„dot.pl" - czasopismo Rejestru domeny .pl

Cyberbezpieczeństwo w cyberprzestrzeni. Zagrożenia i aspekty ochrony w dobie sztucznej inteligencji.

Dominika Grzybowska-Ganszczyk
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0002-6413-306X
E-mail: dominikagrzybowska@yahoo.com
Bartosz Głowacki
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0001-6453-2039
E-mail: b.glowacki@awf.katowice.pl
Janusz Mikitin
Uczelnia Nauk Społecznych, Polska
ORCID: https://orcid.org/0009-0006-6908-7193
E-mail: J.miki@wp.pl

Streszczenie

Postęp technologiczny XXI wieku przyniósł ludzkości ogromne możliwości w zakresie komunikacji, pracy, nauki oraz rozwoju społeczno-gospodarczego. Jednocześnie dynamiczny rozwój technologii cyfrowych doprowadził do pojawienia się nowych, coraz bardziej złożonych zagrożeń, które w istotny sposób wpływają na poczucie bezpieczeństwa jednostki oraz funkcjonowanie całych państw. Cyberprzestrzeń stała się jednym z kluczowych obszarów aktywności człowieka, co potwierdzają najnowsze raporty ENISA i IBM Security. Jedną z podstawowych potrzeb człowieka, według piramidy Abrahama Maslowa, jest potrzeba bezpieczeństwa –

Received: 30.10.2025
Accepted: 09.12.2025
Published: 09.12.2025

Cite this article as:
D. Grzybowska-Ganszczyk, B. Głowacki, J. Mikitin, "*Cyberbezpieczeństwo w cyberprzestrzeni. Zagrożenia i aspekty ochrony w dobie sztucznej inteligencji*"

DOT.PL, no. 1/ 2025, 10.60097/DOTPL/215385

Corresponding author:
Dominika Grzybowska-Ganszczyk, Akademia Wychowania Fizycznego w Katowicach, Polska

E-mail: dominikagrzybowska@yahoo.com

Copyright:
Some rights reserved
Publisher NASK

obecnie jednak jest ona coraz częściej naruszana w wyniku incydentów mających miejsce w cyberprzestrzeni.
Celem niniejszej pracy jest analiza zjawiska cyberzagrożeń oraz ich wpływu na bezpieczeństwo jednostkowe i zbiorowe. Artykuł przedstawia definicje i charakterystykę cyberprzestrzeni, omawia główne rodzaje zagrożeń cyfrowych, w tym zagrożenia rozwijające się wraz z postępem sztucznej inteligencji. W pracy zaprezentowano także aspekty prawne i instytucjonalne cyberbezpieczeństwa w Polsce i Unii Europejskiej, wskazując najważniejsze dokumenty, wśród których kluczową rolę odgrywa Dyrektywa NIS2. Rozwinięto także analizę roli czynnika ludzkiego, wskazując, iż – jak podkreśla raport Verizon – większość incydentów wynika z błędów użytkowników. W końcowej części omówiono przykłady incydentów cyberprzestępczych w Polsce oraz zaprezentowano rekomendacje wzmacniające odporność cyfrową społeczeństwa.
Opracowanie ma charakter analityczno-opisowy i podkreśla, że rozwój technologii, mimo licznych korzyści, niesie ze sobą także rosnące ryzyko utraty danych, prywatności i zaufania społecznego. Świadomość zagrożeń oraz edukacja w zakresie cyberbezpieczeństwa stanowią istotne składowe zapewnienia stabilności i bezpieczeństwa w świecie cyfrowym.

Słowa kluczowe: : cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenia, phishing, ransomware

Cybersecurity in cyberspace. Threats and protection aspects in the age of artificial intelligence.

Abstract

The technological progress of the twenty-first century has brought humanity immense opportunities in communication, work, education, and socio-economic development. At the same time, the dynamic growth of digital technologies has led to the emergence of new, increasingly complex threats that significantly affect both individual perceptions of security and the

functioning of entire states. Cyberspace has become one of the key domains of human activity, as confirmed by recent reports from ENISA and IBM Security. According to Abraham Maslow's hierarchy of needs, security is one of the fundamental human requirements; however, it is increasingly compromised by incidents occurring in cyberspace. The aim of this study is to analyze the phenomenon of cyber threats and their impact on individual and collective security. The article presents definitions and characteristics of cyberspace, discusses the main categories of digital threats—including those evolving alongside advances in artificial intelligence—and examines the legal and institutional aspects of cybersecurity in Poland and the European Union, highlighting key documents such as the NIS2 Directive. The analysis also addresses the human factor, emphasizing—as noted in the Verizon report—that most incidents stem from user errors. The final section discusses examples of cybercrime incidents in Poland and provides recommendations for strengthening the digital resilience of society.

