380.

wiska cyberprzestrzeni, którymi są: „rozległość (zasięg światowy), spajanie wszelkich zasobów w jedną, olbrzymią bazę danych, złożoność oraz bezprzestrzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata”[26]; inaczej mówiąc, cyberprzestrzeń ma charakter „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny”[27].

Pojęcie „wirtualny” odnosi się najczęściej do sztucznego obrazu rzeczywistości wykreowanego przez urządzenia informatyczne przy pomocy programów graficznych. Ale nie tylko – wirtualność cyberprzestrzeni pozwala bowiem także na wykreowanie wspólnot (grup osób) odgrywających określone role, podobnie jak w świecie rzeczywistym, tzw. cyberrole tworzące swoiste cyberwięzi; tego rodzaju wirtualne wspólnoty są aterytorialne, niepowiązane ani czasowo, ani też fizycznie[28]. Wirtualność jest w istocie swoistym abstrakcyjnym złudzeniem obecności w równie abstrakcyjnym świecie umożliwiającym jednocześnie zachowania interakcyjne.

Cyberprzestrzeń oparta jest na elementach technicznych i technologicznych oraz społecznych[29].

Podstawowym czynnikiem tworzącym cyberprzestrzeń jest materialny system teleinformatyczny, będący zespołem 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 telekomunikacyjnego urządzenia końcowego; siecią telekomunikacyjną w rozumieniu ustawy – Prawo telekomunikacyjne są zaś 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. Oznacza to, że cyberprzestrzeni nie da się utożsamić z internetem, traktowanym jako „globalny system wymiany danych funkcjonujący w oparciu o wzajemnie połączone sieci lokalne, rozmieszczone w wielu fizycznych lokalizacjach, umożliwiający jednoczesną wielopłaszyznową interakcję użytkowników z całego świata”[30].

Cyberprzestrzeń obejmuje w równym stopniu internet, sieci telekomunikacyjne czy systemy komputerowe, a zatem wszystkie systemy IT włączone w sieć globalną. Otwarte jest natomiast pytanie, czy pojęcie to obejmuje także systemy IT funkcjonujące

[26] J. Wasilewski, *Zarys definicyjny…*, s. 226.

[27] P. Levy, *Drugi potop*, s. 380.

[28] Szerzej K. Kawecka, D. Wójcik, *Patologie w cyberprzestrzeni – analiza przypadku grupy pomocowej utworzonej w jednym z portali społecznościowych* [w:] *Patologie w cyberprzestrzeni…*, s. 155 i n.

[29] K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 21.

[30] J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57.

w odizolowanej przestrzeni wirtualnej, w tym wszystkie komputery offline. Doktryna raczej skłania się do włączenia również i tej kategorii urządzeń IT do cyberprzestrzeni z uwagi na fakt, że „komputery które nie są podłączone do sieci mają możliwość komunikowania z innymi urządzeniami bądź ich sieciami, każdy z nich może mieć kontakt z resztą cyberprzestrzeni mimo tego, że stanowi z jej perspektywy ośrodek izolowany"[31].

Do kontekstu narzędziowego, technicznego cyberprzestrzeni nawiązuje normatywna definicja tego pojęcia zawarta w polskim ustawodawstwie[32], która cyberprzestrzeń traktuje jako przestrzeń przetwarzania i wymiany informacji, tworzoną przez systemy teleinformatyczne, czyli zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniających 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[33] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Definicję tę powiela też Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[34], jak i Doktryna cyberbezpieczeństwa RP, gdzie wyodrębniono ponadto, przyjmując kryterium terytorialne, cyberprzestrzeń RP, rozumianą jako „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)"[35]. Konstrukcja cyberprzestrzeni RP jest zaprzeczeniem znanej i powszechnie akceptowanej tezy o braku możliwości odniesienia cyberprzestrzeni do fizycznych, a zwłaszcza geograficznych, wymiarów realnego świata[36].

Skupiając się przede wszystkim na kontekście narzędziowym, tego rodzaju definicje pomijają lub też marginalizują komponent społeczny cyberprzestrzeni, który odnosi się do użytkowników cyberprzestrzeni, a który traktuje cyberprzestrzeń jako złożone środowisko będące rezultatem niemających materialnej formy interakcji pomiędzy

[31] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji…*, s. 83–84.

[32] Art. 2 ust. 1a ustawy z 21.06.2002 r. o stanie wyjątkowym (Dz.U. z 2017 r. poz. 1928); art. 2 ust. 1b ustawy z 29.08.2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2022 r. poz. 2091); art. 3 ust. 1 pkt 4 ustawy z 18.04.2002 r. o stanie klęski żywiołowej (Dz.U. z 2017 r. poz. 1897).

[33] W rozumieniu ustawy – Prawo telekomunikacyjne.

[34] Uchwała nr 125 Rady Ministrów z 22.10.2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. poz. 1037) – w myśl której cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 ze zm.), wraz z powiązaniami między nimi oraz relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy z 29.08.2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.

[35] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 r., http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 1.07.2023 r.).

[36] J. Wasilewski, *Zarys definicyjny…*, s. 226.

ludźmi, oprogramowaniem i usługami w internecie realizowanymi poprzez urządzenia techniczne i sieci do niego podłączone; równie ważnym, integralnym i wewnętrznie sprzężonym elementem z infrastrukturą techniczną jest jej relacja z ludźmi oraz interakcje między ludźmi związane z jej wykorzystaniem[37]. Pojęcie interakcji społecznych jest kategorią społeczną i pojęciem socjologicznym, oznaczającym pewną sekwencję wzajemnie zorientowanych działań jednostek społecznych kształtujących swoje działania w zależności od zachowań innych podmiotów funkcjonujących w wirtualnym świecie[38]. W tym kontekście o wiele bardziej trafna jest definicja Centrum Doskonalenia Cyberobrony NATO (ang. *NATO Cooperative Cyber Defence Centre of Excellence*, CCDCOE), według której cyberprzestrzeń jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami"[39].

W konsekwencji przyjmuje się w literaturze, że cyberprzestrzeń to wirtualne środowisko mniej lub bardziej otwartego komunikowania się za pośrednictwem połączonych systemów komputerowych oraz powiązań informatycznych i informacyjnych[40].

1.3. Pojęcie cyberbezpieczeństwa

Jeszcze większe problemy definicyjne sprawia pojęcie cyberbezpieczeństwa, czy też bezpieczeństwa w cyberprzestrzeni, co jest efektem blankietowości samego pojęcia bezpieczeństwa, które nabiera różnej treści w zależności od jego kwantyfikatora i jego podmiotów. Jako pojęcie normatywne bezpieczeństwo jest typową klauzulą generalną, uzasadniającą określone działania państwa podejmowane w interesie publicznym. Pojęcie bezpieczeństwa jest przy tym kategorią dynamiczną, zmienną, wymagającą stałego redefiniowania i o otwartym zakresie przedmiotowym.

Termin „bezpieczeństwo" wywodzi się z języka łacińskiego (*sine cura*), oznacza stan bez troski, pieczy, opieki, ochrony[41], znajduje odzwierciedlenie w wyrażeniu *sine cura vivere*, czyli żyć bez troski; słowo „bezpieczny" jest w efekcie dosłownym tłumaczeniem łacińskiego wyrazu *secura*; termin ten przekształcił się następnie w sformułowanie *securitas*, czyli bezpieczeństwo. Stąd też od strony leksykalnej termin „bezpieczeństwo" oznacza stan, w którym nie istnieje żadne zagrożenie[42]. W słowniku nauk społecznych

[37] J. Rzucidło, J. Węgrzyn, *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni*, „Przegląd Prawa Konstytucyjnego" 2015/5/27, s. 142.

[38] P. Sztompka, *Socjologia. Analiza społeczeństwa*, Kraków 2002, s. 51.

[39] Cyt. za M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012/22/II, s. 129–130.

[40] C. Marcinkowski, *Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka* [w:] *Patologie w cyberprzestrzeni…*, s. 114.

[41] W. Kopaliński, *Słownik języka polskiego*, t. 1, Warszawa 1983, s. 14.

[42] *Słownik języka polskiego*, t. 1, Warszawa 2007, s. 196.

stwierdza się, że bezpieczeństwo jest „właściwie identyczne z pewnością (ang. *safety*) i oznacza brak zagrożenia (ang. *danger*) fizycznego albo ochronę przed nim"[43]. Również w literaturze przedmiotu przyznaje się, że „istotą (…) bezpieczeństwa jest pewność"[44].

O ile brak jest powszechnie akceptowanej definicji bezpieczeństwa, to panuje natomiast powszechna zgoda co do społecznego wymiaru bezpieczeństwa i jego związku z człowiekiem oraz jego świadomością[45]. Bezpieczeństwo to „stan świadomości człowieka, w którym czuje się on wolny od jakichkolwiek zagrożeń, generowanych zarówno w bliższym, jak i w dalszym otoczeniu, to stan bez lęku i niepokoju o siebie i innych, pociągający za sobą uczucie wewnętrznego spokoju, psychicznego komfortu, pewności jutra"[46]. Bezpieczeństwo jest zatem pewną wartością, traktowaną w naukach społecznych jako kategoria odnosząca się do takich potrzeb, jak: istnienie, przetrwanie, całość, tożsamość, niezależność, spokój, posiadanie i pewność rozwoju; dotyczy przy tym zarówno pojedynczych jednostek ludzkich, grup społecznych, jak i państw, ich zrzeszeń czy całych systemów międzynarodowych[47]. Bezpieczeństwo jest w efekcie potrzebą podmiotową i egzystencjalną, związaną z istnieniem danego podmiotu. Społeczny wymiar bezpieczeństwa tworzy podstawę dla koncepcji podmiotowych bezpieczeństwa i subiektywnego jego ujęcia. Oznacza to, że bezpieczeństwo ma wymiar zarówno obiektywny, jako pewien realny, rzeczywisty stan braku zagrożenia, jak i subiektywny, odnoszący się do indywidualnie pojmowanego poczucia istnienia bezpieczeństwa.

Tak rozumiane bezpieczeństwo, będąc w pewnym sensie kategorią ontologiczną, traktowane jest w literaturze społecznej jako „możliwość zaspokojenia potrzeb o charakterze egzystencjalnym, jak i możliwość zaspokojenia istnienia, przetrwania i rozwoju. Bezpieczeństwo jest też stanem pewności, co do wymienionych powyżej możliwości"[48]. Definicja ta akcentuje dwie strony pojmowania bezpieczeństwa – negatywną, jako przeciwieństwo zagrożenia, czyli swoistą wolność od jakichkolwiek zagrożeń i pewność przetrwania (bezpieczeństwo egzystencjalne), oraz pozytywną – wykraczającą poza tradycyjne bezpieczeństwo egzystencjonalne i traktowaną jako wolność do rozwoju podmiotu bezpieczeństwa, ochrony jego interesów i możliwości przeciwstawienia się współczesnym wyzwaniom i zagrożeniom[49]. Do społecznych koncepcji bezpieczeństwa

[43] D. Lerner, *A Dictionary of the Social Sciences*, Londyn 1964, s. 629, cyt. za R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004, s. 27.

[44] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 20.

[45] L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków 2008, s. 52.

[46] J. Ziarko, *Dylematy metodologiczne bezpieczeństwa jako nauki* [w:] *Bezpieczeństwo. Wymiar współczesny i perspektywy badań*, red. R. Kwieciński, Kraków 2010, s. 61–62.

[47] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 1999, s. 27.

[48] R. Rosicki, *O pojęciu i istocie bezpieczeństwa*, „Przegląd Politologiczny" 2010/3, s. 24.

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

nawiązuje też (Mini)Słownik Biura Bezpieczeństwa Narodowego[50], według którego bezpieczeństwo to „teoria i praktyka zapewniania możliwości przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyk oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów. Współczesne bezpieczeństwo ma charakter zintegrowany (kompleksowy, wielowymiarowy), w którym – w zależności od przyjętego kryterium – można wyróżnić różne jego rodzaje, dziedziny, sektory, działy i obszary (…). Z istoty bezpieczeństwa zintegrowanego wynika także występowanie transsektorowych/transdziałowych obszarów bezpieczeństwa, jak np. cyberbezpieczeństwo".

