SECURO 2025, nr 12, ss. 68–80
ISSN: 2353-6330; e-ISSN: 2956-6665; https://securo.wnpism.uw.edu.pl

DOI: https://doi.org/10.33896/Securo.2025.12.6

IZABELA MARKIEWICZ

WIELOASPEKTOWOŚĆ POJĘCIA CYBERBEZPIECZEŃSTWA – ANALIZA DEFINICYJNA

The multifaceted concept of cybersecurity – a definitional analysis

Artykuł prezentuje analizę publikacji naukowych, aktów prawnych oraz norm branżowych dotyczących definicji cyberbezpieczeństwa. Celem artykułu jest identyfikacja przyczyn rozproszenia definicji oraz ocena skutków pluralizmu terminologicznego dla polityk publicznych i praktyk zarządzania ryzykiem. Analiza odpowiada na trzy pytania badawcze: (1) które komponenty definicyjne powtarzają się najczęściej, (2) jakie aspekty generują największe rozbieżności oraz (3) w jaki sposób brak konsensusu wpływa na kształtowanie polityk i praktyk zarządczych. Autorka stawia dwie tezy: (a) niejednoznaczność pojęcia wynika z dynamicznej ewolucji cyberprzestrzeni, (b) każdy z dyskursów uprzywilejowuje własne cele funkcjonalne. Zastosowana metodologia obejmuje systematyczny przegląd literatury oraz porównawczą analizę treści definicji pod kątem zakresu, celu i podmiotowości. Wyniki badania wskazują na istnienie wspólnego rdzenia pojęciowego w postaci ochrony poufności, integralności i dostępności zasobów cyfrowych, przy jednoczesnym zróżnicowaniu w zakresie skali podmiotowej i procesowej. W konkluzji zaproponowano trójwarstwowy model definicyjny (techniczny, organizacyjny, społeczny), stanowiący potencjalną ramę dla przyszłych strategii, legislacji oraz badań interdyscyplinarnych.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo, cyberprzestrzeń

The article presents an analysis of academic publications, legal acts and industry standards concerning the definition of cybersecurity. The aim of the article is to identify the reasons for the dispersion of definitions and to assess the effects of terminological pluralism on public policies and risk management practices. The analysis answers three research questions: (1) which

IZABELA MARKIEWICZ, absolwentka studiów I stopnia na kierunku bezpieczeństwo wewnętrzne (Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, Polska). Obecnie studentka studiów II st. na kierunku cyberbezpieczeństwo (Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, Polska).

ORCID: 0009-0006-4697-2296; e-mail: i.markiewic2@student.uw.edu.pl

definitional components recur most often, (2) which aspects generate the greatest discrepancies, and (3) how the lack of consensus affects the shaping of policies and management practices. The author puts forward two theses: (a) the ambiguity of the concept results from the dynamic evolution of cyberspace, (b) each discourse privileges its own functional goals. The methodology used includes a systematic review of the literature and a comparative analysis of the content of definitions in terms of scope, purpose and subjectivity. The results of the study indicate the existence of a common conceptual core in the form of protecting the confidentiality, integrity and availability of digital resources, with differences in terms of subjectivity and process scale. In conclusion, a three-layer definition model (technical, organisational, social) is proposed as a potential framework for future strategies, legislation and interdisciplinary research.

Keywords: cybersecurity, security, cyberspace

Wprowadzenie

Pojęcie „cyberbezpieczeństwo" zyskało popularność w dyskursie publicznym i naukowym pod koniec XX oraz w XXI wieku. Mimo to pozostaje terminem niejednoznacznym. W literaturze fachowej brak powszechnie akceptowanej definicji, która oddawałaby wielowymiarowy charakter cyberbezpieczeństwa[1]. Pojęcie to bywa definiowane bardzo różnorodnie – często subiektywnie, w sposób mało precyzyjny. Brak zwięzłej i uniwersalnej definicji cyberbezpieczeństwa może utrudniać rozwój badań interdyscyplinarnych oraz praktycznych działań, utrwalając podejście zawężone głównie do aspektów technicznych. Tymczasem cyberbezpieczeństwo dotyczy szeregu zagadnień wykraczających poza samą technologię – obejmuje kwestie organizacyjne, prawne, społeczne, militarne oraz inne, które powinny współdziałać w rozwiązywaniu złożonych wyzwań związanych z bezpieczeństwem. Trudności w zdefiniowaniu cyberbezpieczeństwa wynikają w dużej mierze z faktu, że termin ten łączy dwa odrębne komponenty pojęciowe: „bezpieczeństwo" oraz „cyberprzestrzeń". Każdy z nich sam w sobie jest pojęciem złożonym i wieloaspektowym. Bezpieczeństwo jest rozumiane rozmaicie – inaczej w ujęciu tradycyjnym (np. militarnym, państwowym), a inaczej we współczesnych, szerokich interpretacjach (np. bezpieczeństwo społeczne, informacyjne, personalne). Z kolei cyberprzestrzeń jest terminem stosunkowo nowym, ukształtowanym wraz z rozwojem technologii informacyjno-komunikacyjnych. Próby zdefiniowania cyberprzestrzeni napotykają na trudności związane z jej niematerialnym charakterem oraz dynamicznym rozwojem. W rezultacie cyberbezpieczeństwo jako połączenie tych dwóch elementów stało się terminem wieloznacznym, rozumianym zależnie od kontekstu – technicznego, prawnego, strategicznego czy społecznego[2].