This study adopts an analytical-descriptive approach and underscores that technological development, despite its numerous benefits, also entails growing risks of data loss, privacy breaches, and erosion of public trust. Awareness of threats and education in the field of cybersecurity are essential components for ensuring stability and security in the digital world.

Keywords: cybersecurity, cyberspace, cyber threats, phishing, ransomware

Wstęp

Rozwój technologii informacyjno-komunikacyjnych znacząco zmienił sposób funkcjonowania współczesnych społeczeństw. W literaturze anglojęzycznej podkreśla się, że cyberprzestrzeń stała się „kolejną domeną prowadzenia konfliktów”[1], a aktywność cyberprzestępcza wzrosła zarówno w skali, jak i w poziomie skomplikowania.

[1] M.D., Cavelty, T. Pulver, M., *Smeets, Ewolucja studiów nad cyberkonfliktami*, “International Affairs”, tom 100, numer 6, 2024, s. 2317–2339, https://doi.org/10.1093/ia/iiae175

Według raportu Microsoft Security z 2023 roku odnotowano wyraźny wzrost aktywności grup przestępczych oraz kampanii socjotechnicznych[2].

Postęp technologiczny w XXI wieku przyniósł liczne innowacje, które znacząco ułatwiają codzienne życie. Rozwój narzędzi teleinformatycznych umożliwia szybką komunikację, handel elektroniczny, zdalną edukację oraz efektywną administrację publiczną. Jednocześnie niesie ze sobą liczne zagrożenia, które mogą naruszać podstawowe potrzeby człowieka, w tym potrzebę bezpieczeństwa wskazywaną w piramidzie Maslowa. Cyberprzestrzeń daje ogromne możliwości rozwoju, ale każde zdarzenie o charakterze przestępczym w tej sferze może na trwałe zakłócić poczucie bezpieczeństwa użytkowników[3].

Zmiana sposobu korzystania z narzędzi cyfrowych była szczególnie widoczna w okresie pandemii COVID-19. Wówczas wiele zajęć edukacyjnych zostało przeniesionych na platformy e-learningowe i komunikatory grupowe, takie jak Microsoft Teams czy Zoom. Zakupy, które wcześniej odbywały się w tradycyjnych sklepach, przeniosły się na platformy internetowe, np. Allegro czy Zalando. Również administracja publiczna musiała szybko dostosować swoje funkcjonowanie do nowego środowiska cyfrowego, co zwiększyło ryzyko cyberzagrożeń. W tym czasie pojawiły się m.in. . złośliwe oprogramowania zawierające w nazwie słowa „COVID" lub „corona", wzrosła liczba oszustw internetowych i ataków phishingowych, a także intensyfikowały się działania szkodliwego oprogramowania skierowane przeciwko infrastrukturze krytycznej, np. szpitalom[4]. Analiza cyberbezpieczeństwa wymaga zrozumienia cyberprzestrzeni jako pojęcia oraz mechanizmów jej funkcjonowania. Chociaż cyberprzestrzeń nie posiada jednej spójnej definicji, literatura przedmiotu oraz dokumenty strategiczne – np. Doktryna cyberbezpieczeństwa RP – podkreślają znaczenie bezpieczeństwa w przestrzeni cyfrowej, wymieniając jej główne elementy: ochronę strategicznych zasobów państwa,

[2]Microsoft Digital Defense Report 2023. Redmond: Microsoft Security. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[3]Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, tom 27, nr 3, s. 393–410, https://doi.org/10.1108/ICS-07-2018-0080

[4]Kaspersky. (2021). COVID-19 and Cybersecurity Threats: Global Report. Moscow: Kaspersky Lab. Kaspersky Security Bulletin 2021 – Securelist; https://securelist.com/ksb-2021/

bezpieczeństwo przetwarzania informacji, funkcjonowanie sieci teleinformatycznych, ochronę informacji niejawnych i prawo do prywatności[5].

Bezpieczeństwo w cyberprzestrzeni jest kluczowe nie tylko dla państw i instytucji, ale również dla pojedynczych użytkowników, gdyż cyberzagrożenia stają się coraz bardziej złożone i trudne do przewidzenia. Dlatego istotne jest zarówno zrozumienie natury zagrożeń, jak i wdrażanie odpowiednich działań prewencyjnych, które pozwolą chronić informacje oraz infrastrukturę krytyczną w cyfrowym świecie[6].