Bezpieczeństwo można analizować od strony podmiotowej, przedmiotowej i procesualnej[51], a także terytorialnej. Z punktu widzenia podmiotowego zakres adresatów bezpieczeństwa jest właściwie nieograniczony; mogą to być poszczególne jednostki, ale również inne podmioty prawa, jak np. osoby prawne, ukształtowane według dowolnych kryteriów grupy społeczne, społeczności narodowe i międzynarodowe (regionalne czy globalne); podmiotem bezpieczeństwa jest zatem każdy podmiot mający własne interesy i zainteresowany pewnością ich realizacji. Z punktu widzenia przedmiotowego bezpieczeństwo jest wielokierunkowe i uwarunkowane zakresem interesów jego podmiotu, co sprawia, że od strony przedmiotowej jest otwarte; jego zakres jest pochodną aktywności danego podmiotu. Przykładowo w sferze bezpieczeństwa narodowego wyróżnia się bezpieczeństwo ideologiczne, publiczne, powszechne, polityczne, militarne, kulturowe, społeczne, ekologiczne i ekonomiczne[52]; można wyodrębnić także bezpieczeństwo żywnościowe, sanitarne, energetyczne, socjalne czy prawne.

Ujęcie procesowe wreszcie odzwierciedla dynamiczny charakter bezpieczeństwa i traktowane jest jako ta dziedzina aktywności jakiegoś podmiotu, której treścią jest „(…) zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów"[53]. Do ujęcia procesowego (funkcjonalnego) nawiązuje też definicja bezpieczeństwa, w myśl której pojęcie to oznacza generalnie „pewność istnienia i przetrwania, posiadania oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (ich niewystępowania lub wyeliminowania),

[50] https://koziej.pl/wp-content/uploads/2015/09/MiniS%C5%82ownik-BBN.docx (dostęp: 1.07.2023 r.).

[51] J. Kukułka, *Narodziny nowych koncepcji bezpieczeństwa* [w:] *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, red. J. Kukułka, Warszawa 1994, s. 40–41, za R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego…*, 1999, s. 30.

[52] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 41.

[53] S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011/18/2, s. 20.

ale także powstaje wskutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego"[54]. Ujęcie to pozwala na wychwycenie dynamiki i ewolucji subiektywnych i obiektywnych aspektów bezpieczeństwa i jego uczestników. Motorem jego przebiegu jest ocena zagrożeń, stanowiących podstawę formułowania strategii (polityki) w tym zakresie[55].

Trudności w zdefiniowaniu bezpieczeństwa przekładają się na możliwość jednoznacznego określenia bezpieczeństwa w cyberprzestrzeni (cyberbezpieczeństwa). Występują w tym wypadku dwa pojęcia niedookreślone – bezpieczeństwa i cyberprzestrzeni. W literaturze podnosi się wręcz, że skoro wątpliwe jest wyodrębnienie – z technicznego punktu widzenia – samej przestrzeni cybernetycznej, to trudno mówić o potrzebie bezpieczeństwa i możliwościach ochrony takiego hipotetycznego tworu[56]. Niemniej w literaturze, podobnie jak w aktach prawnych oraz oficjalnych dokumentach, podejmowane są próby zdefiniowania tego pojęcia.

Przykładowo definicja bezpieczeństwa cybernetycznego zaproponowana przez National Initiative for Cybersecurity Careers and Studies (NICCS) – będącą organizacją zarządzaną przez Wydział Edukacji i Świadomości Cyberbezpieczeństwa (usytuowany w Departamencie Bezpieczeństwa Wewnętrznego Urzędu Cyberbezpieczeństwa i Komunikacji Rządu Federalnego USA) – określana jest jako sytuacja gwarantująca, że „(…) systemy informacyjne lub komunikacyjne oraz informacja zawarta w nich są zabezpieczone czy chronione przed uszkodzeniem, nieautoryzowanym użyciem, modyfikacją bądź wykorzystaniem"[57]. Ta sama instytucja zaproponowała też szeroką definicję cyberbezpieczeństwa, jako „strategię, politykę i normy dotyczące zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej – elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej"[58].

Z kolei Międzynarodowy Związek Telekomunikacyjny w Rekomendacji ITU-T X.1205 definiuje cyberbezpieczeństwo jako „zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i technologii, które mogą być wykorzystywane do ochrony środowiska cybernetycznego oraz organizacja i zasoby użytkownika. Organizacja i zasoby

[54] R. Zięba [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, red. R. Zięba, Warszawa 2008, s. 16.
[55] R. Olszewski, *Bezpieczeństwo współczesnego świata*, Toruń 2005, s. 9.
[56] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji…*, s. 49.
[57] Za Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016/2(10), s. 108.
[58] Z. Chmielewski, *Polityka publiczna w zakresie…*, s. 108.

użytkownika obejmują podłączone urządzenia komputerowe, personel, infrastrukturę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przekazanych i/lub przechowywanych informacji w środowisku cybernetycznym. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i zasobów użytkownika względem odpowiednich zagrożeń bezpieczeństwa w środowisku cybernetycznym". Ogólne cele bezpieczeństwa obejmują dostępność, integralność (która może obejmować uwierzytelnianie i niezaprzeczalność) oraz poufność. W istocie zalecenie to zawiera taksonomię zagrożeń bezpieczeństwa z punktu widzenia organizacji.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 utożsamia pojęcie cyberbezpieczeństwa z bezpieczeństwem systemów informacyjnych oraz przetwarzanych w nich informacji, łącząc to pojęcie z bezpieczeństwem teleinformatycznym. Podejście to nawiązuje do postanowień normy międzynarodowej ISO/IEC 27032, w której definiuje się bezpieczeństwo w cyberprzestrzeni jako zachowanie poufności, dostępności i integralności, aczkolwiek zaznacza się, że możliwe jest uwzględnienie również innych właściwości bezpieczeństwa informacji, takich jak: „autentyczność, rozliczalność, niezaprzeczalność i niezawodność w cyberprzestrzeni". Norma ISO/IEC 27032, zawierając zbiór rekomendacji przeznaczonych dla dostawców usług internetowych, siłą rzeczy nie odnosi się natomiast do ochrony cybernetycznej (*cybersafety*), czyli zapobiegania skutkom negatywnych zdarzeń, które mogą wystąpić w efekcie korzystania z technik informacyjnych. Zdecydowanie szerzej podchodzi do tej kwestii ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa[59], która, wykorzystując normę ISO/IEC 27032, definiuje pojęcie cyberbezpieczeństwa jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Jeszcze inaczej podchodzi do tego zagadnienia Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 r., która wyodrębnia cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni), traktując je jako 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, a także bezpieczeństwo cyberprzestrzeni RP, rozumiane z kolei jako 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.

[59] Dz.U. z 2023 r. poz. 913.

Trudności ze zdefiniowaniem pojęcia bezpieczeństwa, a tym bardziej bezpieczeństwa w cyberprzestrzeni (cyberbezpieczeństwa), zwłaszcza ze względu na wielość cech bezpieczeństwa sprawia, że jego „granice są rozmyte, nieostre i nie oddają dogłębnej, znaczeniowej strony tego zjawiska”[60]. Stąd też w literaturze zwraca się uwagę, że ogólne definicje bezpieczeństwa być może wypełni kategoria „zagrożenie”[61], gdyż „desygnatami zakreślającymi zawartość pojęcia «bezpieczeństwo» jest zbiór przeciwieństw «zagrożenia»”[62].

Problem jednak w tym, że dla nauk społecznych pojęcie zagrożenia, podobnie jak bezpieczeństwa, jest kategorią subiektywną, stanem świadomości, wynikającym z oceny (wartościowania) określonych faktów jako niekorzystne przez podmiot zagrożenia[63]; nie jest to zatem stan obiektywny. Z uwagi na specyfikę zjawiska percepcja zagrożeń może być znikoma, z trudnością poddająca się ewaluacji bądź wręcz znajdować się poza świadomością podmiotu oceniającego, chociażby z uwagi na fakt, że zagrożenia w cyberprzestrzeni są otwarte i trudno identyfikowalne. Sprawia to, że pojęcie zagrożenia nie musi być lepszym wyznacznikiem granic pojęcia bezpieczeństwa niż najbardziej nawet ogólne jego definicje.

Trudności definicyjne sprawiają, że niektóre dokumenty odnoszące się do cyberbezpieczeństwa unikają definiowania tego pojęcia, wskazując mniej lub bardziej jego cel i przedmiot ochrony. Podejście takie wydaje się prezentować Strategia bezpieczeństwa cybernetycznego Unii Europejskiej „Otwarta, bezpieczna i chroniona cyberprzestrzeń”[64], w myśl której, cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami; celem zaś ochrony cyberprzestrzeni powinno być: zapewnienie dostępu i otwartości, poszanowania i ochrony praw podstawowych w internecie oraz utrzymanie niezawodności i interoperacyjności internetu. W istocie zasadniczym założeniem tak pojętej ochrony jest zastosowanie w środowisku internetowym tych samych norm, zasad i wartości, które UE wspiera w świecie rzeczywistym, co dotyczy ochrony praw podstawowych, gwarancji demokracji i praworządności.

Podobne ujęcie zaprezentowano także w Systemie bezpieczeństwa cyberprzestrzeni RP[65], gdzie pojęcie cyberbezpieczeństwa odniesiono do zabezpieczeń i działań, jakie mogą być wykorzystywane do ochrony systemów komputerowych, sieci, aplikacji

[60] J. Ziarko, *Dylematy metodologiczne bezpieczeństwa…*, s. 63.

[61] M. Szuniewicz, *Ochrona bezpieczeństwa państwa jako przesłanka ograniczenia praw i wolności jednostki w świetle Europejskiej Konwencji Praw Człowieka*, Warszawa 2016, s. 6.

[62] M. Leszczyński, *Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku*, Warszawa 2011, s. 19.

[63] M. Szuniewicz, *Ochrona bezpieczeństwa państwa…*, s. 7.

[64] Wspólny komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, JOIN (2013) 1 final, s. 2, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52013JC0001 (dostęp: 1.07.2023 r.).

[65] Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji, Warszawa 2015, s. 3, https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf (dostęp: 1.07.2023 r.).

i użytkowników przed zagrożeniami bezpieczeństwa teleinformatycznego. Identyczną definicję zawiera rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[66], gdzie bezpieczeństwo cybernetyczne obejmuje wszystkie działania niezbędne do ochrony przed zagrożeniami cybernetycznymi sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą.

Niezależnie od różnic, a zwłaszcza mniej lub bardziej narzędziowego podejścia do pojęcia cyberbezpieczeństwa, wydaje się, że można sprowadzić to pojęcie do sposobu wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetwarzanych w sposób cyfrowy[67]. Pozwala to odróżnić cyberbezpieczeństwo od bezpieczeństwa informacyjnego traktowanego jako możliwość pozyskania jakościowo dobrej informacji przez jakiś podmiot oraz ochrony posiadanej informacji przed jej utratą, niezależnie od sposobu jej gromadzenia, przesyłania i przetwarzania[68] lub też w ujęciu szerokim „(…) uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji"[69].