---

1 G. Craigen, N. Diakun-Thibault, R. Purse, *Defining cybersecurity*, „Technology Innovation Management Review" 2014, vol. 4(10), https://timreview.ca/article/835 [10.05.2025].

2 M. Górny, *Wokół definicji cyberbezpieczeństwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, t. 27, s. 123–132, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-fd103150-f491-4be3-bb41--464606700dda [15.05.2025].

Wobec rosnącego znaczenia cyberbezpieczeństwa – zarówno dla funkcjonowania państw i organizacji międzynarodowych, jak i podmiotów prywatnych oraz codziennego życia obywateli – uzasadnione jest podjęcie refleksji nad definicją tego pojęcia. Jasne określenie, czym jest cyberbezpieczeństwo, ma konsekwencje praktyczne. Wpływa na kształtowanie strategii bezpieczeństwa, ram prawnych, polityk ochrony infrastruktury krytycznej, edukacji w zakresie bezpieczeństwa cyfrowego, a także prowadzenie badań naukowych w tym obszarze. Niniejszy artykuł podejmuje próbę uporządkowania zagadnienia definicji cyberbezpieczeństwa.

Pojęcie bezpieczeństwa

Termin „bezpieczeństwo" to jedno z kluczowych pojęć w naukach społecznych, studiach strategicznych i naukach o bezpieczeństwie. Pochodzi od łacińskiego *securitas* (od *sine cura* – „bez troski"), co wskazuje na stan wolny od obaw i zagrożeń. W ogólnym ujęciu oznacza brak zagrożenia. Klasyczne definicje skupiały się głównie na poziomie państwa i zagrożeniach militarnych, traktując bezpieczeństwo jako ochronę przed konkretnym niebezpieczeństwem. Współczesne ujęcia bezpieczeństwa ewoluowały w kierunku poszerzenia zakresu znaczeniowego. Po zakończeniu zimnej wojny nastąpiło przewartościowanie tradycyjnych koncepcji. Dostrzeżono, że bezpieczeństwo ma charakter wielowymiarowy i wielopoziomowy. B. Buzan w pracy *People, States and Fear. The National Security Problem in International Relations* odrzucił zasadę, że problemy bezpieczeństwa trzeba rozumieć tylko w ujęciu polityczno-militarnym. Wyróżnił pięć sektorów bezpieczeństwa: militarny, a także polityczny, ekonomiczny, społeczny oraz środowiskowy[3]. Wskazał, że bezpieczeństwo państwa zależy od stabilności w każdym z tych obszarów. Współcześnie bezpieczeństwo definiuje się nie tylko przez brak zagrożeń zewnętrznych, ale także przez zapewnienie warunków do swobodnego rozwoju i realizacji interesów zarówno państw, jak i społeczeństw czy jednostek. Przykładowo, Stanisław Koziej opisuje istotę bezpieczeństwa jako „zapewnienie egzystencji i swobody realizacji interesów aktorów w kontekście szans, wyzwań oraz ryzyk i zagrożeń"[4]. Takie ujęcie wskazuje, że bezpieczeństwo to nie tylko pasywna ochrona przed zagrożeniem, lecz także aktywny proces umożliwiający rozwój w warunkach stabilności i przewidywalności otoczenia. W literaturze polskiej podkreśla się również subiektywny wymiar bezpieczeństwa – rozróżnienie między bezpieczeństwem obiektywnym (rzeczywisty stan, w którym nie występują zagrożenia) a bezpieczeństwem subiektywnym (poczuciem bezpieczeństwa)[5]. Słownik terminów z zakresu bezpieczeństwa narodowego (Akademia Obrony Narodowej) definio-

[3] B. Buzan, *People, States and Fear. An Agenda for International Security Studies in the Post-Cold War Era*, Colchester 2009, s. 38.

[4] S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2, s. 19.

[5] T.W. Grabowski, *Bezpieczeństwo*, [w:] T.W. Grabowski (red.), *Bezpieczeństwo publiczne*, Kraków 2023, s. 13–35, https://doi.org/10.35765/slowniki.370 [16.05.2025].

wał bezpieczeństwo jako stan, który „daje poczucie pewności oraz gwarancję jego zachowania”[6], co podkreśla aspekt psychologiczny obok obiektywnego stanu braku zagrożeń[7]. Ta dualność pojmowania bezpieczeństwa (stan i poczucie) jest istotna również w kontekście cyberbezpieczeństwa, gdzie obiektywna ochrona systemów musi iść w parze z subiektywnym zaufaniem użytkowników do cyberprzestrzeni.