Cyberprzestrzeń – charakterystyka i znaczenie

Wielu badaczy zwraca uwagę, że cyberprzestrzeń jest środowiskiem dynamicznym, pozbawionym granic fizycznych i podatnym na zakłócenia[7]. Obejmuje ona infrastrukturę teleinformatyczną, dane, usługi cyfrowe oraz relacje zachodzące pomiędzy użytkownikami. Doktryna Cyberbezpieczeństwa RP definiuje cyberprzestrzeń jako „przestrzeń przetwarzania informacji tworzona przez systemy teleinformatyczne i użytkowników". W literaturze i raportach podkreśla się, że ochrona infrastruktury krytycznej nabiera coraz większego znaczenia, ponieważ stała się jednym z głównych celów ataków ransomware – szczególnie w sektorach energii, transportu i ochrony zdrowia[8]. Analizę zagadnienia cyberprzestrzeni warto rozpocząć od samej definicji, co pozwoli na dalsze rozważania dotyczące bezpieczeństwa cyfrowego. Pojęcie cyberprzestrzeni rozwinęło się dzięki cybernetyce, jednak jego znaczenie i zakres ewoluowały w ciągu ostatnich kilkudziesięciu lat.

W literaturze przedmiotu często przywołuje się Williama Gibsona, autora powieści Burning Chrome, który określił cyberprzestrzeń jako „królestwo przestrzennych paradoksów". Od czasu wydania książki minęło ponad 30 lat, jednak wizja przedstawiona

[5] M. Carr, Public–private partnerships in national cyber-security strategies. International Affairs, 2016, 92(1),ss. 43–62, https://doi.org/10.1111/1468-2346.12504

[6] ENISA. (2023). ENISA Threat Landscape 2023. Athens: European Union Agency for Cybersecurity

[7] M. Foulon, G. Meibauer, *How cyberspace affects international relations: The promise of structural modifiers*. "Contemporary Security Policy", 2024, 45(3), ss. 426–458, https://doi.org/10.1080/13523260.2024.2365062

[8] Dragos Industrial Ransomware Analysis: Q4 2024 https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024

w powieści znalazła odzwierciedlenie w rzeczywistości – cyberprzestrzeń stała się integralną częścią życia codziennego[9].

Nie istnieje jedna, spójna definicja cyberprzestrzeni. Pojęcie to jest używane zarówno przez organizacje rządowe, polityków, jak i specjalistów ds. bezpieczeństwa. Najczęściej odnosi się do opisu zagrożeń w sieci oraz sposobów przeciwdziałania im. Przykłady definicji przedstawiają Paulina Tekielska i Łukasz Czekaj: „Cyberprzestrzeń to sieć powiązań między jednostkami sprzętowymi i centralnymi, umożliwiająca przesyłanie informacji oraz zapewniająca przestrzeń i środki do ich przetwarzania[10].”

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zastąpiła wcześniejsze ramy polityki i doktrynę Cyberbezpieczeństwa RP z 2015 roku. Strategia ta podkreśla, że cyberprzestrzeń to środowisko przetwarzania i wymiany informacji, tworzone przez systemy teleinformatyczne, użytkowników oraz relacje między nimi, a jej ochrona obejmuje zarówno sektor publiczny, prywatny, jak i wojskowy[11]. Z powyższych definicji wynika, że cyberprzestrzeń charakteryzuje się następującymi cechami: jest przestrzenią nieograniczoną, funkcjonuje dzięki sieciom teleinformatycznym oraz służy wymianie informacji. Bezpieczeństwo w cyberprzestrzeni stanowi wielowymiarowy obszar badań i praktyki, obejmujący zarówno aspekty technologiczne, jak i prawne oraz organizacyjne. Istotne komponenty tego bezpieczeństwa to ochrona strategicznych zasobów państwa, zapewnienie dokładności i wiarygodności przetwarzanych informacji, utrzymanie sprawnego funkcjonowania sieci teleinformatycznych oraz infrastruktury krytycznej, a także ochrona informacji niejawnych i ustawowo chronionych przy jednoczesnym poszanowaniu prawa do prywatności[12].

W literaturze podkreśla się, że cyberprzestrzeń jest środowiskiem szczególnie podatnym na zakłócenia, a jej ochrona wymaga zintegrowanego podejścia łączącego technologie, regulacje i edukację społeczną. Pomimo stosowania zaawansowanych systemów

---

[9] T.R., Andersen, (2019). *Cyberspace Revisited: A Radial Reading of William Gibson's "Burning Chrome".* "Journal of American Culture", vol. 42(2), ss. 121–136, https://doi.org/10.1111/jacc.13019

[10] B. Farrand, H. Carrapico, A. Turobov, *Nowa geopolityka cyberbezpieczeństwa UE: bezpieczeństwo, gospodarka i suwerenność*, „International Affairs", tom 100, numer 6, 2024, ss. 2379–2397, https://doi.org/10.1093/ia/iiae231

[11] Digital Skills and Jobs Platform. (2023). Poland – Cybersecurity Strategy of the Republic of Poland 2019–2024. Updated March 27, 2023. Retrieved from Digital Skills & Jobs EU

[12] B. Farrand, H. Carrapico, A. Turobov, (2024). *The new geopolitics of EU cybersecurity: security, economy and sovereignty.* „International Affairs", vol. 100(6), ss. 2379–2397. https://doi.org/10.1093/ia/iiae231

monitoringu i detekcji, pełne określenie wszystkich danych dotyczących cyberataków pozostaje trudne ze względu na anonimowość sprawców, transnarodowy charakter działań oraz złożoność incydentów, które często obejmują wiele warstw infrastruktury cyfrowej i wymagają współpracy międzynarodowej w zakresie ich przeciwdziałania (Farrand, Carrapico, & Turobov, 2024).