2. Cyberbezpieczeństwo jako przedmiot badań

Przywołane powyżej próby zdefiniowania bezpieczeństwa w cyberprzestrzeni wyraźnie uświadamiają trudności z dookreśleniem pojęć cyberprzestrzeni i cyberbezpieczeństwa. Jest to o tyle zrozumiałe, że już samo pojęcie bezpieczeństwa jest pojęciem blankietowym, którego treść jest zmienna, poddana ewolucji stosownie do zmian stosunków społecznych. W literaturze stwierdza się wprost, że „trwająca już od dawna redefinicja bezpieczeństwa nabiera cech permanentności", co wyraża się stałym poszerzaniem zakresu podmiotowego, przedmiotowego i procesowego tego pojęcia[70]. Klasyczne rozumienie bezpieczeństwa, odwołujące się do ochrony terytorium przy pomocy potencjału obronnego, współcześnie musi uwzględniać także gospodarkę, środowisko ekologiczne i społeczne czy właśnie nowe technologie[71]; ten ostatni element sprawia zaś, że bezpieczeństwo w cyberprzestrzeni staje się zasadniczym elementem definicji bezpieczeństwa

[66] Dz.Urz. UE L 151, s. 15–69.

[67] C. Marcinkowski, *Cyberprzestrzeń a istota…*, s. 115. Podobnie *Bezpieczeństwo teleinformatyczne…*, red. M. Madej, M. Terlikowski, s. 10 i n.

[68] L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 147; K. Liderman, *Bezpieczeństwo…*, s. 22. Zob. także J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 18 i n.

[69] K. Liderman, *Bezpieczeństwo…*, s. 22.

[70] J. Stańczyk, *Istota współczesnego pojmowania bezpieczeństwa – zasadnicze tendencje*, „Rocznik Bezpieczeństwa Międzynarodowego" 2011/5, s. 17.

[71] Zob. J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

w ogóle. Stąd też tego rodzaju pojęcia poddane próbom zdefiniowania i generalizacji zawsze będą siłą rzeczy swoistym uproszczeniem.

Pewne uproszczenie i zarazem ożywione dyskusje wprowadza już sam przedrostek „cyber". Nie brak poglądów, że zbitki słowne z udziałem tego prefiksu są swoistą nowomową, bezkrytycznie konstruującą słowa wytrychy będące efektem swego rodzaju imperializmu naukowego[72] na oznaczenie najnowszych trendów społecznych lub naukowych[73]. Zastrzeżenia dotyczą także terminu „przestrzeń", który proponuje się, w nawiązaniu do wspomnianej normy ISO/IEC 270032, zastąpić terminem „środowisko"[74]. Tego rodzaju propozycje rozszerzają w istocie dyskusje pojęciowe o konieczność zdefiniowania terminu „środowisko", traktowanego w normie jako efekt interakcji ludzi, oprogramowania oraz usług internetowych, realizowane za pomocą podłączonych urządzeń i sieci informatycznych, który nie istnieje w formie materialnej. Można mieć przy tym wątpliwości, czy termin „środowisko" lepiej odzwierciedla istotę cyberprzestrzeni.

Warto zwrócić uwagę, że w nauce pojęcie przestrzeni ma swoje znaczenia w filozofii, matematyce czy fizyce; podobnie w naukach humanistycznych, jak socjologia, psychologia czy nauki prawne, w których od dawna funkcjonuje pojęcie przestrzeni prawnej, jako narzędzie badawcze kultury prawnej w jakimś obszarze[75]. Dla wielu różnych dziedzin przestrzeń jest pojęciem uniwersalnym, chociaż metodologicznie zróżnicowanym. Przedstawiciele geografii humanistycznej trafnie przyjmują, że odkrywanie kolejnych rodzajów przestrzeni i związane z tym przekraczanie obszarów badawczych odmiennych dyscyplin naukowych prowadzi do wniosku, że przestrzeń, należąca do podstawowych pojęć myśli ludzkiej, jest podstawą refleksji związanej z poznawaniem i rozumieniem otaczającego człowieka świata, zaś „rozważania nad przestrzenią nie mogą dotyczyć jednego, uniwersalnego określenia przestrzeni"[76]. Pogląd ten nie budzi wątpliwości; przestrzeń jest nie tylko abstrakcyjną ideą (matematyczną) i własnością materii, ale także ludzkim tworem, antropogenicznym, kulturowym i społecznym[77]. Termin „cyberprzestrzeń" oddaje właśnie fenomen ukształtowania się nowego wymiaru przestrzeni. Pojęcie cyberprzestrzeni wydaje się być przy tym utrwalone w świadomości użytkowników sieci, ale także i w nauce. W literaturze nie brak poglądów, że przedrostek „cyber-" jest używany zarówno do tworzenia pojęć społecznie użytecznych, jak i pojęć naukowych, tworzonych z jego wykorzystaniem[78].

[72] K. Liderman, *O zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową*, Konferencja „Cyberspace 2009" za D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji…*, s. 49.

[73] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 31.

[74] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji…*, s. 50.

[75] Zob. zwłaszcza *Przestrzeń w prawie administracyjnym*, red. J. Zimmermann, Warszawa 2013.

[76] J. Kaczmarek, *Podejście geobiograficzne w geografii społecznej. Zarys teorii i podstawy metodyczne*, Łódź 2005, s. 17.

[77] B. Jałowiecki, *Przestrzeń społeczna. Encyklopedia socjologii*, t. 3, Warszawa 2002, s. 301.

[78] C. Marcinkowski, *Cyberprzestrzeń a istota…*, s. 114.

Trudności definicyjne sprawiają, że cyberprzestrzeń, podobnie jak cyberbezpieczeństwo, są pewną konwencją terminologiczną. Cyberprzestrzeń pozostaje hasłowym określeniem interaktywnego i multimedialnego systemu komunikacji, na który składają się w równym stopniu elementy techniczne i technologiczne, jak również społeczne[79]. Z kolei bezpieczeństwo w cyberprzestrzeni, którego desygnaty tkwią w świadomości każdego operatora i użytkownika sieci, i której konkretyzacja ma wprawdzie charakter podmiotowy, uwarunkowany zakresem aktywności danego podmiotu, to z punktu widzenia przedmiotowego pozwala sprowadzić się do ochrony bezpieczeństwa informacyjnego; również ujęcie narzędziowe, jak np. ochrona infrastruktury teleinformatycznej przed atakiem czy naruszeniem integralności, jest w istocie ochroną informacji.

Otwarte jest pytanie, na ile cyberprzestrzeń i jej bezpieczeństwo można by zaliczyć do – wypracowanej w stosunkach międzynarodowych – nowej kategorii globalnych dóbr publicznych (ang. *global public goods*), czyli dóbr niepodlegających rywalizacji w zakresie ich wykorzystywania (ang. *non-rivalrous*), z których korzyści uzyskują wszystkie podmioty, czyli użycie takiego dobra przez jakiś podmiot nie zmniejsza ilości dostępnej dla innych (ang. *non-excludable*), a ich zasięg jest globalny (ang. *availablemore-or-less worldwide*)[80]. Pojęcie globalnych dóbr publicznych nie jest powszechnie akceptowane; podnosi się, że kategorii tej można zarzucić kreację pustego bytu, bez nowych treści, lub kreację bytów o zbędnej treści, co wynika z jej ogólności, łatwą do zastąpienia przez kategorię interesu publicznego[81]. Pogląd ten też nie do końca jest trafny, gdyż pomija fakt, że pojęcie interesu publicznego jest terminem równie trudnym do zdefiniowania; z uwagi na wielość jego funkcji, wewnętrzną złożoność i silne uwarunkowania zewnętrzne[82], a zwłaszcza zróżnicowanie jego znaczenia zarówno w zależności od celu, jak i treści przedmiotu działania, w którym znajduje zastosowanie, trudno jest uogólniać jego znaczenie. Pojęcie interesu publicznego jako klauzula generalna odsyła do reguł i ocen pozaprawnych, pozwalając organowi władzy publicznej na podejmowanie różnych treściowo decyzji w zależności od okoliczności danego przypadku[83]. W konsekwencji, pojęcie interesu publicznego wymaga każdorazowo konkretyzacji stosownie do określonych stanów faktycznych[84], w świetle określonego stanu normatywnego. Stąd też pojęcie interesu publicznego nie spełnia wymogu poprawności metodologicznej w odniesieniu do bezpieczeństwa w cyberprzestrzeni.

[79] K. Dobrzeniecki, *Prawo a etos…*, s. 21.

[80] J. Bielawski, *Współpraca międzynarodowa na rzecz globalnych dóbr publicznych*, „Sprawy Międzynarodowe" 2003/1, s. 35–46.

[81] R. Rosicki, *O pojęciu…*, s. 23 i n.

[82] M. Wyrzykowski, *Pojęcie interesu społecznego w prawie administracyjnym*, Warszawa 1986, s. 44.

[83] T. Zieliński, *Klauzule generalne w prawie pracy*, Warszawa 1988, s. 56. Tak też W. Jakimowicz, *Wykładnia w prawie administracyjnym*, Kraków 2006, s. 124 i n.; A. Borkowski, *Interes publiczny jako determinant działań władzy publicznej i klauzula generalna w publicznym prawie gospodarczym* [w:] *Nowe problemy badawcze w teorii publicznego prawa gospodarczego (z uwzględnieniem samorządu terytorialnego)*, red. L. Kieres, Wrocław 2010, s. 9 i n.

[84] B. Adamiak, J. Borkowski, *Postępowanie administracyjne i sądowoadministracyjne*, Warszawa 2002, s. 135.

Koncepcja globalnych dóbr publicznych oparta jest natomiast na założeniu, że kategoria dobra wspólnego nie jest stała i niezmienna, będąc ponadto kategorią niezdeterminowaną przez państwo, jego typ lub sposób sprawowania władzy[85]. Jest to o tyle istotne, że rewolucja informatyczna, która stworzyła w istocie cyberprzestrzeń i potrzebę bezpieczeństwa w niej, ma charakter globalny, obejmując zasoby, ale i wartości, które wykraczają poza zakresy terytorialne czy jurysdykcyjne państw. Ponadto koncepcja dobra publicznego była z założenia konstruowana jako wartość konkurencyjna w stosunku do interesów jednostkowych, aczkolwiek ostatecznie służąca zabezpieczeniu tych interesów[86]. Stąd też koncepcja globalnych dóbr publicznych znacznie lepiej odzwierciedla istotę bezpieczeństwa w cyberprzestrzeni niż pojęcie interesu publicznego. Ponadto warto zwrócić uwagę, że skoro pojęcia niedookreślone uzyskują treściowe kontury dopiero w momencie zastosowania tego pojęcia do konkretnego przypadku, ich zawartość treściowa rzadko może zostać zdefiniowana[87]; może co najwyżej być przedmiotem opisu ich cech zasadniczych[88]. Istota globalizacji znacząco wzmacnia ten opis.

Koncepcja globalnych dóbr publicznych w sposób oczywisty nie rozwiewa wszystkich wątpliwości co do prawnej istoty cyberprzestrzeni; przybliżony jedynie w ten sposób przedmiot ochrony pozostaje nadal niedookreślony. Otwarte jest też pytanie, na ile możliwe jest przeniesienie koncepcji świata rzeczywistego, nadającej się do regulacji np. przestrzeni kosmicznej, do świata wirtualnego, podobnie jak i pytanie o zakres rywalizacji w zakresie wykorzystania cyberprzestrzeni. Kwestie te wymagają dalszych badań; niemniej celowe jest zasygnalizowanie też i tego kierunku interpretacji pojęcia cyberprzestrzeni i bezpieczeństwa w niej.

Próby zinterpretowania pojęcia bezpieczeństwa w cyberprzestrzeni są w istocie odzwierciedleniem wzrostu zainteresowania tą problematyką, wynikającego z narastających zagrożeń występujących w tym środowisku. Cyberprzestrzeń niesie za sobą wiele istotnych zagrożeń zarówno dla poszczególnych osób, całych społeczności, jak i instytucji i państw; problemy cyberbezpieczeństwa jednego państwa stały się pochodną bezpieczeństwa w cyberprzestrzeni innych państw. Globalny charakter cyberprzestrzeni i anonimowość jej uczestników jest też źródłem zagrożeń i ryzyk w poszanowaniu praw podstawowych. Zarówno korzyści z cyberprzestrzeni, jak i zagrożenia w jej funkcjonowaniu sprawiają, że problematyka cyberprzestrzeni i bezpieczeństwa w niej stały się przedmiotem badań, a także regulacji prawnych, tworzących podstawy pod kształtowanie się nowej dyscypliny naukowej, jaką jest cyberbezpieczeństwo. Jeżeli tylko uwzględni się, że ponad 60% ludności świata korzysta z internetu, to samo to w sobie jest

[85] A. Młynarska-Sobaczewska, *Dobro wspólne jako kategoria normatywna*, „Acta Universitatis Lodziensis. Folia Iuridica" 2009/69, s. 65.