Podsumowując, pojęcie bezpieczeństwa przeszło ewolucję od wąskich, klasycznych definicji akcentujących wymiar militarny i przetrwanie państwa, do współczesnych, szerokich ujęć traktujących bezpieczeństwo jako stan i proces wielowymiarowej ochrony wartości oraz zapewniania warunków rozwoju. Bezpieczeństwo obecnie rozpatruje się na wielu poziomach (od indywidualnego, przez lokalny, narodowy, aż po międzynarodowy czy globalny) i w wielu kontekstach tematycznych. Ta złożoność sprawia, że bezpieczeństwo jest nierzadko określane mianem pojęcia zasadniczo spornego (*essentially contested concept*). Należy mieć świadomość semantycznej pojemności terminu „bezpieczeństwo”, przechodząc do analizy drugiego komponentu zagadnienia – cyberprzestrzeni.

Pojęcie cyberprzestrzeni jako wyzwanie definicyjne

Pojęcie „cyberprzestrzeń” początkowo funkcjonowało jako termin fantastycznonaukowy, spopularyzowany w latach 80. XX w. przez pisarza Williama Gibsona (powieść *Neuromancer*, 1984[8]), określający wirtualną rzeczywistość istniejącą w sieciach komputerowych[9]. Od tamtej pory termin ten przeniknął do języka potocznego i dyskursu naukowego, jednak uchwycenie jego precyzyjnego znaczenia okazało się trudne. Cyberprzestrzeń jest rzeczywistością niematerialną, stworzoną przez człowieka poprzez globalne połączenie systemów teleinformatycznych. Brakuje jej fizycznych granic – to raczej pewna konstrukcja wirtualna, obejmująca całość przetwarzanych i wymienianych w skali globalnej informacji oraz infrastrukturę komunikacyjną, która to umożliwia.

W literaturze przedmiotu spotkać można wiele definicji cyberprzestrzeni, akcentujących jej różne aspekty. J. Wasilewski, który zebrał najczęściej cytowane ujęcia tego terminu, wskazuje m.in., że cyberprzestrzeń bywa definiowana jako: „globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę informatyczną oraz zawarte w nich dane, w tym Internet, sieci telekomunikacyjne, systemy komputerowe, a także wbudowane w nie procesory i kontrolery”. W tym ujęciu cyberprzestrzeń to część środowiska informacyjnego obejmująca wszystkie połączone ze sobą systemy teleinformatyczne (*hardware*, *software*, dane). Inna definicja przytoczona przez J. Wasilewskiego określa cyberprzestrzeń zwięźlej jako „wirtualną przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery z całego świata” – a więc kon-

6 *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2008.

7 D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 19.

8 W. Gibson, *Neuromancer*, New York 1984.

9 H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Siedlce 2021, s. 219.

centruje się na samym fakcie istnienia globalnej wymiany danych w sieci. Kolejne ujęcie opisuje cyberprzestrzeń jako „interaktywną domenę stworzoną z cyfrowych sieci, wykorzystywaną do przechowywania, modyfikowania oraz przekazywania informacji; jej częścią jest Internet, ale obejmuje ona także inne systemy informacyjne obsługujące biznes, infrastrukturę i świadczenie usług”[10].

Mimo zróżnicowanych sformułowań, wspólnym mianownikiem tych definicji jest postrzeganie cyberprzestrzeni jako pewnej całości utworzonej przez połączone systemy teleinformatyczne na skalę globalną, jako wirtualnego środowiska informacji i komunikacji. W debatach akademickich pojawia się jednak pytanie, czy w definicjach cyberprzestrzeni uwzględniać jedynie komponent infrastrukturalno-techniczny czy także użytkowników i relacje społeczne. Część definicji skupia się wyłącznie na sieciach, systemach i przepływach danych (cyberprzestrzeń jako sieć urządzeń i oprogramowania). Inne kładą nacisk na aspekt społeczny wskazując, że cyberprzestrzeń tworzą również ludzie komunikujący się za pośrednictwem technologii oraz powiązania między nimi.

Jak zauważa J. Wasilewski, wybór podejścia definicyjnego ma konsekwencje dla rozumienia jej bezpieczeństwa. Jeśli zdefiniujemy cyberprzestrzeń wąsko, poprzez pryzmat infrastruktury informacyjnej, to również bezpieczeństwo cyberprzestrzeni utożsamimy głównie z ochroną technicznych elementów sieci. Natomiast włączenie do definicji użytkowników i relacji między nimi wymaga pojmowania bezpieczeństwa w cyberprzestrzeni w sposób dynamiczny i wieloaspektowy, łączący ochronę zarówno systemów, jak i ludzi oraz ich aktywności. Współczesne tendencje zdają się iść w kierunku definiowania cyberprzestrzeni szeroko, tak aby obejmowała zarówno infrastrukturę teleinformatyczną, jak i treści oraz interakcje zachodzące za jej pośrednictwem. Interesujący przykład definicji integrującej oba te komponenty znajduje się w Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej. Według tego dokumentu, cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (…), wraz z powiązaniami między nimi oraz relacjami z użytkownikami”[11]. Pełne brzmienie tej definicji zawiera rozbudowane objaśnienie, iż systemy teleinformatyczne to zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie oraz przesyłanie i odbieranie danych, zaś sama cyberprzestrzeń obejmuje również relacje między systemami a ich użytkownikami. W definicji tej wyraźnie zatem zaakcentowano dwuskładnikowy charakter cyberprzestrzeni: jest ona jednocześnie tworem technicznym (siecią systemów i połączeń) oraz społeczno-informacyjnym (relacje z użytkownikami, wymiana informacji).