Cyberbezpieczeństwo można postrzegać jako system porządkujący struktury cyberprzestrzeni, którego celem jest zapewnienie stabilności i odporności środowiska cyfrowego. Do jego głównych zadań należy ochrona poufności informacji, zabezpieczenie danych i prywatności użytkowników, a także ochrona infrastruktury krytycznej przed zagrożeniami, w tym cyberterroryzmem. Istotnym elementem jest również utrzymanie ciągłości i sprawności zasobów niezbędnych do świadczenia e-usług, które stały się fundamentem funkcjonowania administracji publicznej, gospodarki oraz życia społecznego. W literaturze podkreśla się, że cyberbezpieczeństwo nie jest jedynie zbiorem technicznych procedur, lecz systemem integrującym aspekty prawne, organizacyjne i edukacyjne, co pozwala na skuteczniejsze przeciwdziałanie zagrożeniom i budowanie odporności instytucji oraz obywateli[13].

Cyberprzestrzeń jest dynamicznym środowiskiem, w którym rozwój technologii niesie zarówno ogromne możliwości, jak i nowe zagrożenia, wymagające odpowiednich działań ochronnych oraz prewencyjnych.

Klasyczne cyberzagrożenia

Phishing pozostaje najpowszechniejszą formą ataku cybernetycznego. Według danych ENISA ponad 80% incydentów inicjowanych jest poprzez manipulację socjotechniczną[14]. Podobną tendencję obserwuje Microsoft, wskazując na rosnący poziom profesjonalizacji kampanii phishingowych. Ransomware stał się natomiast najbardziej kosztownym

[13] E. Claessen, (2020). *Przekształcanie Internetu – wpływ sekurytyzacji infrastruktury internetowej na podejścia do zarządzania Internetem: przypadek Rosji i UE*. „Journal of Cyber Policy", vol. 5(1), ss.140–157. https://doi.org/10.1080/23738871.2020.1728356

[14]ENISA Threat Landscape 2024 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

rodzajem ataku – IBM X-Force wskazuje, że średni koszt incydentu w 2023 roku przekroczył 1,5 mln USD[15].

1. **Charakterystyka cyberzagrożeń**

Cyberzagrożenia są konsekwencją rosnącej roli technologii w życiu codziennym oraz funkcjonowaniu państw i organizacji. Ich głównymi celami mogą być: kradzież środków pieniężnych, zakłócenie pracy firm, szpiegostwo i nielegalne pozyskiwanie informacji.

Każda informacja w świecie cyfrowym podlega różnym zagrożeniom. Incydent bezpieczeństwa to zdarzenie zagrażające poufności, integralności lub dostępności danych. W kontekście ochrony informacji kluczowe jest stosowanie działań prewencyjnych, ponieważ lepiej zapobiegać niż naprawiać skutki ataku.

2. **Najczęściej występujące cyberzagrożenia**

Cyberzagrożenia przybierają różnorodne formy i obejmują zarówno klasyczne, jak i coraz bardziej zaawansowane techniki ataków. Do najczęściej spotykanych należą złośliwe oprogramowanie (malware), którego celem jest uszkodzenie urządzenia lub przejęcie informacji, a także phishing – polegający na wyłudzaniu danych poprzez fałszywe wiadomości e-mail lub strony internetowe. Szczególnie niebezpieczną odmianą jest spear phishing, w którym atakujący podszywa się pod osobę znaną ofierze. Istotnym zagrożeniem pozostaje również atak typu Man-in-the-Middle (MitM), polegający na przechwyceniu komunikacji między dwiema stronami. Do kategorii szkodliwego oprogramowania zaliczają się m.in. . konie trojańskie, które podszywają się pod legalne aplikacje w celu infekowania systemu, oraz ransomware, szyfrujące dane ofiary i żądające okupu za ich odblokowanie. Wśród poważnych incydentów bezpieczeństwa wymienia się także ataki typu Denial of Service (DoS/DDoS), polegające na przejęciu funkcji wielu urządzeń w celu zakłócenia działania systemu docelowego[16].

Coraz częściej zagrożenia dotyczą urządzeń Internetu Rzeczy (IoT), takich jak kamery czy czujniki, które często działają na przestarzałym oprogramowaniu. Do typowych incydentów zalicza się także wycieki danych – obejmujące kradzież informacji

[15]Microsoft. (2024). Microsoft Digital Defense Report 2024. Security Insider. Retrieved December 7, 2025, from https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024; ss. 27-66.