[86] M. Zdyb, *Prawny interes jednostki w sferze materialnego prawa administracyjnego. Studium teoretyczno-prawne*, Lublin 1991, s. 201, za L. Góral, *Interes publiczny jako przesłanka ingerencji państwa w sferę funkcjonowania rynku bankowego w Polsce i we Francji*, „Studia Prawno-Ekonomiczne" 2010/83, s. 53.

[87] C. Banasiński, *Dyskrecjonalność w prawie antymonopolowym*, Warszawa 2015, s. 123 i n.

[88] M. Wyrzykowski, *Pojęcie interesu społecznego…*, s. 50.

aksjologiczną podstawą wyodrębnienia cyberbezpieczeństwa jako samodzielnej dyscypliny naukowej, której specyfika jest pochodną wielowymiarowości cyberprzestrzeni, która jest wieloszczeblowa, transsektorowa i zarazem globalna. Kwestia bezpieczeństwa w cyberprzestrzeni staje się jednym z kluczowych obszarów badawczych współczesnych nauk o bezpieczeństwie, nawet jeżeli pojęcia cyberbezpieczeństwa i cyberprzestrzeni nie są jednoznacznie zdefiniowane.

Bezpieczeństwo w cyberprzestrzeni sytuuje się jako istotna część nowej dyscypliny naukowej jaką jest securitologia, której obszar zainteresowań obejmie badania dotyczące zagrożeń odnoszących się do istnienia, rozwoju i funkcjonowania człowieka[89]. W literaturze wskazuje się, że z uwagi na multi- i interdyscyplinarny charakter bezpieczeństwa securitologia ma naturę transdyscyplinarną, co oznacza konieczność korzystania z dorobku teoretycznego i warsztatu metodologicznego innych dyscyplin naukowych; zakłada to zarazem konieczność podejścia holistycznego i systemowego do problematyki bezpieczeństwa[90]. Podejście to w pełni odpowiada problematyce bezpieczeństwa w cyberprzestrzeni.

Rewolucja cyfrowa zaowocowała zupełnie odmiennym spojrzeniem na efektywność ekonomiczną, możliwości świadczenia usług użyteczności publicznej, a zwłaszcza ich dostępność i zakres, sposób komunikacji społecznej czy wreszcie współpracę międzynarodową. Sprawia to, że problematyki cyberprzestrzeni nie da się analizować wyłącznie w kategoriach technologicznych; cyberprzestrzeń jest przede wszystkim społeczną płaszczyzną komunikacji całkowicie odrębną od tradycyjnego (realnego) obszaru aktywności człowieka. W tym też sensie cyberprzestrzeń jest nie tylko cyfrową postacią komunikowania się, ale przede wszystkim określoną instytucją społeczną, tworzącą zasadniczą bazę dla budowania społeczeństwa informacyjnego; jest to specyficzna, dzięki technologii cyfrowej, równoległa wobec tradycyjnej (materialnej i realnej) przestrzeń kształtowania się relacji pomiędzy ludźmi, która z trudnością daje się analizować z użyciem tradycyjnej siatki pojęciowej, właściwej dla świata realnego. Analiza bezpieczeństwa w cyberprzestrzeni musi tę specyfikę uwzględniać.

Przedmiotem badań i regulacji cyberprzestrzeni jest w równym stopniu poszanowanie praw podstawowych czy zwalczanie cyberprzestępczości, jak również globalna interoperacyjność systemów informatycznych oraz konieczność zagwarantowania stabilności działania systemów teleinformatycznych, zwłaszcza w odniesieniu do tzw. infrastruktury krytycznej, w tym sieci informatycznych, których sprawne funkcjonowanie zapewnia bieżące i nieprzerwane świadczenie usług powszechnych.

[89] L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka…*, s. 87.
[90] L.F. Korzeniowski, *Securitologia. Nauka o bezpieczeństwie człowieka…*, s. 48–49.

3. Podstawy prawne cyberbezpieczeństwa

3.1. Regulacje cyberbezpieczeństwa w działalności ONZ

Ciężar działań legislacyjnych ONZ w sprawach cyberbezpieczeństwa międzynarodowego ogniskuje się wokół rezolucji Zgromadzenia Ogólnego. Rezolucje te, nie zawierając jednak – w przeciwieństwie do rezolucji Rady Bezpieczeństwa ONZ – norm prawnie wiążących, są wyłącznie zaleceniami adresowanymi do państw członkowskich.

Problem cyberbezpieczeństwa ONZ podjęła w rezolucji ZO ONZ nr 45/121[91] z 14.12.1990 r., w której Zgromadzenie Ogólne zatwierdziło zalecenia ósmego Kongresu Organizacji Narodów Zjednoczonych w sprawie zapobiegania przestępczości, zwracając szczególną uwagę na przestępstwa komputerowe i zalecając państwom członkowskim bardziej skuteczne wzmacnianie wysiłków na rzecz zwalczania nadużyć komputerowych.

Potrzeba precyzyjnej diagnozy w obszarze bezpieczeństwa w cyberprzestrzeni zaowocowała uchwaleniem rezolucji ZO ONZ nr 53/70 z 4.12.1998 r.[92] w sprawie rozwoju sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego (ang. *Developments in the field of information and telecommunications in the context of international security*). W rezolucji podkreślono rolę nauki i technologii w rozwoju cywilizacji, rozszerzeniu możliwości współpracy dla wspólnego dobra wszystkich państw, wzmocnieniu potencjału twórczego ludzkości i usprawnieniu obiegu informacji w globalnej społeczności. Zgromadzenie wyraziło jednocześnie zaniepokojenie, że technologie i środki informatyczne mogą zostać wykorzystane do celów, które są niezgodne z celami utrzymania stabilności i bezpieczeństwa na świecie oraz mogą negatywnie wpływać na bezpieczeństwo państw, co oznacza konieczność zapobiegania niewłaściwemu wykorzystywaniu technologii informatycznych do celów przestępczych lub terrorystycznych. Wezwano w związku z tym państwa członkowskie do przedstawienia stanowiska w kwestii definicji podstawowych pojęć związanych z bezpieczeństwem informacji, w tym nieuprawnionej ingerencji z wykorzystaniem lub niewłaściwym wykorzystaniem systemów informatycznych i telekomunikacyjnych, a także zasobów informacyjnych, oraz celowości opracowania międzynarodowych zasad, które zwiększyłyby globalne bezpieczeństwo systemów informatycznych i telekomunikacyjnych, pomagając w walce z terroryzmem informacyjnym i przestępczością.

Problematyka ta skonkretyzowana została ostatecznie w dwóch rezolucjach w sprawie zwalczania kryminalnych nadużyć w technologiach informacyjnych (ang. *Combating the criminal misuse of information technologies*) – rezolucji ZO ONZ nr 55/63

[91] https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/572/84/IMG/NR057284.pdf?OpenElement (dostęp: 1.07.2023 r.).

[92] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement (dostęp: 1.07.2023 r.).

z 4.12.2000 r.[93] oraz rezolucji ZO ONZ nr 56/121 z 19.12.2001 r.[94], w których wezwano państwa członkowskie do wprowadzenia regulacji gwarantujących skuteczną ochronę integralności i dostępność danych w systemach komputerowych, a także wprowadzenia przepisów realizujących zwalczanie przestępstw dokonywanych z użyciem technologii informacyjnych. W rezolucjach podkreślono, że postępujący wzrost globalnej współpracy międzynarodowej przy niezgodnym z prawem wykorzystaniu technologii informatycznych może mieć poważny wpływ na wszystkie państwa członkowskie. Wymaga to zarówno współpracy między państwami i organizacjami międzynarodowymi, jak i sektorem prywatnym. W rezolucjach wezwano też, aby przepisy i praktyka państw członkowskich eliminowały możliwość bezpiecznego schronienia dla sprawców nadużyć technologii informatycznych oraz zwrócono uwagę na konieczność daleko idącej współpracy w sprawach karnych organów ścigania w dochodzeniu i ściganiu w sytuacji międzynarodowych przypadków niewłaściwego wykorzystania tych technologii. Systemy prawne powinny ponadto chronić poufność, integralność i dostępność danych w systemach informatycznych przed niepowołanym naruszeniem, zapewniając jednocześnie karalność ich naruszeń. Co istotne, zwłaszcza w rezolucji nr 56/121 podkreśla się, że walka z wykorzystaniem technologii informatycznych przez przestępców wymaga opracowania rozwiązań uwzględniających zarówno ochronę wolności jednostki i prywatności, jak i zachowanie zdolności państw do skutecznego przeciwdziałania tego rodzaju nadużyciom.

Dynamiczny postęp technologiczny zmierzający w kierunku informatyzacji państw oraz społeczeństw i zarazem postępujący wzrost zagrożeń cyberprzestępczością w sieci zaowocował kolejnymi dwoma rezolucjami ZO ONZ, ukierunkowanymi na konieczność stworzenia globalnej kultury cyberbezpieczeństwa. W rezolucji ZO ONZ nr 57/239 z 20.12.2002 r.[95] w sprawie stworzenia globalnej kultury cyberbezpieczeństwa (ang. *Creation of global culture of cybersecurity*) wyraźnie podkreślono znaczenie bezpiecznego uczestnictwa w sieci, zapewniającego przy tym swobodę wypowiedzi i nieskrępowany przepływ wymiany informacji, ale przy zagwarantowaniu ochrony danych osobowych. Rezolucję tę wzmocniła rezolucja ZO ONZ nr 58/199 z 23.12.2003 r.[96] w sprawie stworzenia globalnej kultury cyberbezpieczeństwa i ochrony informatycznej infrastruktury krytycznej (ang. *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*). Ich zwieńczeniem była rezolucja ZO ONZ nr 64/211 z 21.12.2009 r.[97] w sprawie stworzenia globalnej kultury cyberbezpieczeństwa

[93] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement (dostęp: 1.07.2023 r.).

[94] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement (dostęp: 1.07.2023 r.).

[95] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement (dostęp: 1.07.2023 r.).

[96] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement (dostęp: 1.07.2023 r.).

[97] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/49/PDF/N0947449.pdf?OpenElement (dostęp: 1.07.2023 r.).

i podsumowania wysiłków krajowych w dziedzinie informatycznej infrastruktury krytycznej (ang. *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*). Odwołując się do dotychczasowych rezolucji w sprawie zwalczania nadużyć komputerowych, Zgromadzenie Ogólne wezwało państwa członkowskie do dalszych wysiłków w zakresie wzmocnienia globalnej kultury cyberbezpieczeństwa poprzez wzajemną pomoc we wdrażaniu praktyk i środków realizacji strategii ochrony krytycznej infrastruktury informatycznej.

Na podstawie oceny dotychczas stosowanych praktyk i środków wskazano ponadto narzędzia dobrowolnej samooceny stanu bezpieczeństwa dotyczącego ochrony krytycznej infrastruktury informatycznej. W odniesieniu do rozwoju kultury narodowej cyberbezpieczeństwa podniesiono jednocześnie konieczność wdrożenia planu cyberbezpieczeństwa dla systemów obsługiwanych przez rząd, budowy krajowych programów podnoszenia świadomości, zwłaszcza wśród dzieci i indywidualnych użytkowników sieci, oraz wymagań dotyczących szkoleń w zakresie ochrony infrastruktury.