Reasumując, cyberprzestrzeń jest pojęciem wielowymiarowym i trudnym do jednoznacznego zdefiniowania. Można ją ogólnie ująć jako całość globalnych zasobów informacyjnych wraz z infrastrukturą teleinformatyczną umożliwiającą ich przetwarzanie i wymianę, przy czym warto rozróżnić podejścia kładące nacisk na aspekt techniczny od

[10] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 5(9), s. 225–234.

[11] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015, s. 7.

tych uwzględniających także użytkowników i tworzone przez nich relacje społeczne *online*. Trudność definicyjna cyberprzestrzeni wynika więc zarówno z jej niematerialnej natury, jak i z dynamicznego rozwoju technologii. Definicje tworzone kilkanaście lat temu mogą dziś nie obejmować zjawisk takich jak np. internet rzeczy czy rozszerzona rzeczywistość, które poszerzają zakres cyberprzestrzeni.

Cyberbezpieczeństwo jako pojęcie złożone: przegląd definicji i podejść

Cyberbezpieczeństwo stanowi konglomerat dwóch omówionych wcześniej pojęć – bezpieczeństwa oraz nowoczesnej domeny cyberprzestrzeni. Intuicyjnie termin ten odnosi się do bezpieczeństwa w wymiarze cyber, czyli bezpieczeństwa systemów informacyjnych, sieci komputerowych, danych oraz wszelkich aktywności zachodzących w cyberprzestrzeni. Na pierwszy rzut oka wydaje się to dość klarowne, jednak w praktyce pojęcie cyberbezpieczeństwa bywa definiowane odmiennie. Można wskazać trzy główne podejścia definicyjne: (1) ujęcie prawne i instytucjonalne, (2) ujęcie techniczne (informatyczne), oraz (3) ujęcie strategiczne i ogólnosystemowe. Poniżej przedstawione zostaną przykłady definicji cyberbezpieczeństwa funkcjonujące w literaturze i dokumentach, z podziałem na wskazane podejścia, przy czym warto zaznaczyć, że granice między nimi nie są ostre, a niektóre definicje próbują być holistyczne.

Cyberbezpieczeństwo w ujęciu prawnym

W aktach prawnych często pojawia się potrzeba zdefiniowania cyberbezpieczeństwa na potrzeby stosowania przepisów. Definicje te mają charakter operacyjny, bywają węższe od definicji akademickich i koncentrują się na pewnych właściwościach systemów informacyjnych. Polska ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. wprowadziła definicję cyberbezpieczeństwa. Zgodnie z art. 2, cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług”[12]. Innymi słowy, w ujęciu ustawowym cyberbezpieczeństwo sprowadzone zostało do zdolności systemów teleinformatycznych do przeciwstawienia się incydentom, które mogłyby zagrozić podstawowym atrybutom bezpieczeństwa informacji. Taka definicja podkreśla aspekt techniczny. Mówi o systemach informacyjnych i ich odporności oraz odnosi się do klasycznych celów ochrony informacji. Warto przy tym zaznaczyć, że definicja ta ma charakter legalny. Obowiązuje na gruncie prawa polskiego i służy przede wszystkim określeniu zakresu stosowania przepisów o krajowym systemie cyberbezpieczeństwa.

Podobnie jest w prawodawstwie Unii Europejskiej. Rozporządzenie (UE) 2019/881 (tzw. Akt o cyberbezpieczeństwie, powołujący m.in. Agencję UE ds. Cyberbezpieczeństwa ENISA) definiuje cyberbezpieczeństwo jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych

[12] Dz.U. 2024 poz. 1077, ze zm.

osób przed cyberzagrożeniami”[13]. Z kolei nowa dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS 2)[14] również posługuje się zbliżonym ujęciem. Można zauważyć, że unijne podejście kładzie nacisk nie tylko na same systemy, ale i na działania ochronne. Definiuje cyberbezpieczeństwo poprzez czynności i środki podejmowane w celu zapewnienia bezpieczeństwa sieci, systemów i ich użytkowników. W pewnym sensie łączy więc element stanu (bezpieczne systemy wolne od incydentów) z elementem procesu (działania służące osiągnięciu tego stanu).

W polskiej literaturze przedmiotu spotyka się próby ujęcia definicyjnego godzącego perspektywę prawną z szerszym kontekstem. Przykładowo, w *Encyklopedii Bezpieczeństwa Narodowego* zaproponowano rozróżnienie dwóch poziomów rozumienia cyberbezpieczeństwa: szerokiego i wąskiego. W ujęciu szerokim cyberbezpieczeństwo to „stan i proces zapewniania bezpiecznego funkcjonowania podmiotu lub użytkownika wykorzystującego systemy informacyjne w cyberprzestrzeni”. Definicja ta ujmuje cyberbezpieczeństwo holistycznie jako kombinację stanu (bezpieczeństwo w cyber środowisku) oraz procesu (działania zapewniające ten stan) i wiąże je z ochroną działalności podmiotów korzystających z technologii informacyjnych. Jednocześnie autorzy encyklopedii wyróżniają ujęcie wąskie sprowadzające cyberbezpieczeństwo do odporności systemów informacyjnych na zakłócenia podstawowych cech informacji[15].

