

Bezpieczeństwo wewnętrzne w erze cyfrowej – wyzwania i kierunki rozwoju

Internal security in the digital age – challenges and development areas

MICHAŁ ANTONIUK

Autor niezależny

 <https://orcid.org/0009-0006-7710-0685>

Abstrakt

Celem artykułu jest przedstawienie oraz usystematyzowanie współczesnych kierunków rozwoju bezpieczeństwa wewnętrznego w warunkach postępującej cyfryzacji. Przedmiotem opracowania jest wpływ technologii cyfrowych na specyfikę zagrożeń wewnętrznych oraz funkcjonowanie instytucji odpowiedzialnych za zapewnienie bezpieczeństwa państwa. Artykuł ma charakter przeglądowo-analityczny. W badaniu zastosowano analizę literatury przedmiotu, aktów prawnych i dokumentów strategicznych. Autor porównał rozwiązania dotyczące stosowania technologii cyfrowych w zakresie bezpieczeństwa przyjęte w różnych państwach i organizacjach międzynarodowych. Przeprowadzona analiza wykazała, że rozwój tych technologii prowadzi do zasadniczej transformacji systemów bezpieczeństwa wewnętrznego, wymuszając zmianę modeli zarządzania, rozwój współpracy międzyinstytucjonalnej oraz dostosowanie regulacji prawnych do nowych zagrożeń. We wnioskach autor wskazuje, że skuteczne zapewnienie bezpieczeństwa wewnętrznego w erze cyfrowej wymaga zintegrowanego podejścia łączącego rozwiązania technologiczne, odpowiednie ramy prawne, rozwój kompetencji instytucjonalnych oraz współpracę międzynarodową.

Słowa kluczowe bezpieczeństwo wewnętrzne, cyfryzacja, cyberbezpieczeństwo, zagrożenia cyfrowe, transformacja cyfrowa

Abstract The aim of this article is to present and systematize contemporary directions in the development of internal security in the context of advancing digital transformation. The subject of the study is the impact of digital technologies on the nature of internal threats and on the functioning of institutions responsible for ensuring state security. The article has a review-analytical character. The study employs a review of the relevant literature, an analysis of legal acts and strategic documents. The author compared the solutions for application of digital technologies in the field of security adopted in different countries and international organisations. The conducted analysis demonstrates that the development of these technologies has fundamentally transformed internal security systems, requiring changes in management models, the development of interinstitutional cooperation, and the adaptation of legal frameworks to emerging threats. In the conclusions, the author indicates that effective internal security in the digital age requires an integrated approach combining technological solutions, appropriate legal frameworks, development of institutional capacities, and international cooperation.

Keywords internal security, digitalisation, cybersecurity, digital threats, digital transformation

Wprowadzenie

Bezpieczeństwo wewnętrzne stanowi jeden z filarów funkcjonowania państwa. Obejmuje ono ochronę porządku publicznego, bezpieczeństwa obywateli, infrastruktury krytycznej oraz stabilności instytucji państwowych. Rozwój technologii cyfrowych spowodował zasadniczą zmianę środowiska bezpieczeństwa. Współczesne zagrożenia coraz częściej mają charakter transgraniczny, są realizowane w cyberprzestrzeni i oddziałują jednocześnie na wiele sektorów funkcjonowania państwa¹.

¹ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, London 1998, s. 21–35; M.D. Cavelty, *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009, s. 78–95.

W literaturze przedmiotu podkreśla się, że cyfryzacja nie tylko zwiększa efektywność funkcjonowania administracji publicznej i służb odpowiedzialnych za bezpieczeństwo, lecz także tworzy nowe obszary podatności. Autorzy tacy jak Barry Buzan, Myriam Dunn Cavelty czy Richard Clarke i Robert Knake, wskazują, że bezpieczeństwo wewnętrzne wymaga współcześnie odejścia od wyłącznie terytorialnego sposobu postrzegania zagrożeń na rzecz podejścia uwzględniającego cyberprzestrzeń, odporność infrastruktury krytycznej oraz bezpieczeństwo informacyjne. Z kolei dane z raportów Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (The European Union Agency for Cybersecurity, ENISA) oraz Organizacji Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation and Development, OECD) wskazują, że rosnąca liczba incydentów cybernetycznych wymusza zmianę sposobu organizacji instytucji odpowiedzialnych za bezpieczeństwo oraz rozwój współpracy publiczno-prywatnej².