[16] Por. J. R. Vacca (red.), Computer and Information Security Handbook, 3rd Edition, Elsevier, 2017; ss.215

osobowych, finansowych lub poufnych – oraz złośliwe aplikacje mobilne, instalowane w celu uzyskania dostępu do wrażliwych danych użytkownika.

Dodatkowo raporty wskazują na inne formy zagrożeń między innymi: zagrożenia wewnętrzne wynikające z działań pracowników, ingerencje fizyczne, uszkodzenia lub kradzieże systemów, kradzież kryptowalut[17].

3. Współczesne tendencje

Wraz z rozwojem technologii rośnie liczba potencjalnych celów cyberataków, a grupy przestępcze coraz bardziej specjalizują się w ich planowaniu. Coraz częściej obserwuje się współpracę pomiędzy organizacjami cyberprzestępczymi oraz udostępnianie narzędzi w formie „gotowych komponentów", co umożliwia osobom o ograniczonym doświadczeniu prowadzenie działalności cyberprzestępczej[18].

Zagrożenia związane ze sztuczną inteligencją

Rozwój sztucznej inteligencji (AI) otworzył nowe możliwości w zakresie automatyzacji procesów, analizy danych oraz wspierania decyzji strategicznych. Jednocześnie jednak pojawiły się nowe formy zagrożeń, które znacząco komplikują krajobraz cyberbezpieczeństwa. Nowoczesne modele sztucznej inteligencji umożliwiają generowanie niezwykle przekonujących treści, takich jak deepfake, które – jak wskazuje Europol – znacząco zwiększają skuteczność oszustw finansowych. Technologia ta wykorzystywana jest nie tylko do manipulacji wizerunkiem osób publicznych, lecz także w atakach socjotechnicznych, gdzie fałszywe nagrania audio lub wideo służą do wyłudzania danych bądź środków finansowych[19].

Szczególnie groźnym zjawiskiem w obszarze sztucznej inteligencji jest adversarial machine learning, czyli manipulowanie danymi treningowymi lub wejściowymi modeli w celu uzyskania błędnych wyników. Ataki tego typu mogą prowadzić do kompromitacji systemów bezpieczeństwa – przykładowo poprzez błędną klasyfikację obrazów w

[17] J. R. Vacca, (Ed.). (2017). Computer and information security handbook (3rd ed.). Elsevier; s. 233.

[18] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, X. (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*. "Computers & Security", vol. 105, ss.2-4. https://doi.org/10.1016/j.cose.2021.102248;

[19] Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol Innovation Lab. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes; ss. 14-20.

systemach monitoringu czy generowanie fałszywych alarmów w systemach wykrywania intruzów[20].

Wraz z rozwojem technologii sztucznej inteligencji pojawiają się nowe formy zagrożeń, w tym ataki wspierane przez AI, które stają się coraz bardziej autonomiczne i trudniejsze do wykrycia. Modele te mogą adaptować swoje strategie w czasie rzeczywistym, co znacząco utrudnia ich neutralizację przez tradycyjne systemy bezpieczeństwa[21].

Do największych zagrożeń związanych ze sztuczną inteligencją zalicza się manipulację obrazem, dźwiękiem i tekstem w postaci deepfake oraz innych treści generatywnych, które mogą być wykorzystywane do oszustw finansowych, dezinformacji czy szantażu. Istotnym problemem pozostaje również adversarial machine learning, polegający na celowym wprowadzaniu błędów do danych treningowych lub wejściowych, co prowadzi do kompromitacji modeli. Coraz większe znaczenie mają także autonomiczne ataki AI-powered, w których systemy uczą się samodzielnie i adaptują swoje strategie, przez co stają się trudniejsze do wykrycia przez klasyczne narzędzia bezpieczeństwa. Wreszcie, sztuczna inteligencja znajduje zastosowanie w cyberprzestępczości zorganizowanej, gdzie algorytmy wspierają automatyzację phishingu, ransomware czy ataków DDoS[22].

Aspekty prawne i instytucjonalne

Cyberbezpieczeństwo w Europie i Polsce opiera się na rozbudowanych regulacjach prawnych oraz strukturach instytucjonalnych, które mają na celu zwiększenie odporności państw i organizacji na rosnące zagrożenia cyfrowe.

Najważniejszym dokumentem regulującym kwestie bezpieczeństwa w Unii Europejskiej jest Dyrektywa NIS2, której celem jest zwiększenie odporności sektorów kluczowych i ważnych[23].

[20]B. Biggio, F. Roli, (2018). *Wild patterns: Ten years after the rise of adversarial machine learning*.“Pattern Recognition”, vol. 84, ss. 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

[21] L. Huang, A. D. Joseph, B. Nelson, B. I. P. Rubinstein, J. D. Tygar, (2020). *Adversarial machine learning: A survey of attacks on machine learning systems*. “ACM Computing Surveys”, vol. *53*(3), ss. 1–43.