W rezolucji ZO ONZ nr 65/230[98] z 21.12.2010 r. (ang. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*) powierzono Biuru Narodów Zjednoczonych ds. Narkotyków i Przestępczości (ang. *United Nations Office on Drugs and Crime*, UNODC) opracowanie i wdrożenie globalnego programu zwalczania cyberprzestępczości. Biuro jest instytucją powołaną do walki z przestępczością międzynarodową, nielegalnym handlem narkotykami oraz terroryzmem. Promuje ono długofalowe i trwałe budowanie potencjału w walce z cyberprzestępczością poprzez wspieranie krajowych struktur i działań, aby zapewnić pomoc techniczną w budowaniu potencjału, zapobieganiu i zwiększaniu świadomości, współpracy międzynarodowej oraz gromadzeniu danych, badaniach i analizach dotyczących cyberprzestępczości. Programy globalne mają na celu elastyczne reagowanie na zidentyfikowane potrzeby przede wszystkim w krajach rozwijających się poprzez wspieranie państw członkowskich w holistycznym zapobieganiu i zwalczaniu cyberprzestępczości.

Nie bez znaczenia dla problematyki cyberbezpieczeństwa jest także działalność Forum Zarządzania Internetem (ang. *Internet Governance Forum*, IGF), wyłonionego w 2005 r. w trakcie Światowego Szczytu Społeczeństwa Informacyjnego (ang. *The World Summit on the Information Society*, WSIS), działającego pod auspicjami ONZ. Forum Zarządzania Internetem służy łączeniu ludzi z różnych grup interesariuszy w dyskusjach na temat zagadnień polityki publicznej związanych z internetem. Chociaż nie ma żadnych wynegocjowanych wyników, IGF informuje i inspiruje tych, którzy mają władzę w zakresie kształtowania polityki zarówno w sektorze publicznym, jak i prywatnym. Celem IGF jest powszechne zrozumienie, jak zmaksymalizować szanse korzystania z internetu i rozwiązać pojawiające się zagrożenia i wyzwania.

[98] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement (dostęp: 1.07.2023 r.).

W rezolucji ZO ONZ nr 70/125 z 16.12.2015 r.[99] dotyczącej efektów ogólnego przeglądu wdrażania wyników światowego szczytu w sprawie społeczeństwa informacyjnego (ang. *Document on 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*) dotychczasowy mandat IGF, o którym mowa w agendzie szczytu w Tunisie, przedłużono o kolejne 10 lat. Mandat ten obejmuje takie kwestie, jak: 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 istniejącego organu międzynarodowego, wymianę informacji i najlepszych praktyk, identyfikację pojawiających się problemów oraz ewentualnie wydawanie zaleceń czy wcielenie zasad WSIS w procesach zarządzania internetem, zwłaszcza odnoszących się do krytycznych zasobów internetu.

Warto odnotować także, że 3.11.2022 r. Komitet Zgromadzenia Ogólnego ONZ przyjął rezolucję w sprawie programu działania (*Plan of Action*, PoA) dotyczącego cyberbezpieczeństwa[100], który jest kontynuacją poprzednich programów uchwalanych corocznie. Program zakłada bieżące omawianie istniejących i potencjalnych zagrożeń, promowanie i współpracę z odpowiednimi zainteresowanymi stronami oraz dokonywanie okresowych przeglądów postępów w realizacji programu działania, a także przyszłych prac programu. W rezolucji zaapelowano również do sekretarza generalnego ONZ o zwrócenie się do państw członkowskich ONZ z prośbą o opinię na temat zakresu, struktury i treści programu działań, a także na temat prac przygotowawczych i warunków jego utworzenia.

Równie istotne są działania Międzynarodowego Związku Telekomunikacyjnego (ang. *International Telecommunication Union*, ITU), który jest organizacją wyspecjalizowaną ONZ ds. technologii informacyjnych i komunikacyjnych (ICT). Został on ustanowiony w celu standaryzowania oraz regulowania rynku telekomunikacyjnego i radiokomunikacyjnego. Związek zrzesza zarówno państwa, jak i podmioty sektora prywatnego działające w obszarze łączności elektronicznej. Stałym organem ITU jest tzw. ITU-T działający w sektorze normalizacji telekomunikacyjnej ITU, który odpowiada za badania techniczne, operacyjne i taryfowe, wydając zalecenia w celu standaryzacji telekomunikacji na całym świecie. Przykładem może być zalecenie ITU-T X.1500 odnoszące się do wymiany informacji dotyczących bezpieczeństwa cyberprzestrzeni (CYBEX). Zalecenia wydawane są także odnośnie do problemów będących przedmiotem obrad Światowego Zgromadzenia ds. Normalizacji Telekomunikacji (ang. *World Telecommunication Standardization Assembly*, WTSA), które zbiera się co cztery lata.

[99] http://unctad.org/en/PublicationsLibrary/ares70d125_en.pdf; United Nations A/RES/70/125 (dostęp: 1.07.2023 r.).

[100] https://digitallibrary.un.org/nanna/record/3991743/files/A_C.1_77_L.73-EN.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1 (dostęp: 1.07.2023 r.).

Zatwierdzenie zaleceń ITU-T jest objęte procedurą określoną w uchwale WTSA nr 1. W trakcie Światowego Zgromadzenia w Hammamet, 25.10–3.11.2016 r., podjęto uchwałę dotyczącą cyberbezpieczeństwa[101], gdzie podkreślono konieczność wypracowania standardów cyberbezpieczeństwa zarówno na podstawie „Mapy drogowej dotyczącej standardów" i działania ITU-D w zakresie cyberbezpieczeństwa i innych regionalnych i międzynarodowych inicjatyw oraz działań promujących ogólnoświatową harmonizację strategii i podejść w tym obszarze, jak i na podstawie Globalnej Agendy Cyberbezpieczeństwa ITU (ang. *Global Cybersecurity Agenda*, GCA), która stanowi ramy międzynarodowej współpracy mającej na celu zwiększenie zaufania i bezpieczeństwa w społeczeństwie informacyjnym. GCA została zaprojektowana z myślą o współpracy i wydajności, zachęcaniu do współpracy z wszystkimi odpowiednimi partnerami i rozwijaniu istniejących między nimi inicjatyw, aby uniknąć powielania działań.

Powyższe działania są istotne, ale niewystarczające; coraz częściej zwraca się uwagę na potrzebę stworzenia międzynarodowego traktatu o cyberprzestrzeni na wzór podpisanego w 1967 r. Międzynarodowego Układu o Przestrzeni Kosmicznej. Miałoby to być porozumienie adresowane do państw (rządów) i normujące zasady zachowań samych państw w cyberprzestrzeni. W tym też celu powołano w 2004 r., działającą w ramach ONZ, Grupę Ekspertów Rządowych ONZ (ang. *Group of Government Experts*, UN GGE), której zadaniem ma być wypracowanie „wspólnego zrozumienia" zachowań państw w cyberprzestrzeni. W praktyce działania Grupy nie jest to zadanie łatwe z uwagi na prezentowane na łamach ONZ dwa ogólne podejścia państw członkowskich do problemu tzw. normy cyberprzestrzeni, czyli zachowań państw w środowisku teleinformatycznym. O ile pierwsze z nich opiera się na założeniu wolności działania wszystkich podmiotów w cyberprzestrzeni przy poszanowaniu ładu, pokoju, godności ludzkiej oraz wolności konkurowania w gospodarce, o tyle drugie przyjmuje, że celem regulacji powinno być przeciwdziałanie wykorzystaniu cyberprzestrzeni dla celów niezgodnych z Kartą ONZ[102], przy czym państwa powinny zachować pełną kontrolę nad cyberprzestrzenią z uwagi na ich suwerenność i niezbędne wymogi bezpieczeństwa[103].

Oba stanowiska są wobec siebie wyjątkowo kolizyjne, zostawiając niewiele miejsca na wypracowanie niezbędnego konsensusu. Potwierdza to chociażby fiasko ostatniego (piątego) spotkania Grupy Ekspertów Rządowych ONZ z uwagi na brak zgody co do kwestii stosowania norm prawa międzynarodowego, a zwłaszcza stosowania zasad statutu ONZ w zakresie wykorzystania siły i międzynarodowego prawa humanitarnego. W szczególności pojawiły się kontrowersje wobec propozycji równoważności między

[101] https://www.itu.int/pub/T-RES-T.50-2016 (dostęp: 1.07.2023 r.).

[102] https://www.unic.un.org.pl/dokumenty/karta_onz.php (dostęp: 1.07.2023 r.).

[103] E. Haliżak, *Cyberprzestrzeń: zagrożenia i nowe możliwości rozwoju w stosunkach międzynarodowych*, *CyberVademecum, Materiały z Konferencji Warszawskiej*, Warszawa 2017, s. 20–21.

świadomym wykorzystaniem technologii teleinformatycznej a koncepcją zbrojnego ataku, gdyż oznaczałoby to możliwość reakcji w sposób konwencjonalny w odpowiedzi na cyberataki.

Równie trudną kwestią do uzgodnienia jest możliwość stosowania międzynarodowego prawa humanitarnego do działań w cyberprzestrzeni[104]. Międzynarodowe prawo humanitarne służy bowiem rozwiązywaniu problemów humanitarnych wynikających z konfliktów zbrojnych, poprzez normy prawne zawierające ograniczenia w metodach i środkach prowadzenia działań zbrojnych oraz zasady ochrony mienia i ludności niezaangażowanej w działania zbrojne przed skutkami tych działań[105]; w szczególności strony konfliktu zbrojnego muszą w każdym momencie rozróżniać siły zbrojne od ludności cywilnej, która nie może być atakowana[106]. Zastosowanie międzynarodowego prawa humanitarnego do działań w cyberprzestrzeni w pewnym sensie legitymizuje w niej militarne działania agresywne, pomijając już fakt trudności rozróżnienia cywilnej i agresywnej infrastruktury. W praktyce jest to też swoiste „granie na zwłokę" przez państwa aktywnie zaangażowane w budowanie ofensywnych możliwości działania w cyberprzestrzeni.

W tej sytuacji ciężar przygotowania regulacji prawnomiędzynarodowej spoczywa w efekcie na World Summit on the Information Society (WSIS) i jego organie wykonawczym, jakim jest Internet Governance Forum (IGF), który ma mandat do działania do 2025 r., oraz na International Telecommunication Union (ITU). Zadaniem tych organów jest wypracowanie dobrych praktyk w zakresie użytkowania internetu i zachowań w cyberprzestrzeni[107].

3.2. Inicjatywy legislacyjne Rady Europy

W skali regionalnej podstawy prawne cyberbezpieczeństwa międzynarodowego tworzy przede wszystkim Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie 23.11.2001 r.[108]

[104] T. Widłak, *Legitymizacja uniwersalnej jurysdykcji jako narzędzia implementacji międzynarodowego prawa humanitarnego*, „Międzynarodowe Prawo Humanitarne" 2015/6, s. 29 i n.

[105] A. Szpak, *Międzynarodowe prawo humanitarne*, Toruń 2014; J.M. Henckaerts, *Studium poświęcone zwyczajowemu międzynarodowemu prawu humanitarnemu: wkład w zrozumienie i poszanowanie zasad prawa dotyczących konfliktu zbrojnego*, Warszawa 2006.

[106] Fundamentalnymi umowami międzynarodowymi z tego zakresu są przede wszystkim tzw. konwencje haskie z 29.07.1899 r. i 18.10.1907 r. oraz tzw. konwencje genewskie z 12.08.1949 r., wraz z dwoma protokołami dodatkowymi do nich z 1977 r.

[107] Dotyczy to zwłaszcza IGF, które jest forum dialogu politycznego w sprawach zarządzania internetem, reprezentowanym przez rządy, sektor prywatny czy społeczeństwo obywatelskie, w tym społeczność techniczną i akademicką, na równych zasadach i w drodze otwartego procesu integracji.

[108] Przyjęta przez Polskę i opubl. w Dz.U. z 2015 r. poz. 728.