Podsumowując, w ujęciu prawnym cyberbezpieczeństwo jest najczęściej definiowane poprzez pryzmat ochrony systemów teleinformatycznych i informacji. W polskim i unijnym ustawodawstwie podkreśla się zapewnienie poufności, integralności, dostępności danych oraz ciągłości działania usług cyfrowych. Definicje te, choć precyzyjne, nie obejmują wszystkich wymiarów zagadnienia. Stąd też krytycy wskazują, że legalne definicje pomijają np. kontekst społeczny czy aspekt polityczny cyberbezpieczeństwa, i traktują cyberbezpieczeństwo wyłącznie jako kwestię technicznej odporności systemów.

Definicje techniczne i standardy (perspektywa informatyczna)

W dziedzinie nauk ścisłych i praktyce zarządzania bezpieczeństwem informacji funkcjonują definicje cyberbezpieczeństwa wypracowane w ramach standardów i norm branżowych. Przykładem jest międzynarodowa norma ISO/IEC 27032:2012 dotycząca zagadnień bezpieczeństwa w cyberprzestrzeni. W normie tej przyjęto definicję, wedle której cyber-

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 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).

[14] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

[15] S. Gwoździewicz, S. Sadowski, M. Szyłkowska, *Cyberbezpieczeństwo*, [w:] *Encyklopedia Bezpieczeństwa Narodowego*, https://encyklopedia.revite.pl/articles/view/123 [10.05.2025].

bezpieczeństwo to „ochrona prywatności, integralności i dostępności danych w cyberprzestrzeni”[16] oraz zapewnienie, że użytkownicy mogą polegać na systemach cyfrowych. Innymi słowy, w duchu norm ISO cyberbezpieczeństwo utożsamiane jest z utrzymaniem podstawowych właściwości bezpieczeństwa informacji (poufność, integralność i dostępność) w odniesieniu do systemów sieciowych. Bardziej rozbudowaną, a zarazem często cytowaną międzynarodową definicję proponuje Międzynarodowy Związek Telekomunikacyjny (ITU). W Rekomendacji ITU-T X.1205 (2008) podano, iż „cyberbezpieczeństwo jest zbiorem narzędzi, zasad, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i technologii, które mogą być wykorzystane do ochrony środowiska cybernetycznego oraz zasobów organizacji i użytkownika”[17]. Definicja ITU podkreśla, że celem cyberbezpieczeństwa jest zapewnienie osiągnięcia i utrzymania właściwości bezpieczeństwa zasobów w obliczu zagrożeń występujących w cyber środowisku. Można zauważyć, że ta definicja jest bardzo szeroka i kompleksowa. Obejmuje właściwie wszystkie możliwe elementy składające się na praktykę zabezpieczania cyberprzestrzeni: od narzędzi technicznych, przez polityki i procedury, po edukację i najlepsze praktyki. ITU-T X.1205 jest często punktem odniesienia w literaturze anglojęzycznej, stanowiąc próbę encyklopedycznego ujęcia cyberbezpieczeństwa.

Warto wspomnieć, że w literaturze przedmiotu dyskutuje się także nad relacją między pojęciami „cyberbezpieczeństwo” a „bezpieczeństwo informacji” (*information security*) czy „bezpieczeństwo systemów teleinformatycznych” (*IT security*). Niektórzy autorzy traktują cyberbezpieczeństwo jako pojęcie szersze, odnoszące się do całego cyfrowego ekosystemu (włącznie z elementami społecznymi i zjawiskami specyficznymi dla cyberprzestrzeni, jak cyberprzestępczość, cyberwojna itp.), podczas gdy bezpieczeństwo informacji miałoby dotyczyć głównie klasycznej ochrony danych i systemów przed zagrożeniami informatycznymi. Inni z kolei używają tych terminów zamiennie lub uznają cyberbezpieczeństwo za współczesny synonim bezpieczeństwa teleinformatycznego poszerzonego o nowe realia. Normy takie jak ISO 27032 starają się te relacje uporządkować wskazując, że cyberbezpieczeństwo obejmuje współdziałanie kilku dziedzin: bezpieczeństwa informacji, bezpieczeństwa sieci, bezpieczeństwa Internetu i ochrony infrastruktury krytycznej w kontekście teleinformatycznym. Jednak w praktyce terminologia bywa płynna i zależna od kontekstu, np. w dziale IT firmy często mówi się o *cybersecurity* mając na myśli po prostu bezpieczeństwo systemów komputerowych i danych, bez szerszych konotacji strategicznych. Reprezentatywną techniczną definicję podaje amerykański instytut NIST oraz związana z nim inicjatywa NICCS. Według NICCS (National Initiative for Cybersecurity Careers and Studies): „*cybersecurity* to zbiór technik, procesów i praktyk stosowanych w celu ochrony

16 ISO/IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*, International Organization for Standardization, https://www.iso.org/standard/44375.html [30.05.2025].