[22]M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, B. et al.,(2018*). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint arXiv:1802.07228; s.12

[23] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. “International Cybersecurity Law Review”, vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4; s.210

Dyrektywę NIS2 uzupełnia Cybersecurity Act, który ustanawia europejski system certyfikacji bezpieczeństwa, wzmacniając zaufanie do usług cyfrowych i produktów ICT. W Polsce kluczowe znaczenie ma natomiast ustawa o krajowym systemie cyberbezpieczeństwa, która precyzuje zadania CSIRT GOV, CSIRT MON oraz CSIRT NASK, zapewniając koordynację działań w zakresie reagowania na incydenty i podnoszenia odporności infrastruktury krytycznej[24].

1. **Regulacje unijne**

Regulacje unijne w obszarze cyberbezpieczeństwa obejmują szereg kluczowych dokumentów. Dyrektywa NIS (UE 2016/1148) nakłada na państwa członkowskie obowiązki dotyczące bezpieczeństwa sieci i systemów informatycznych, wymagając m.in. . opracowania krajowej strategii bezpieczeństwa, powołania zespołów reagujących na incydenty (CSIRT) oraz ustalenia zasad zgłaszania incydentów przez operatorów usług kluczowych i cyfrowych. Strategia Cyberbezpieczeństwa UE, aktualizowana w latach 2017, 2020 i 2023, koncentruje się na odporności, prewencji i ochronie, umożliwia korzystanie z wiarygodnych komponentów cyfrowych oraz wzmacnia zdolność państw członkowskich do przeciwdziałania cyberzagrożeniom. Uzupełnieniem tych działań jest Cybersecurity Act (2019), który wprowadza europejski system certyfikacji bezpieczeństwa, mający na celu podniesienie zaufania do usług cyfrowych i produktów ICT[25].

2. **Regulacje krajowe – Polska**

W Polsce podstawowym aktem prawnym regulującym kwestie bezpieczeństwa cyfrowego jest ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która określa ramy prawne i instytucjonalne dla działań związanych z ochroną cyberprzestrzeni. Dokument ten wskazuje m.in. . na funkcjonowanie trzech zespołów CSIRT: CSIRT GOV, któremu przewodniczy szef Agencji Bezpieczeństwa Wewnętrznego;

[24]European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, ss. 15–69. http://data.europa.eu/eli/reg/2019/881/oj;

[25] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. "International Cybersecurity Law Review", vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4

CSIRT MON, przyporządkowany Ministrowi Obrony Narodowej; oraz CSIRT NASK, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Rozwiązania te mają na celu zapewnienie skutecznej koordynacji działań w zakresie reagowania na incydenty i podnoszenia odporności krajowej infrastruktury krytycznej[26].

Obowiązki operatorów infrastruktury kluczowej obejmują m.in.: szacowanie ryzyka, wdrażanie środków technicznych, gromadzenie informacji o podatności systemu, prowadzenie działań związanych z incydentami oraz zapewnienie skutecznej komunikacji w przypadku zagrożeń[27].

Najbardziej zaawansowane systemy ochrony danych mogą okazać się nieskuteczne, jeśli użytkownicy nie przestrzegają podstawowych zasad bezpieczeństwa lub stają się ofiarami manipulacji psychologicznej. Do najczęstszych przyczyn udanych cyberataków należą korzystanie z prostych lub powtarzalnych haseł, brak aktualizacji urządzeń i oprogramowania, ignorowanie zasad ograniczonego zaufania wobec wiadomości e-mail czy linków oraz nieświadome udostępnianie danych osobowych w mediach społecznościowych. Z kolei zasady ograniczające ryzyko obejmują stosowanie silnych i unikalnych haseł wraz z weryfikacją dwuetapową, regularne aktualizacje systemów i aplikacji, używanie programów antywirusowych i narzędzi szyfrujących, zachowanie ograniczonej ufności w kontaktach online, weryfikację podejrzanych wiadomości oraz ochronę prywatności w mediach społecznościowych i komunikatorach[28].

Wnioski i podsumowanie

Cyberbezpieczeństwo stanowi obecnie jeden z najważniejszych filarów funkcjonowania państwa i społeczeństwa informacyjnego. Współczesne zagrożenia – od klasycznych form ataków, takich jak phishing czy ransomware, po nowoczesne wyzwania

[26] A. Klimkiewicz, (2020). Krajowy system cyberbezpieczeństwa – założenia i praktyka. Przegląd Prawa i Administracji, vol. 121, ss. 83–96. Wrocław: Uniwersytet Wrocławski. https://doi.org/10.19195/0137-1134.121.6

[27] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. "International Cybersecurity Law Review", vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4