Konwencja uważana jest obecnie za szczególne osiągnięcie Rady w tym zakresie. Jest ona podsumowaniem i zarazem kontynuacją prac Rady Europy nad tworzeniem międzynarodowych standardów normatywnych ukierunkowanych na zwalczanie przestępstw komputerowych. Prace te objęły wydanie Zalecenia Komitetu Ministrów Rady Europy Nr R(89)9 o przestępczości komputerowej (ang. *Computer-Related Crime*)[109], w którym zawarto wytyczne dla legislacji krajowej dotyczące przestępstw komputerowych oraz Zalecenia Komitetu Ministrów Rady Europy Nr R(95)13 w sprawie problemów karnoprocesowych związanych z nowoczesną technologią przetwarzania informacji (ang. *Problems of Criminal Procedural Law Connected with Information Technology*)[110]. Nie bez znaczenia jest także rezolucja nr 1 przyjęta na 21 Konferencji Europejskich Ministrów Sprawiedliwości (Praga, 10–11.06.1997 r.), w której zlecono Komitetowi Ministrów wspieranie prac prowadzonych przez Europejski Komitet ds. Problematyki Przestępczości (ang. *European Committee on Crime Problems*, CDPC) w zakresie cyberprzestępczości w celu wzajemnego zbliżenia postanowień w zakresie prawa karnego oraz umożliwienia stosowania efektywnych środków ścigania takich przestępstw, jak również rezolucja nr 3 przyjęta na 23 Konferencji Europejskich Ministrów Sprawiedliwości (Londyn, 8–9.06.2000 r.), która zachęcała strony do kontynuowania ich wysiłków mających na celu znalezienie właściwych rozwiązań, które umożliwiłyby przystąpienie do Konwencji jak największej liczbie państw, oraz apelowała o stworzenie szybkiego i efektywnego systemu współpracy międzynarodowej, uwzględniającej szczególne wymagania walki z cyberprzestępczością. Istotnym dokumentem jest także Plan Działania przyjęty przez szefów państw i rządów Rady Europy podczas ich Drugiego Szczytu (Strasburg, 10–11.10.1997 r.) w celu wypracowania wspólnych stanowisk w kwestii rozwoju nowych technologii, opartych na standardach i wartościach Rady Europy.

Konwencja o cyberprzestępczości jest ukierunkowana na powstrzymanie działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych poprzez uznanie takiego postępowania za przestępstwo oraz przyjęcie środków, które będą przydatne w skutecznym zwalczaniu przestępstw, co dotyczy ułatwienia ich wykrywania, prowadzenia, dochodzenia i ścigania zarówno na szczeblu krajowym, jak i międzynarodowym. Konwencja przyjmuje przy tym rozwiązania sprzyjające szybkiej i rzetelnej współpracy międzynarodowej, jak np. reguły ekstradycyjne czy zasady wzajemnej pomocy prawnej w sytuacji nawet braku stosownych porozumień w tym zakresie.

Konwencja wyróżnia cztery rodzaje przestępstw w cyberprzestrzeni, a mianowicie: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (nielegalny dostęp, nielegalne przechwytywanie danych, naruszenie

[109] https://rm.coe.int/09000016804f1094 (dostęp: 1.07.2023 r.).

[110] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (dostęp: 1.07.2023 r.).

integralności danych, naruszenie integralności systemu, niewłaściwe użycie urządzeń), przestępstwa komputerowe (fałszerstwo i oszustwo komputerowe), przestępstwa ze względu na charakter zawartych informacji (co dotyczy pornografii dziecięcej) oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych. Do zagadnienia wykorzystania seksualnego dzieci odnosi się również inny akt prawa międzynarodowego. Jest to Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzona w Lanzarote 25.10.2007 r., czasem zwana Konwencją Rady Europy z Lanzarote[111]. Dotyczy ona wykorzystania dzieci w celach seksualnych w ogóle, a nie tylko w cyberprzestrzeni[112].

Konwencji o cyberprzestępczości nie sposób nie docenić[113]; stanowi bowiem efektywne narzędzie międzynarodowej ochrony podmiotów wykorzystujących technologie komputerowe oraz podmiotów, wobec których technologie te umożliwiają lub ułatwiają popełnianie przestępstw. Konwencja zawiera uniwersalne standardy w zakresie problematyki przestępstw popełnianych przy zastosowaniu technologii informatycznych, a przede wszystkim definicje czynów zabronionych i norm dotyczących współpracy międzynarodowej w ich ściganiu.

Konwencja jest, jak na razie, pierwszym i jedynym aktem prawa międzynarodowego w tym zakresie[114]. Jako zbiór standardów prawnych służących współpracy międzynarodowej w dziedzinie ścigania przestępstw transgranicznych popełnianych z wykorzystaniem technologii informatycznych cieszy się zainteresowaniem społeczności międzynarodowej i wywiera istotny wpływ na ustawodawstwa karne państw europejskich i pozaeuropejskich.

3.3. Dorobek prawny Unii Europejskiej

Podstawy prawne cyberbezpieczeństwa w UE są silnie zintegrowane z dokumentami programowymi, które albo stanowią zapowiedź określonych regulacji prawnych na poziomie europejskim, albo ich uzupełnienie o działania je wspomagające. Wyrazem tego podejścia jest Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa UE (ang. *A Global Strategy for the EU's Foreign and Security Policy*)[115], zastępująca

[111] Dz.U. z 2015 r. poz. 608.

[112] Pornografii dziecięcej dotyczy także Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych 20.11.1989 r. (Dz.U. z 1991 r. Nr 120, poz. 526 ze zm.). Nie reguluje ona jednak kwestii rozpowszechniania pornografii dziecięcej, tym bardziej rozpowszechniania w cyberprzestrzeni. Z tego powodu została tu pominięta.

[113] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012/7–8, s. 247.

[114] Stronami konwencji są 62 państwa, w tym 26 państw członkowskich Unii Europejskiej.

[115] https://eur-lex.europa.eu/PL/legal-content/summary/common-foreign-and-security-policy-global-strategy.html (dostęp: 1.07.2023 r.).

Europejską Strategię Bezpieczeństwa z 2003 r.[116] Globalna strategia o tyle jest istotna, że określiła priorytety działań zewnętrznych UE, którymi są: bezpieczeństwo, odporność (ang. *resilience*) państw i społeczeństw, zintegrowane podejście do konfliktów i kryzysów, wspieranie współpracy regionalnej oraz zarządzanie globalne w XXI w. W strategii wskazano konieczność wzmocnienia cyberbezpieczeństwa w drodze zwiększenia odporności infrastruktury krytycznej i sieci przesyłowych, walki z cyberprzestępczością, a przede wszystkim poprzez włączenie kwestii związanych z tym obszarem w inne polityki unijne oraz zacieśnienie współpracy między państwami członkowskimi, a także USA i NATO. W literaturze zwraca się uwagę, że zaletą strategii było „zintegrowane podejście do realizacji powyższych priorytetów, łączące szerokie instrumentarium, jakim dysponuje Unia: od polityk handlowej, rozwojowej i migracyjnej po pomoc humanitarną czy zarządzanie kryzysowe"[117].

Jeżeli chodzi o bezpieczeństwo sieci i informacji przepisy UE skoncentrowane były początkowo na ochronie infrastruktury krytycznej. Efektem tzw. Zielonej Księgi w sprawie europejskiego programu ochrony infrastruktury krytycznej[118], w której Komisja wyodrębniła trzy typy zasobów infrastruktury (infrastruktura publiczna, prywatna i rządowa, procedury i ewentualnie osoby, które zarządzają infrastrukturą krytyczną oraz „miękkie cele", które obejmują imprezy masowe, jak: sport, rozrywka czy kultura), stała się dyrektywa Rady 2008/114/WE z 8.12.2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[119], będąca zasadniczym elementem europejskiego programu ochrony infrastruktury krytycznej (EPOIK). Celem dyrektywy było ustanowienie procedury rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej (EIK) oraz wspólne podejście do oceny potrzeb w zakresie poprawy ochrony takiej infrastruktury w celu lepszej ochrony ludności.

W świetle dyrektywy 2008/114/WE infrastruktura krytyczna oznacza składnik, system lub część infrastruktury, zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji. Jeżeli tego rodzaju sieci teleinformatyczne zlokalizowane są na terytorium państw członkowskich, a zakłócenie ich pracy lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie, to sieć tę zalicza się do europejskiej infrastruktury krytycznej. Włączenie przez polskiego ustawodawcę

[116] Strategia nie ma charakteru prawnie wiążącego. Rada Europejska na szczycie z 28.06.2016 r. nie zatwierdziła jej, lecz wyłącznie „przyjęła z zadowoleniem".

[117] M. Wróblewska-Łysik, *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, „Bezpieczeństwo Narodowe" 2016/1–4, s. 67 i n.

[118] COM(2005) 576 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52005DC0576 (dostęp: 1.07.2023 r.).

[119] Dz.Urz. UE L 345, s. 75.

systemów teleinformatycznych do infrastruktury krytycznej było w pełni zasadne. Nie rozwiązuje jednak problemów z ochroną tego rodzaju systemów przed cyberatakami z uwagi na generalny charakter ustawy z 26.04.2007 r. o zarządzaniu kryzysowym[120], pomijający specyfikę cyberprzestępczości.

Potrzebę odrębnego unormowania bezpieczeństwa systemów teleinformatycznych zasygnalizowała Komisja Europejska w komunikacie z 30.03.2009 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej pt. „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"[121], proponując plan działania oparty na pięciu filarach:

1) gotowości i zapobiegania,
2) zapewnienia odpowiednich mechanizmów wczesnego ostrzegania,
3) wzmocnienia unijnych mechanizmów obronnych dla infrastruktury krytycznej umożliwiających łagodzenie skutków i przywracanie zdolności operacyjnej,
4) współpracy międzynarodowej,
5) wspierania wdrażania dyrektywy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej w sektorze ICT.

Jednakże punktem wyjścia dla budowy strategii bezpieczeństwa cybernetycznego był przede wszystkim Program Sztokholmski – Otwarta i bezpieczna Europa dla Dobra i Ochrony Obywateli (2010/C 115/01)[122], który zwrócił uwagę m.in. na kwestię ochrony praw obywatela w społeczeństwie informacyjnym oraz konieczność ochrony prywatności w kontekście wymiany danych osobowych. W Programie Sztokholmskim Rada Europejska wezwała ponadto Radę, Komisję, Parlament Europejski i państwa członkowskie do opracowania i realizacji polityk gwarantujących bezpieczeństwo sieci i przesyłu informacji oraz wzmocnienia infrastruktury krytycznej w zakresie technologii informacyjno-komunikacyjnych. Efektem Programu Sztokholmskiego było położenie większego nacisku na bezpieczeństwo w cyberprzestrzeni, a zwłaszcza utworzenie Europejskiego Centrum do spraw Walki z Cyberprzestępczością przy Europolu[123].

W wyniku Programu Sztokholmskiego, a także rezolucji Parlamentu Europejskiego z 22.11.2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony[124], opracowana została Strategia bezpieczeństwa cybernetycznego Unii Europejskiej – otwarta,

[120] Dz.U. z 2023 r. poz. 122.

[121] COM(2009) 0149 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52009DC0149 (dostęp: 1.07.2023 r.).

[122] Dz.Urz. UE C 115 z 2010 r., s. 1.

[123] Szerzej A. Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013/8, s. 113 i n.