17 „*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets”* – International Telecommunication Union, Recommendation ITU-T X.1205: Overview of cybersecurity, ITU-T, Geneva 2008, s. 2 [tłum. aut.].

sieci, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem".

Podsumowując, w perspektywie technicznej i standardów cyberbezpieczeństwo jest przede wszystkim rozpatrywane jako dziedzina działań ochronnych zmierzających do zapewnienia poufności, integralności i dostępności informacji w cyberprzestrzeni. Definicje kładą nacisk na środki techniczne i organizacyjne służące zabezpieczaniu systemów przed cyberatakami, *malware*, nieautoryzowanym dostępem itp. W przeciwieństwie do definicji prawnych, które mają charakter syntetyczny i ogólny, definicje techniczne bywają albo bardzo krótkie (skupione na istocie ochrony zasobów cyfrowych) albo bardzo rozbudowane (próbujące wymienić wszystkie elementy ekosystemu bezpieczeństwa cybernetycznego, jak w przypadku ITU). W obu wypadkach jednak perspektywa jest dość inżynierska, koncentrująca się na bezpieczeństwie systemów i informacji.

Ujęcia strategiczne

Trzecie istotne podejście do definiowania cyberbezpieczeństwa ma charakter strategiczny. Wywodzi się z nauk o bezpieczeństwie, polityki bezpieczeństwa narodowego oraz studiów nad bezpieczeństwem międzynarodowym. Cyberbezpieczeństwo bywa postrzegane jako nowy wymiar bezpieczeństwa państwa, element polityki bezpieczeństwa wewnętrznego i międzynarodowego, zjawisko o znaczeniu społecznym i gospodarczym. Definicje tworzone przez ekspertów od strategii często starają się uchwycić wielopłaszczyznowość cyberbezpieczeństwa. Przykładowo, E. Żywucka-Kozłowska i R. Dziembowski stwierdzają, że termin cyberbezpieczeństwo jest rozumiany jako „system blokujący zagrożenia polegające na niszczeniu, zmienianiu oraz nieuprawnionym przejmowaniu danych"[18]. Taka definicja wprost wskazuje na zagrożenia cyberbezpieczeństwa i ujmuje cyberbezpieczeństwo jako system środków blokujących te zagrożenia. Niektórzy autorzy jak D. Lisiak-Felicka, M. Szmit zakładają wręcz, że w wyniku trudności z jednoznacznym zidentyfikowania czym jest przestrzeń cybernetyczna trudno byłoby dywagować o „możliwościach ochrony takiego hipotetycznego tworu"[19]. Dokumenty strategiczne często zawierają definicje lub przynajmniej opisy pojęcia cyberbezpieczeństwa. Wspomniana już Doktryna cyberbezpieczeństwa RP, opracowana przez Biuro Bezpieczeństwa Narodowego, zdefiniowała na własne potrzeby termin „bezpieczeństwo cyberprzestrzeni RP" 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".

Inny dokument – przyjęta w 2019 r. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 – również zawiera odwołanie do definicji ustawowej, ale jedno-

[18] E. Żywucka-Kozłowska, R. Dziembowski, *Wokół definicji cyberbezpieczeństwa*, „Cybersecurity and Law" 2023, nr 2, s. 123–132.

[19] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo…*, s. 49.

cześnie określa strategiczne cele i działania w obszarze cyberbezpieczeństwa, od edukacji kadr IT, przez rozwój zdolności obronnych, po współpracę międzynarodową. Podkreśla to, że w ujęciu strategicznym termin „cyberbezpieczeństwo" obejmuje nie tylko stan systemów, ale także całokształt działań państwa zmierzających do tego, aby cyberprzestrzeń była bezpieczna i służyła rozwojowi społecznemu oraz gospodarczemu.

Warto w tym miejscu zwrócić uwagę na jeszcze jeden aspekt. W literaturze anglojęzycznej czasem dokonuje się rozróżnienia terminologicznego między *cyber security* a *cyber safety*. To drugie pojęcie (cyberbezpieczeństwo jako *safety*) bywa definiowane jako stan bycia chronionym przed negatywnymi skutkami zdarzeń w cyberprzestrzeni, nie tylko ataków, ale wszelkich awarii, błędów, które mogą powodować szkody fizyczne, psychiczne, finansowe itp. Innymi słowy *cyber safety* odnosi się bardziej do bezpieczeństwa użytkownika (jego dobrostanu) w cyberprzestrzeni, podczas gdy *cyber security* tradycyjnie do bezpieczeństwa systemów przed zagrożeniami. W języku polskim oba te aspekty mieszczą się zazwyczaj w terminie „cyberbezpieczeństwo", stąd jego pojemność. Kwestia ta pokazuje, że nawet w obrębie języka angielskiego toczyły się dyskusje co dokładnie obejmuje *cyber security* – czy tylko kwestie ochrony systemów przed atakami (*security*), czy także zapewnienie, że korzystanie z nich nie wyrządzi nikomu krzywdy (*safety*). W praktyce jednak obecnie przeważa użycie terminu *cybersecurity*.