Pytania badawcze niniejszego opracowania to: w jaki sposób postępująca cyfryzacja wpływa na funkcjonowanie systemu bezpieczeństwa wewnętrznego oraz jakie kierunki jego rozwoju wskazują współczesna literatura naukowa i dokumenty strategiczne?

Celem artykułu jest usystematyzowanie aktualnego stanu wiedzy dotyczącego wpływu transformacji cyfrowej na bezpieczeństwo wewnętrzne oraz identyfikacja najważniejszych wyzwań, kierunków rozwoju i rozwiązań z tym związanych, stosowanych w wybranych państwach oraz organizacjach międzynarodowych.

Artykuł ma charakter przeglądowo-analityczny. W badaniu wykorzystano analizę literatury przedmiotu, aktów prawnych i dokumentów strategicznych oraz metodę porównawczą. Zastosowanie tych metod dało możliwość zestawienia poglądów prezentowanych w literaturze, porównania rozwiązań instytucjonalnych i regulacyjnych oraz sformułowanie syntetycznych wniosków dotyczących kierunków rozwoju bezpieczeństwa wewnętrznego w erze cyfrowej.

Przekształcenie pojęcia bezpieczeństwa wewnętrznego w środowisku cyfrowym

Rozwój technologii cyfrowych doprowadził do zasadniczej zmiany sposobu postrzegania bezpieczeństwa wewnętrznego. Pojęcie to, wcześniej utożsamiane przede

² Zob. np. *ENISA Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [dostęp: 11 VIII 2026]; OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf?, s. 34–37 [dostęp: 11 VIII 2026].

wszystkim z ochroną porządku publicznego, zwalczaniem przestępczości oraz zapewnieniem stabilności funkcjonowania państwa w granicach jego terytorium, zostało rozszerzone o zwalczanie zagrożeń występujących w cyberprzestrzeni, których charakter wykracza poza klasyczne ujęcie bezpieczeństwa państwa³.

Barry Buzan, Ole Wæver i Jaap de Wilde wskazują, że bezpieczeństwo należy rozpatrywać wielowymiarowo, obejmując zarówno aspekty militarne, jak i polityczne, gospodarcze, społeczne i technologiczne. W ich ujęciu rozwój technologii informacyjnych zmienia sposób identyfikacji zagrożeń oraz mechanizmy reagowania państwa, prowadząc do rozszerzenia zakresu odpowiedzialności instytucji bezpieczeństwa. Oznacza to, że bezpieczeństwo wewnętrzne powinno obejmować nie tylko ochronę obywateli przed zagrożeniami fizycznymi, lecz także zapewnienie odporności infrastruktury cyfrowej oraz bezpieczeństwa informacji⁴.

Podobne stanowisko prezentuje Cavelti, która podkreśla, że cyfryzacja doprowadziła do powstania nowego środowiska bezpieczeństwa, w którym zagrożenia mają charakter dynamiczny, trudny do przewidzenia oraz często transgraniczny. Autorka zwraca uwagę, że cyberprzestrzeń stała się obszarem, w którym działania przestępcze, operacje wywiadowcze oraz kampanie dezinformacyjne mogą być prowadzone równocześnie wobec wielu państw, bez konieczności fizycznej obecności sprawców na ich terytorium. W rezultacie tradycyjne instrumenty ochrony bezpieczeństwa wewnętrznego okazują się niewystarczające, jeżeli nie są uzupełnione rozwiązaniami organizacyjnymi i technologicznymi dostosowanymi do specyfiki środowiska cyfrowego⁵.

Znaczenie tej transformacji potwierdza również ENISA. W raporcie tej organizacji za rok 2023 wskazano, że liczba ataków wymierzonych w administrację publiczną, sektor ochrony zdrowia oraz operatorów infrastruktury krytycznej systematycznie rośnie. Jednocześnie zwiększa się stopień złożoności wykorzystywanych metod, obejmujących m.in. ataki ransomware, kampanie phishingowe oraz działania prowadzone przez grupy sponsorowane przez państwa. Oznacza to, że bezpieczeństwo wewnętrzne coraz silniej zależy od zdolności państwa do ochrony infrastruktury cyfrowej oraz szybkiego reagowania na incydenty cybernetyczne⁶.