[124] 2012/2096(INI), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52012IP0457 (dostęp: 1.07.2023 r.).

bezpieczna i chroniona cyberprzestrzeń, sformułowana we Wspólnym Komunikacie Komisji z 7.02.2013 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów[125]. W strategii politykę obronną i rozbudowę zdolności w dziedzinie bezpieczeństwa cybernetycznego powiązano ze wspólną polityką bezpieczeństwa i obrony (WPBiO) i zarazem spójną międzynarodową polityką w zakresie cyberprzestrzeni dla Unii Europejskiej, łącząc te kwestie z rozbudową zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego i koniecznością osiągnięcia odporności na zagrożenia cybernetyczne. W strategii sformułowano jednocześnie podstawowe zasady bezpieczeństwa cybernetycznego, czyli zasady, którymi UE kieruje się przy opracowywaniu polityki w zakresie cyberbezpieczeństwa w UE i na arenie międzynarodowej. Do zasad tych zaliczono:

1) tożsamość podstawowych wartości UE w świecie realnym i cyfrowym,
2) poszanowanie i ochronę praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności, czyli podstawowych wartości UE,
3) dostęp dla wszystkich,
4) demokratyczne i efektywne zarządzanie wielostronne internetem oraz
5) wspólną odpowiedzialność za zapewnienie bezpieczeństwa w cyberprzestrzeni.

Zwieńczeniem tych działań był komunikat Komisji z 28.04.2015 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Europejska agenda bezpieczeństwa"[126]. Agendę oparto nie tylko na Strategii bezpieczeństwa cybernetycznego, ale także na istniejących strategiach sektorowych[127]. W Agendzie podkreślono wprost konieczność podejścia wielosektorowego do kwestii bezpieczeństwa. Dotyczy to także cyberprzestępczości, która w świetle komunikatu stanowi rosnące zagrożenie dla podstawowych praw obywateli i gospodarki, jak również dla skutecznego wprowadzenia jednolitego rynku cyfrowego.

[125] JOIN(2013) 1 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52013JC0001 (dostęp: 1.07.2023 r.).

[126] COM(2015) 185 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0185&from=DE (dostęp: 1.07.2023 r.).

[127] JOIN(2013) 1 final. Zob. Wspólny Komunikat do Parlamentu Europejskiego i Rady w sprawie aktualizacji strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i jej planu działania – Udoskonalona strategia Unii Europejskiej w zakresie bezpieczeństwa morskiego w obliczu zmieniających się zagrożeń morskich, Bruksela, 10.03.2023 r., JOIN(2023) 8 final; Strategia w zakresie zarządzania ryzykiem celnym, COM(2014) 527 final z 21.08.2014 r., https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52014DC0527 (dostęp: 1.07.2023 r.); Strategiczne ramy europejskiej współpracy w dziedzinie kształcenia i szkolenia na rzecz europejskiego obszaru edukacji i w szerszej perspektywie (2021–2030) (konkluzje Rady z 12.05.2009 r.), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021G0226(01) (dostęp: 1.07.2023 r.); Strategia UE na rzecz młodzieży na lata 2019–2027, Strategia UE na rzecz młodzieży | European Youth Portal (europa.eu); Intensyfikacja walki z przemytem papierosów i innymi formami nielegalnego handlu wyrobami tytoniowymi – Kompleksowa strategia UE (COM(2013) 324 final z 6.06.2013 r.). Agenda uzupełnia również bieżące inicjatywy, takie jak przegląd strategicznych kontroli eksportu (COM(2014) 244 final z 24.04.2014 r., https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52014DC0244, dostęp: 1.07.2023 r.).

Zwalczanie cyberprzestępczości uznano w Agendzie za jeden z trzech priorytetów działania organów UE w dziedzinie bezpieczeństwa, z uwagi przede wszystkim na fakt, że handel i bankowość przestawiają się na działalność online; to samo dotyczy infrastruktury krytycznej, która w coraz większym zakresie uzależniona jest od sieci teleinformatycznej. Europejska agenda bezpieczeństwa ukierunkowana jest w efekcie na globalne i skoordynowane podejście do problemu zagrożeń w cyberprzestrzeni. Tego rodzaju kompleksowe podejście do problematyki bezpieczeństwa cybernetycznego i cyberobrony potwierdziła też rezolucja Parlamentu Europejskiego z 23.11.2016 r. w sprawie wdrażania wspólnej polityki bezpieczeństwa i obrony (na podstawie sprawozdania rocznego Rady dla Parlamentu Europejskiego na temat wspólnej polityki zagranicznej i bezpieczeństwa)[128], w której podkreślono, że konflikty we współczesnym świecie rozgrywają się również w cyberprzestrzeni, zaś „z uwagi na swój charakter cyberbezpieczeństwo jest obszarem polityki, w którym najważniejsza jest współpraca i integracja, nie tylko między państwami członkowskimi UE, kluczowymi partnerami i NATO, ale także między różnymi podmiotami w obrębie społeczeństwa, ponieważ odpowiedzialność za tę kwestię nie ma jedynie charakteru wojskowego". Parlament podkreślił też potrzebę dalszego pogłębienia współpracy w zakresie cyberobrony i zagwarantowania pełnej cyberodporności w ramach WPBiO; wezwał też Radę do uwzględnienia cyberobrony jako integralnej części jej debat na temat obronności przy jednoczesnej budowie krajowych strategii cyberobrony.

Istotnym aktem programowym UE w zakresie cyberbezpieczeństwa był także komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego"[129], w którym zapowiedziano działania na rzecz utworzenia jednolitego rynku bezpieczeństwa cybernetycznego Europy, jako elementu wspólnego rynku. Barierą bowiem w rozwoju tego obszaru jest podział geograficzny podaży produktów i usług w dziedzinie bezpieczeństwa ICT, co utrudniało europejskim przedsiębiorstwom konkurowanie na poziomie europejskim i światowym, ograniczając jednocześnie wybór technologii bezpieczeństwa cybernetycznego dostępnych na wspólnym rynku. Problem ten wynikał stąd, że sektor bezpieczeństwa cybernetycznego w Europie rozwija się głównie dzięki popytowi ze strony administracji krajowej, w tym na potrzeby sektora obrony. Z uwagi na brak zaufania do rozwiązań oferowanych transgranicznie ograniczało to możliwość rozszerzenia działalności innowacyjnych przedsiębiorców, zwłaszcza małych i średnich przedsiębiorstw działających na rynkach produktów specjalistycznych i rynkach niszowych (np. rynkach systemów kryptograficznych) czy działających wprawdzie na rynkach ugruntowanych o względnie trwałej

[128] 2016/2067(INI), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016IP0440 (dostęp: 1.07.2023 r.).

[129] COM(2016) 410 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016DC0410 (dostęp: 1.07.2023 r.).

strukturze podmiotowej, to jednak działających na zupełnie nowych, nieutrwalonych jeszcze modelach.

Punktem zwrotnym na rzecz zintegrowanego podejścia do problematyki cyberbezpieczeństwa była jednak przede wszystkim Europejska agenda cyfrowa[130] będąca elementem przyjętej przez Komisję strategii „Europa 2020", która zakładała, że technologie informacyjno-komunikacyjne powinny pełnić podstawową funkcję rozwojową, jeśli Europa chce zrealizować swoje ambitne założenia do 2020 r. W strategii „Europa 2020"[131] wyraźnie zwrócono bowiem uwagę na znaczenie upowszechnienia szerokopasmowego internetu, co ma sprzyjać włączeniu społecznemu i konkurencyjności gospodarki UE. Efektem strategii było przyjęcie dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z 12.08.2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW[132] oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[133], tzw. dyrektywy NIS. Dyrektywa NIS znajduje zastosowanie bez uszczerbku dla dyrektywy 2008/114/WE, dyrektywy 2011/93/UE oraz dyrektywy 2013/40/UE. Wdrożenie dyrektywy NIS powinno nie tylko wspierać lepszą współpracę między organami ścigania i organami odpowiedzialnymi za bezpieczeństwo cybernetyczne, lecz także zapewniać budowanie zdolności w zakresie bezpieczeństwa cybernetycznego wśród właściwych organów państw członkowskich oraz w zakresie transgranicznego zgłaszania incydentów komputerowych. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa uczestniczy w działaniach podejmowanych przez UE w reakcji na kwestie związane z bezpieczeństwem cybernetycznym poprzez dążenie do zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji.

W dziesięcioletniej Europejskiej Agendzie Cyfrowej po raz pierwszy wskazano na kluczową rolę sprawczą ICT w osiąganiu celów Europy. W 2020 r. w drugiej pięcioletniej strategii cyfrowej – Kształtowanie cyfrowej przyszłości Europy – skupiono się na trzech kluczowych celach w dziedzinie cyfryzacji: technologia przynosząca korzyści ludziom, uczciwa i konkurencyjna gospodarka oraz otwarte, demokratyczne i zrównoważone społeczeństwo. W 2021 r. strategia ta została uzupełniona dziesięcioletnim cyfrowym kompasem – Europejska droga w cyfrowej dekadzie[134], zawierającym cztery cele cyfrowe, które mają zostać osiągnięte do 2030 r., a mianowicie:

[130] COM(2010) 245, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52010DC0245 (dostęp: 1.07.2023 r.).

[131] COM(2010) 2020, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52010DC2020 (dostęp: 1.07.2023 r.).

[132] Dz.Urz. UE L 218, s. 8.

[133] Dz.Urz. UE L 194, s. 1.

[134] Komunikat Komisji z 9.03.2021 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, COM(2021) 118 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0118 (dostęp: 1.07.2023 r.).

1) umiejętności cyfrowe co najmniej 80% wszystkich osób dorosłych,
2) korzystanie z usług w chmurze oraz dużych zbiorów danych i sztucznej inteligencji przez min. 75% przedsiębiorstw,
3) posiadanie przez wszystkie gospodarstwa domowe w UE łączności gigabitowej, przy zasięgu obszarów zaludnionych sieci 5G, a także
4) dostępność online wszystkich kluczowych usług publicznych.

W obowiązującej, drugiej Europejskiej agendzie cyfrowej na lata 2020–2030 skoncentrowano się na głębokich zmianach, których źródłem są technologie cyfrowe, roli usług i rynków cyfrowych oraz na nowych celach technologicznych i geopolitycznych UE. Opierając się na dwóch komunikatach strategicznych, a mianowicie: Kształtowaniu cyfrowej przyszłości Europy[135] oraz Cyfrowej dekadzie Europy – cele na 2030[136], Komisja przedstawiła konkretne działania, które podejmie, by wesprzeć tworzenie bezpiecznych i chronionych usług i rynków cyfrowych. Ponadto priorytetami na obecną dekadę są: rozwój kwantowych technologii obliczeniowych, rozwój technologii łańcucha bloków[137] łącznie z polityką handlową w tym zakresie[138], ukierunkowana na człowieka i godna zaufania sztuczna inteligencja (AI), półprzewodniki (Europejski akt o mikrochipach[139]), suwerenność cyfrowa, cyberbezpieczeństwo, łączność gigabitowa 5G i 6G, europejskie przestrzenie i infrastruktura danych, a także ustanowienie światowych standardów technologicznych.

Drugim z filarów Europejskiej agendy cyfrowej jest udostępnianie danych. Założeniem Agendy jest równowaga między swobodnym przepływem danych a zachowaniem prywatności, bezpieczeństwa, ochrony i norm. Chodzi o sposoby wykorzystywania i udostępniania danych nieosobowych na potrzeby opracowywania nowych opłacalnych technologii i modeli biznesowych. Komisja opracowała w lutym 2020 r. wraz z Białą księgą w sprawie sztucznej inteligencji Europejską strategię w zakresie danych[140], której podstawą jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi)[141], które obowiązuje od września 2023 r. Założeniem rozporządzenia jest zwiększenie dostępności danych i ich zdatności

[135] https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf (dostęp: 1.07.2023 r.).

[136] Komunikat Komisji z 9.03.2021 r., COM(2021) 118 final.

[137] Strategia Blockchain. Kształtowanie cyfrowej przyszłości Europy, https://digital-strategy.ec.europa.eu/pl/policies/blockchain-strategy (dostęp: 1.07.2023 r.).

[138] Blockchain: a forward-looking trade policy, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0528_EN.html (dostęp: 1.07.2023 r.).