[28] M. Abidin, A. Nawawi, A. Salin, (2019), *Bezpieczeństwo danych klientów i kradzież: doświadczenie malezyjskiej organizacji.* „Information and Computer Security", tom 27 nr 1, ss. 81–100, https://doi.org/10.1108/ICS-04-2018-0043

związane ze sztuczną inteligencją – pokazują, że bezpieczeństwo cyfrowe jest procesem dynamicznym i wielowymiarowym. Wymaga ono nie tylko stosowania zaawansowanych technologii ochronnych, lecz także odpowiednich regulacji prawnych oraz szeroko zakrojonej edukacji społecznej[29]. Rozwój sztucznej inteligencji tworzy zarówno nowe szanse, jak i ryzyka. Z jednej strony umożliwia skuteczniejsze wykrywanie incydentów oraz automatyzację działań obronnych, z drugiej – generuje nowe typy zagrożeń, takie jak deepfake czy adversarial machine learning. Technologie te mogą być wykorzystywane zarówno w celu poprawy bezpieczeństwa, jak i w działaniach przestępczych, co czyni cyberprzestrzeń obszarem szczególnie podatnym na dynamiczne i trudne do przewidzenia wyzwania[30]. W literaturze podkreśla się, że systemy sztucznej inteligencji mogą znacząco zwiększać odporność organizacji poprzez wspieranie procesów wykrywania incydentów i automatyzację działań obronnych. Jednocześnie wskazuje się, iż wymagają one odpowiednich ram prawnych i etycznych, które ograniczałyby ryzyko nadużyć oraz zapewniały zgodność z zasadami odpowiedzialnego wykorzystania technologii[31].

Regulacje prawne, takie jak Dyrektywa NIS2 oraz Cybersecurity Act, stanowią fundament dla budowania odporności instytucji publicznych i prywatnych w Europie. Dokumenty te rozszerzają zakres obowiązków w zakresie cyberbezpieczeństwa, obejmując nowe sektory i podmioty, a także wprowadzają europejski system certyfikacji bezpieczeństwa, który ma na celu podniesienie zaufania do usług cyfrowych i produktów ICT. W literaturze podkreśla się, że regulacje te są kluczowe dla zapewnienia wysokiego poziomu ochrony infrastruktury krytycznej oraz dla harmonizacji działań państw członkowskich[32].

Wdrażanie regulacji dotyczących cyberbezpieczeństwa w państwach członkowskich, w tym w Polsce, pokazuje, że skuteczna ochrona cyberprzestrzeni wymaga współpracy

---

[29] A. Piazza, S. Vasudevan, M. Carr, *Cyberbezpieczeństwo na uniwersytetach w Wielkiej Brytanii: mapowanie (lub zarządzanie) udostępnianiem informacji wywiadowczych o zagrożeniach w sektorze szkolnictwa wyższego*,"Journal of Cybersecurity", tom 9, numer 1, 2023, tyad019, s. 214; https://doi.org/10.1093/cybsec/tyad019

[30] M. Brundage et al., (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint arXiv:1802.07228. https://arxiv.org/abs/1802.07228

[31] L. Floridi et al., (2018). *AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*. "Minds and Machines", vol. 28(4), ss. 689–707. https://doi.org/10.1007/s11023-018-9482-5

[32] J. Ruohonen, (2024). *A systematic literature review on the NIS2 Directive*. arXiv preprint arXiv:2412.08084. s.6 https://arxiv.org/abs/2412.08084

międzyinstytucjonalnej oraz integracji działań na poziomie lokalnym, narodowym i europejskim. Tylko skoordynowane podejście, obejmujące zarówno instytucje publiczne, jak i prywatne, pozwala na budowanie odporności wobec rosnącej liczby zagrożeń cyfrowych oraz zapewnia harmonizację standardów bezpieczeństwa w całej Europie[33]. Nie można jednak zapominać o czynniku ludzkim. Najbardziej zaawansowane systemy ochrony danych mogą okazać się nieskuteczne, jeśli użytkownicy nie stosują podstawowych zasad bezpieczeństwa lub stają się ofiarami manipulacji psychologicznej. W literaturze podkreśla się, że to właśnie zachowania i nawyki użytkowników – takie jak korzystanie ze słabych haseł, brak ostrożności wobec wiadomości e-mail czy podatność na socjotechnikę – stanowią jeden z głównych czynników ryzyka w obszarze cyberbezpieczeństwa[34].

Podsumowując, cyberbezpieczeństwo należy traktować jako proces ciągły, wymagający integracji działań prawnych, technologicznych i edukacyjnych. Tylko w ten sposób możliwe jest zapewnienie odporności państw, instytucji i obywateli na rosnące zagrożenia w cyberprzestrzeni. Jak wskazują Kasper i Vernygora (2021), Unia Europejska stopniowo buduje swoją strategiczną narrację w obszarze cyberbezpieczeństwa, łącząc elementy odporności, odstraszania i współpracy międzynarodowej. W tym kontekście edukacja społeczna oraz podnoszenie świadomości użytkowników stają się równie istotne jak regulacje prawne i innowacyjne technologie, ponieważ dopiero ich wspólne zastosowanie pozwala na skuteczne wzmacnianie odporności cyfrowej w dynamicznie zmieniającym się środowisku globalnym[35].