Analiza porównawcza rozwiązań przyjętych w wybranych państwach wskazuje, że proces dostosowania instytucji bezpieczeństwa przebiega w różnym tempie. Państwa członkowskie Unii Europejskiej rozwijają swoje systemy przede

³ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework...*, s. 27–29.

⁴ Tamże, s. 31–33.

⁵ M.D. Cavelti, *Cyber-Security and Threat Politics...*, s. 78–81.

⁶ ENISA *Threat Landscape 2023...*, s. 45–46.

wszystkim na podstawie wspólnych regulacji prawnych, takich jak dyrektywa NIS 2⁷, oraz współpracę w ramach ENISA.

Z kolei Stany Zjednoczone opierają rozwój cyberbezpieczeństwa na modelu zarządzania ryzykiem opracowanym przez National Institute of Standards and Technology (NIST), w którym szczególną rolę odgrywa współpraca administracji publicznej z sektorem prywatnym⁸.

Oba modele zmierzają do zwiększenia odporności państwa, jednak różnią się zakresem centralizacji oraz sposobem podziału odpowiedzialności między instytucje publiczne i podmioty prywatne.

Istotną konsekwencją transformacji cyfrowej jest również zmiana charakteru zagrożeń. Clarke i Knake wskazują, że cyberataki mogą oddziaływać jednocześnie na wiele sektorów państwa i prowadzić do zakłócenia pracy administracji, systemów finansowych, energetyki czy transportu. Nie wymagają przy tym użycia siły militarnej ani fizycznej obecności sprawcy, a ich skutki mogą obejmować zarówno straty ekonomiczne, jak i destabilizację społeczną oraz utratę zaufania obywateli do instytucji publicznych⁹.

Przegląd literatury przedmiotu prowadzi do wniosku, że bezpieczeństwo wewnętrzne w erze cyfrowej należy postrzegać przede wszystkim jako zdolność państwa do zapewnienia ciągłości funkcjonowania jego podstawowych struktur, ochrony infrastruktury krytycznej oraz skutecznego reagowania na zagrożenia powstające w cyberprzestrzeni. Oznacza to odejście od modelu skoncentrowanego na reagowaniu na incydenty na rzecz podejścia opartego na budowaniu odporności organizacyjnej, zarządzaniu ryzykiem oraz współpracy krajowej i międzynarodowej¹⁰.

Zagrożenia cyfrowe i ich wpływ na bezpieczeństwo wewnętrzne

Rozwój technologii cyfrowych doprowadził do zmiany charakteru zagrożeń oddziałujących na bezpieczeństwo wewnętrzne państwa. W przeciwieństwie do zagrożeń

⁷ 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).

⁸ *The NIST Cybersecurity Framework (CSF) 2.0*, February 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>, s. 21–23 [dostęp: 17 VIII 2026].

⁹ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010, s. 12–14.

¹⁰ M.D. Cavelty, *Cyber-Security and Threat Politics...*, s. 90–95; OECD, *Digital Security and Resilience...*, s. 34–37.

w wymiarze fizycznym, zagrożenia cyfrowe częściej mają charakter transgraniczny, są trudniejsze do identyfikacji, a ich skutki mogą obejmować jednocześnie wiele sektorów funkcjonowania państwa. Jak zauważa David S. Wall, cyberprzestępczość przestała być zjawiskiem ograniczonym do pojedynczych przestępstw komputerowych. Stała się złożonym systemem działalności przestępczej wykorzystującej globalne sieci teleinformatyczne. Obejmuje zarówno oszustwa finansowe, kradzieże tożsamości, jak i ataki na administrację publiczną, przedsiębiorstwa oraz infrastrukturę krytyczną¹¹.

Clarke i Knake wskazują, że cyberataki coraz częściej są ukierunkowane nie na pojedyncze systemy informatyczne, lecz na zakłócenie funkcjonowania całych sektorów gospodarki i administracji publicznej. Przykładem są ataki typu ransomware na szpitale, przedsiębiorstwa energetyczne oraz jednostki administracji samorządowej, których skutkiem jest nie tylko utrata danych, lecz także czasowe ograniczenie świadczenia usług publicznych. Autorzy podkreślają, że skuteczność takich działań wynika przede wszystkim z wysokiego stopnia cyfryzacji współczesnych państw oraz zależności między systemami teleinformatycznymi¹².