[139] Commission Staff Working Document a Chips Act for Europe, 11.05.2022 r., SWD(2022) 147 final, https://ec.europa.eu/newsroom/dae/redirection/document/86690 (dostęp: 1.07.2023 r.).

[140] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów – Europejska strategia w zakresie danych, COM/2020/66 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0066 (dostęp: 1.07.2023 r.).

[141] Dz.Urz. UE L 152, s. 1–44.

do ponownego wykorzystywania i zarazem przekonanie użytkowników, że udostępnianie danych jest bezpieczne. Ponadto w 2022 r. Komisja opublikowała wniosek (projekt) rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)[142]. Jednocześnie Komisja zaproponowała deklarację europejskich praw i zasad cyfrowych[143], która ma na celu sprzyjanie ukierunkowanej na człowieka transformacji cyfrowej opartej na wartościach europejskich. Co istotne, dane zostały uznane za zasób o zasadniczym znaczeniu dla postępu społecznego, a zwłaszcza wzrostu gospodarczego, konkurencyjności, innowacji i tworzenia miejsc pracy. Priorytetem Komisji na lata 2019–2025 stało się utworzenie europejskiej przestrzeni danych. Stąd też zamiar stworzenia europejskiej chmury obliczeniowej na podstawie Gali-X, czyli otwartego, przejrzystego i bezpiecznego ekosystemu cyfrowego, w którym swobodny strumień danych i usług może być udostępniany, zestawiany i współdzielony w środowisku opartym na zaufaniu.

Celem Europejskiej agendy cyfrowej jest także stworzenie bezpieczniejszego jednolitego rynku cyfrowego, który zapewni ochronę podstawowych praw użytkowników i równe warunki działania dla przedsiębiorstw. Inicjatywa ta zaowocowała rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.09.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych)[144], które obowiązuje od 2.05.2023 r. oraz wnioskiem (projektem) aktu o rynkach cyfrowych[145]. Celem tych aktów jest unowocześnienie przepisów regulujących usługi cyfrowe w UE. W akcie o usługach cyfrowych zostały wyraźnie określone zasady odpowiedzialności i rozliczalności dostawców usług pośrednich, a w szczególności platform internetowych, takich jak media społecznościowe i platformy handlowe o rynkach cyfrowych, ustanowiono natomiast granice zachowań rynkowych przedsiębiorstw mających status strażników dostępu (*gatekeepers*), czyli przedsiębiorstw, które działają jako łącznik między dwiema lub większą liczbą grup użytkowników, np. między kupującymi i sprzedającymi (uzyskanie dostępu przez takie przedsiębiorstwo znacznej części użytkowników po jednej stronie danej platformy (np. kupujących), może skutkować pełną kontrolą nad dostępem do niektórych rynków lub klientów po drugiej stronie platformy np. sprzedawców, którzy mogą nie mieć wielkiego wyboru i mogą być zmuszeni do korzystania z infrastruktury strażników dostępu).

[142] COM/2022/68 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0068 (dostęp: 1.07.2023 r.).

[143] European Declaration on Digital Rights and Principles for the Digital Decade, 26.01.2022 r., COM(2022) 28 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A28%3AFIN (dostęp: 1.07.2023 r.).

[144] Dz.Urz. UE L 265, s. 1–66.

[145] Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15.12.2020 r., COM(2020) 825 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN (dostęp: 1.07.2023 r.).

Istotnym uzupełnieniem działań na rzecz jednolitego rynku cyfrowego są programy organów UE ukierunkowane na wdrożenie e-demokracji i e-administracji.

Wyrazem tych działań była rezolucja Parlamentu Europejskiego z 16.03.2017 r. w sprawie e-demokracji w Unii Europejskiej: potencjał i wyzwania[146] oraz komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Plan działania UE na rzecz administracji elektronicznej na lata 2016–2020. Przyspieszenie transformacji cyfrowej w administracji"[147]. W rezolucji Parlamentu Europejskiego zwrócono uwagę na korzyści płynące z e-demokracji, zdefiniowanej jako wsparcie i wzmocnienie demokracji tradycyjnej za pomocą ICT, która może uzupełniać i wzmacniać procesy demokratyczne przez dodanie elementów służących umocnieniu pozycji obywateli dzięki różnym działaniom online, obejmującym m.in. administrację elektroniczną, e-rządzenie, e-debaty, e-uczestnictwo i e-głosowanie. Rezolucja podkreśliła też, że celem e-demokracji jest propagowanie kultury demokratycznej, która ubogaca i wzmacnia praktyki demokratyczne przez zapewnianie dodatkowych środków zwiększających przejrzystość i uczestnictwo obywateli, a jej celem nie jest ustanowienie alternatywnego systemu demokratycznego ze szkodą dla demokracji przedstawicielskiej. Zwraca uwagę, że ICT przyczyniają się do rozwoju przestrzeni zaangażowania obywatelskiego i debaty publicznej, a jednocześnie podnoszą jakość i wzmacniają legitymację systemów demokratycznych. W rezolucji podnosi się także potrzebę ochrony prywatności i danych osobowych podczas korzystania z narzędzi e-demokracji oraz wspierania bezpieczniejszego środowiska internetowego, w szczególności w odniesieniu do bezpieczeństwa informacji i danych, w tym „prawa do bycia zapomnianym", a także potrzebę zapewnienia zabezpieczeń przed oprogramowaniem inwigilacyjnym oraz weryfikowalności źródeł.

Z kolei celem planu działania UE na rzecz e-administracji było usunięcie istniejących barier cyfrowych oraz powstrzymanie fragmentacji, która nastąpiła w związku z modernizacją administracji publicznych. Wdrożenie planu oparto na siedmiu zasadach:

1) domyślnej cyfrowości, co oznacza, że usługi administracji publicznych powinny być z założenia cyfrowe, przy zachowaniu innych kanałów dla osób nieposiadających dostępu do internetu z wyboru lub z konieczności;
2) jednorazowości, opartej na założeniu, że obywatele i przedsiębiorstwa podają administracji te same informacje tylko raz;
3) powszechności i dostępności publicznych usług cyfrowych;
4) otwartości i przejrzystości;
5) domyślnej transgraniczności, zapobiegającej krajowej fragmentacji, wspierając tym samym mobilność w ramach jednolitego rynku;

[146] 2016/2008(INI), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017IP0095 (dostęp: 1.07.2023 r.).

[147] COM(2016) 0179, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016DC0179 (dostęp: 1.07.2023 r.).

6) domyślnej interoperacyjności, co oznacza, że usługi publiczne powinny być opracowywane w taki sposób, aby funkcjonowały bezproblemowo w ramach jednolitego rynku i między strukturami organizacyjnymi, opierając się na swobodnym przepływie danych i usług cyfrowych w Unii Europejskiej;
7) niezawodności i bezpieczeństwa.

Wybór systemów i technologii, a także rozproszonych lub scentralizowanych projektów powinien być całkowicie zależny od preferencji i potrzeb administracji krajowych, ale musi być w pełni zgodny z wymogami w zakresie interoperacyjności. Nowe ramy interoperacyjności wdraża komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Europejskie ramy interoperacyjności – strategia wdrażania"[148]. Interoperacyjność stanowi kluczowy czynnik umożliwiający transformację cyfrową. Umożliwia bowiem podmiotom administracyjnym elektroniczną wymianę między sobą oraz z obywatelami i przedsiębiorcami istotnych informacji w sposób zrozumiały dla wszystkich stron. Dotyczy przy tym wszystkich dziedzin, które wpływają na świadczenie cyfrowych usług publicznych w UE. W komunikacie stwierdza się wprost, że „kwestie bezpieczeństwa i prywatności są głównymi źródłami obaw w odniesieniu do świadczenia usług użyteczności publicznej". W ocenie Komisji administracja publiczna powinna zapewnić wymogi bezpieczeństwa już na etapie projektowania, aby zabezpieczyć całą infrastrukturę informatyczną i jej moduły, gwarantując jednocześnie odporność usług na ataki, które mogą zakłócać ich funkcjonowanie oraz powodować kradzież lub uszkodzenie danych. Wymaga to wdrożenia nie tylko planów zarządzania ryzykiem, gwarantujących, że poziom bezpieczeństwa pozostaje proporcjonalny do stopnia ryzyka, lecz także planów ciągłości działania oraz planów awaryjnych i planów przywrócenia gotowości do pracy, umożliwiających jak najszybsze przywrócenie normalnego działania wszystkich funkcji systemu informatycznego. Wymaga to także korzystania z kwalifikowanych usług zaufania zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[149] (rozporządzenie eIDAS), aby zapewnić integralność, autentyczność, poufność i niezaprzeczalność danych.

W 2021 r. Komisja przedstawiła nową strategię UE w zakresie cyberbezpieczeństwa. Strategia ta, jako kluczowy element kształtowania cyfrowej przyszłości Europy, planu odbudowy dla Europy i strategii UE w zakresie unii bezpieczeństwa, wzmocnić ma zbiorową odporność Europy na zagrożenia dla cyberbezpieczeństwa i pomóc zapewnić wszystkim obywatelom i przedsiębiorstwom możliwość pełnego korzystania z wiarygodnych i sprawdzonych usług i narzędzi cyfrowych. Nowa strategia w zakresie

[148] COM(2017) 134, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0134 (dostęp: 1.07.2023 r.).
[149] Dz.Urz. UE L 257, s. 73, ze zm.

cyberbezpieczeństwa ma umożliwić również UE zwiększenie międzynarodowych norm i standardów w cyberprzestrzeni oraz zacieśnienie współpracy z partnerami na całym świecie w celu promowania globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni, opartej na praworządności, prawach człowieka, podstawowych wolnościach i wartościach demokratycznych.

Celem strategii UE w zakresie cyberbezpieczeństwa jest ochrona globalnego i otwartego internetu, a jednocześnie ustanowienie gwarancji nie tylko w zakresie bezpieczeństwa, ale także ochrony europejskich wartości i praw podstawowych ludności. Strategia zawiera konkretne propozycje inicjatyw regulacyjnych, inwestycyjnych i politycznych w trzech obszarach działań UE: odporności i suwerenności technologicznej, zdolności operacyjnej w celu zapobiegania, powstrzymywania i reagowania na incydenty cybernetyczne oraz rozwoju globalnej i otwartej cyberprzestrzeni dzięki zacieśnionej współpracy. Co istotne, UE jest zaangażowana we wspieranie nowej strategii w zakresie cyberbezpieczeństwa za pomocą bezprecedensowego poziomu inwestycji w transformację cyfrową UE na najbliższe siedem lat, za pośrednictwem kolejnego długoterminowego budżetu UE, w szczególności programu „Cyfrowa Europa" i programu „Horyzont Europa", a także planu odbudowy dla Europy. Celem jest doprowadzenie do łącznych inwestycji UE, państw członkowskich i przemysłu o wartości do 4,5 mld EUR, w szczególności w ramach Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji[150], a także zapewnienie, by znaczna część środków trafiała do MŚP.

Komisja dąży również do wzmocnienia przemysłowych i technologicznych zdolności UE w dziedzinie cyberbezpieczeństwa, w tym poprzez projekty wspierane wspólnie z budżetu UE i budżetów krajowych. Unia Europejska ma wyjątkową możliwość połączenia zasobów własnych w celu zwiększenia swojej strategicznej autonomii i wzmocnienia przywództwa w dziedzinie cyberbezpieczeństwa w całym cyfrowym łańcuchu dostaw (w tym zbioru danych i chmury obliczeniowej, technologii procesorów nowej generacji, ultrabezpiecznej łączności i sieci 6G) zgodnie ze swoimi wartościami i priorytetami. Efektem Strategii jest m.in. dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 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 (dyrektywa NIS 2)[151] oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557

[150] Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji, Wkład Komisji Europejskiej na temat spotkania przywódców w Salzburgu w dniach 19–20.09.2018 r., COM/2018/630 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018PC0630 (dostęp: 1.07.2023 r.).

[151] Dz.Urz. UE L 333, s. 80–152.