Bibliografia

1. Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Bezpieczeństwo danych klientów i kradzież: doświadczenie malezyjskiej organizacji. Information & Computer Security, 27(1), 81–100. https://doi.org/10.1108/ICS-04-2018-0043
2. Andersen, T. R. (2019). Cyberspace revisited: A radial reading of William Gibson's "Burning Chrome". Journal of American Culture, 42(2), 121–136. https://doi.org/10.1111/jacc.13019

[33] M. Carr, (2021). *The EU's cybersecurity strategy: A framework for resilience*. "Journal of Cyber Policy", vol. 6(1), ss. 1–20. https://doi.org/10.1080/23738871.2021.1884802

[34] L. Hadlington, (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. "Heliyon", vol. 3(7), e00346, ss. 489–497. https://doi.org/10.1016/j.heliyon.2017.e00346

[35] A. Kasper, V. A. Vernygora, (2021). *Cybersecurity of the EU: A strategic narrative of a cyber power or a confusing policy for a local common market?* "Cuadernos Europeos de Deusto", vol. 65(2021), ss. 29–71 https://doi.org/10.18543/ced-65-2021pp

3. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023
4. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228. https://arxiv.org/abs/1802.07228
5. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504
6. Carr, M. (2021). The EU's cybersecurity strategy: A framework for resilience. Journal of Cyber Policy, 6(1), 1–20. https://doi.org/10.1080/23738871.2021.1884802
7. Claessen, E. (2020). Przekształcanie internetu – wpływ sekurytyzacji infrastruktury internetowej na podejścia do zarządzania internetem: przypadek Rosji i UE. Journal of Cyber Policy, 5(1), 140–157. https://doi.org/10.1080/23738871.2020.1728356
8. Digital Skills and Jobs Platform. (2023). Poland – Cybersecurity Strategy of the Republic of Poland 2019–2024. Updated March 27, 2023. Retrieved from Digital Skills & Jobs EU.
9. Dragos. (2024). Industrial Ransomware Analysis: Q4 2024. Retrieved from https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024
10. Dunn Cavelty, M., Pulver, T., & Smeets, M. (2024). The evolution of cyber conflict studies. International Affairs, 100(6), 2317–2339. https://doi.org/10.1093/ia/iiae175
11. ENISA. (2023). ENISA Threat Landscape 2023. Athens: European Union Agency for Cybersecurity.
12. ENISA. (2024). ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
13. European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. http://data.europa.eu/eli/reg/2019/881/oj
14. Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol Innovation Lab. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes
15. Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. International Affairs, 100(6), 2379–2397. https://doi.org/10.1093/ia/iiae231
16. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
17. Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy, 45(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062
18. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346, 489–497. https://doi.org/10.1016/j.heliyon.2017.e00346
19. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I. P., & Tygar, J. D. (2020). Adversarial machine learning: A survey of attacks on machine learning systems. ACM Computing Surveys, 53(3), 1–43.
20. Kasper, A., & Vernygora, V. A. (2021). Cybersecurity of the EU: A strategic narrative of a cyber power or a confusing policy for a local common market? Cuadernos Europeos de Deusto, 65(2021), 29–71. https://doi.org/10.18543/ced-65-2021pp
21. Kaspersky. (2021). COVID-19 and Cybersecurity Threats: Global Report. Moscow: Kaspersky Lab. Kaspersky Security Bulletin 2021 – Securelist. https://securelist.com/ksb-2021/
22. Klimkiewicz, A. (2020). Krajowy system cyberbezpieczeństwa – założenia i praktyka. Przegląd Prawa i Administracji, 121, 83–96. Wrocław: Uniwersytet Wrocławski. https://doi.org/10.19195/0137-1134.121.6
23. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248
24. Microsoft. (2023). Microsoft Digital Defense Report 2023. Redmond: Microsoft Security. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

25. Microsoft. (2024). Microsoft Digital Defense Report 2024. Security Insider. Retrieved December 7, 2025, from https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
26. Piazza, A., Vasudevan, S., & Carr, M. (2023). Cybersecurity in UK universities: Mapping (or managing) threat intelligence sharing within the higher education sector. Journal of Cybersecurity, 9(1), tyad019. https://doi.org/10.1093/cybsec/tyad019
27. Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084
28. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. International Cybersecurity Law Review, 6(2), 207–220. https://doi.org/10.1365/s43439-025-00154-4
29. Vacca, J. R. (Ed.). (2017). Computer and information security handbook (3rd ed.). Elsevier.