Podsumowując przegląd definicji, cyberbezpieczeństwo jest definiowane różnorodnie. W prawie, dość wąsko jako odporność systemów lub działania ochronne. W standardach technicznych jako praktyka zapewniania CIA (*confidentiality, integrity and availability*) danych i systemów. W ujęciach strategicznych jako złożony system zapewniania bezpieczeństwa państwa i obywateli w wymiarze cyber. Niektórzy badacze próbują łączyć te perspektywy. Przykładowo, D. Craigen zaproponował, że „cybersecurity to organizacja i zbiór zasobów, procesów i struktur używanych do ochrony cyberprzestrzeni oraz systemów cybernetycznych przed zdarzeniami, które powodują rozbieżność pomiędzy stanem zgodnym z prawem a stanem faktycznym własności"[20]. Jest to definicja trudna w odbiorze, ale zawiera ciekawą myśl – istotą cyberbezpieczeństwa jest zapobieganie sytuacjom, w których ktoś uzyskuje dostęp lub kontrolę nad zasobami informacyjnymi wbrew uprawnieniom. Podkreśla aspekt praw własności do informacji i ich ochrony. Propozycja ta nie zdobyła powszechnej popularności, lecz jest przykładem myślenia kategoriami prawnymi w definicji czysto technicznego zjawiska, co ponownie pokazuje wieloaspektowość pojęcia.

Wspólne elementy i różnice definicji

Analizując powyższe przykłady można wskazać na kilka wspólnych elementów obecnych w różnych definicjach cyberbezpieczeństwa: (1) ochrona zasobów cyfrowych przed zagrożeniami – wszyscy zasadniczo zgadzają się, że chodzi o zabezpieczenie systemów,

[20] D. Craigen, N. Diakun-Thibault, R. Purse, *Defining*..., s. 13–21.

sieci, danych przed działaniami niepożądanymi; (2) cele ochrony – często wymieniane są atrybuty, które ta ochrona ma zapewnić: poufność informacji, integralność danych, dostępność usług; (3) zakres podmiotowy – większość definicji odnosi się zarówno do poziomu technicznego jak i użytkowników; (4) środki i działania – wiele definicji, zwłaszcza kompleksowych, wylicza środki (technologie, polityki, procedury, edukacja) składające się na system cyberbezpieczeństwa.

Różnice definicyjne dotyczą głównie stopnia szerokości oraz akcentów. Definicje prawne są często węższe i bardziej skonkretyzowane. Definicje strategiczne bywają szersze, obejmując elementy organizacyjne, edukacyjne i społeczne. Niektóre definicje traktują cyberbezpieczeństwo jako stan, inne jako proces, a wiele jako kombinację stanu i procesu. Ponadto spotkać można różnice terminologiczne dotyczące np. tego, czy używać terminu bezpieczeństwo cyberprzestrzeni, czy cyberbezpieczeństwo (czasem są one używane zamiennie, ale niektórzy autorzy sugerują, że „bezpieczeństwo cyberprzestrzeni" może odnosić się bardziej do stanu, a „cyberbezpieczeństwo" do dziedziny działań). W praktyce jednak granica jest płynna i w języku polskim termin cyberbezpieczeństwo przyjął się powszechnie. Część definicji, zwłaszcza strategicznych, rozpatruje zwalczanie cyberprzestępczości jako element cyberbezpieczeństwa państwa, podczas gdy np. w ujęciu czysto technicznym bezpieczeństwo systemów nie obejmuje aspektów ścigania przestępstw. W rezultacie różne instytucje mogą inaczej rozumieć, co należy do zakresu cyberbezpieczeństwa. Dla jednych to głównie technologia i sieci, dla innych również ludzie, prawo i procedury.

Zakończenie

Przeprowadzone analizy wskazują jednoznacznie, że pojęcie „cyberbezpieczeństwo" jest wieloznaczne. Przyczyn tego stanu rzeczy jest kilka. Po pierwsze, nowość i dynamiczność zjawiska – cyberbezpieczeństwo wyłoniło się jako obszar zainteresowania dopiero w ostatnich dekadach, w ślad za rewolucją cyfrową. Dynamiczny rozwój technologii informatycznych, powstawanie nowych zagrożeń sprawiają, że zakres pojęciowy cyberbezpieczeństwa nieustannie ewoluuje. Definicje formułowane kilkanaście lat temu mogą dziś wydawać się niepełne, a za kolejne kilkanaście lat zapewne pojawią się nowe komponenty poszerzające zakres tego terminu. Po drugie, interdyscyplinarny charakter cyberbezpieczeństwa powoduje, że różne środowiska definiują je z własnej perspektywy. Informatycy skupią się na technicznych aspektach ochrony systemów, prawnicy na zdefiniowaniu ram prawnych i odpowiedzialności, specjaliści od stosunków międzynarodowych na aspektach konfliktu i współpracy między państwami w cyberprzestrzeni, socjologowie na bezpieczeństwie użytkowników i społeczeństwa informacyjnego. Każda z tych dyscyplin „zagospodarowała" termin cyberbezpieczeństwo we właściwy sobie sposób, stąd w literaturze taka mozaika definicji cząstkowych. Po trzecie, pewną rolę odgrywa lingwistyczna złożoność samego słowa „cyberbezpieczeństwo", która sugeruje pewną analogię do terminów typu „bezpieczeństwo narodowe" lub „bezpieczeństwo publiczne", co intuicyjnie kieruje myśle-

nie ku kwestii bezpieczeństwa państwa w obszarze cyber. Jednak w praktyce używa się go także w kontekście bezpieczeństwa pojedynczego systemu komputerowego czy ochrony prywatności jednostki *online*. Wielość skali powoduje dezorientację. Czasem jest mowa o cyberbezpieczeństwie globalnym, czasem o cyberbezpieczeństwie lokalnym. Brak doprecyzowania skali również przyczynia się do niejednoznaczności.

Konsekwencje braku jednoznacznej definicji cyberbezpieczeństwa są odczuwalne zarówno w teorii, jak i praktyce. W obszarze badawczym utrudnia to rozwój spójnej teorii cyberbezpieczeństwa. Trudno budować paradygmat naukowy, gdy podstawowe pojęcie jest różnie rozumiane przez różnych badaczy. Może to prowadzić do sytuacji, które D. Craigen i inni określili jako *impediment* – hamulec/przeszkoda postępu badań. Fragmentacja definicyjna sprzyja też powstawaniu silosów, np. specjaliści IT rozmawiają głównie między sobą a eksperci polityczni między sobą, używając tego samego słowa, lecz wkładając do niego inne treści, co prowadzi do odizolowania i utrudnia dialog interdyscyplinarny. W sferze praktycznej różnice w rozumieniu cyberbezpieczeństwa mogą powodować niejednoznaczności kompetencyjne, np. które instytucje mają się zajmować danymi aspektami, czy cyberbezpieczeństwo to tylko ochrona sieci teleinformatycznych czy także zwalczanie dezinformacji w Internecie? Brak klarowności może również prowadzić do luk w systemie bezpieczeństwa. Jeśli pewien obszar nie zostanie uznany za element cyberbezpieczeństwa, może zostać zaniedbany. Z drugiej strony, pojęcie o nadmiernie szerokim zakresie znaczeniowym bywa krytykowane jako kategoria pojemna o charakterze argumentacyjnym, wykorzystywana instrumentalnie do legitymizowania rozmaitych działań, od nadzoru nad przestrzenią cyfrową po praktyki cenzorskie, co w konsekwencji może generować istotne napięcia i obawy społeczne. Dlatego coraz częściej postulowane jest podejście bardziej precyzyjne, np. aby w dokumentach oficjalnych jasno określać zakres znaczeniowy używanych terminów związanych z cyberbezpieczeństwem. Niektórzy autorzy sugerują wręcz, że należy zaakceptować wielowymiarowość cyberbezpieczeństwa i mówić o nim w liczbie mnogiej (jako o zbiorze działań z różnych domen) lub każdorazowo dodawać kontekst (np. „cyberbezpieczeństwo techniczne", „cyberbezpieczeństwo narodowe" itp.).

Na zakończenie warto podkreślić, że choć definicje są ważne, to kluczowa jest świadomość ich zróżnicowania. Każdorazowo posługując się terminem „cyberbezpieczeństwo" należy brać pod uwagę kontekst i możliwe rozumienie przez odbiorcę. Artykuł ten miał na celu uwypuklenie trudności definicyjnych, co paradoksalnie jest pierwszym krokiem do ich przezwyciężenia. Zrozumienie, dlaczego trudno zdefiniować cyberbezpieczeństwo pozwala lepiej komunikować się ponad podziałami dyscyplinarnymi. Należy wyrazić nadzieję, że przyszłe prace badawcze, zarówno w języku polskim, jak i angielskim, będą stopniowo zbliżać nas do wypracowania bardziej spójnej i klarownej terminologii w obszarze cyberbezpieczeństwa, co przełoży się na skuteczniejsze działania na rzecz bezpiecznej cyberprzestrzeni.

Bibliografia

Artykuły naukowe

Craigen G., Diakun-Thibault N., Purse R., *Defining cybersecurity*, „Technology Innovation Management Review" 2014, vol. 4(10).

Górny M., *Wokół definicji cyberbezpieczeństwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, t. 27.

Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 5(9).

Żywucka-Kozłowska E., Dziembowski R., *Wokół definicji cyberbezpieczeństwa*, „Cybersecurity and Law" 2023, nr 2.

Druki zwarte

Buzan B., *People, States and Fear. An Agenda for International Security Studies in the Post-Cold War Era*, Colchester 2009.

Gibson W., *Neuromancer*, New York 1984.

Grabowski T.W., *Bezpieczeństwo*, [w:] T.W. Grabowski (red.), *Bezpieczeństwo publiczne*, Kraków 2023.

Gwoździewicz S., Sadowski S., Szyłkowska M., *Cyberbezpieczeństwo*, [w:] *Encyklopedia Bezpieczeństwa Narodowego*, https://encyklopedia.revite.pl/articles/view/123 [10.05.2025].

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

Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2008.

Wyrębek H., *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Siedlce 2021.