Odrębną kategorię zagrożeń stanowią kampanie dezinformacyjne prowadzone z wykorzystaniem mediów społecznościowych i platform internetowych. Lucas Kello zwraca uwagę, że współczesne konflikty coraz częściej obejmują działania informacyjne, których celem jest wpływanie na procesy polityczne, osłabianie zaufania obywateli do instytucji publicznych oraz pogłębianie podziałów społecznych. W przeciwieństwie do klasycznych cyberataków działania te nie prowadzą bezpośrednio do zniszczenia infrastruktury, lecz oddziałują na procesy decyzyjne oraz bezpieczeństwo społeczne, co czyni je jednym z najtrudniejszych wyzwań dla współczesnych systemów bezpieczeństwa wewnętrznego¹³.

Znaczenie zagrożeń informacyjnych potwierdzają również raporty ENISA oraz OECD. Wynika z nich, że od 2022 r. jest obserwowany wzrost liczby skoordynowanych kampanii dezinformacyjnych towarzyszących konfliktom międzynarodowym oraz procesom wyborczym. Jednocześnie wskazuje się, że skuteczność przeciwdziałania tego rodzaju zagrożeniom zależy od rozwiązań technologicznych, poziomu edukacji społeczeństwa, odporności informacyjnej obywateli oraz sprawnego systemu komunikacji instytucji publicznych¹⁴.

¹¹ D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007, s. 55–57.

¹² R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat...*, s. 24–28.

¹³ L. Kello, *The virtual weapon and international order*, New Haven–London 2017, s. 59–62.

¹⁴ ENISA *Threat Landscape 2023...*, s. 27–29; OECD, *Digital Security and Resilience...*, s. 56–58.

Analiza porównawcza doświadczeń państw Unii Europejskiej i Stanów Zjednoczonych wskazuje na odmienne modele reagowania na zagrożenia cyfrowe. W państwach UE położono nacisk na rozwój wspólnych standardów bezpieczeństwa, obowiązki zgłaszania incydentów oraz ochronę infrastruktury krytycznej wynikające z dyrektywy NIS 2. W Stanach Zjednoczonych podstawę stanowi *The NIST Cybersecurity Framework (CSF) 2.0*. Jest to model zarządzania ryzykiem koncentrujący się na identyfikacji zagrożeń, ochronie zasobów, wykrywaniu incydentów, reagowaniu oraz odbudowie zdolności operacyjnych po zakończeniu ataku.

W literaturze zwraca się uwagę również na asymetryczny charakter zagrożeń cyfrowych. Martin Libicki wskazuje, że relatywnie niewielkie grupy przestępcze lub podmioty sponsorowane przez państwa są w stanie osiągać skutki porównywalne z klasycznymi działaniami militarnymi, wykorzystując luki w zabezpieczeniach systemów teleinformatycznych. Oznacza to, że skuteczność działań nie zależy wyłącznie od potencjału ekonomicznego czy militarnego państwa, lecz także od poziomu jego odporności cyfrowej, przygotowania instytucji publicznych oraz jakości współpracy z operatorami infrastruktury krytycznej¹⁵.

Przegląd literatury prowadzi do wniosku, że zagrożenia cyfrowe obejmują cyberprzestępczość, cyberterroryzm, działania hybrydowe, operacje dezinformacyjne oraz ataki na infrastrukturę krytyczną, których wspólną cechą jest możliwość jednoczesnego oddziaływania na bezpieczeństwo państwa, gospodarkę i społeczeństwo. Z tego względu współczesne bezpieczeństwo wewnętrzne powinno być postrzegane jako system zarządzania ryzykiem cyfrowym, który integruje rozwiązania technologiczne, organizacyjne i prawne, a nie jako jedynie działania podejmowane po wystąpieniu incydentu¹⁶.

Stanowiska przedstawione w literaturze wskazują również, że skuteczność ochrony przed zagrożeniami cyfrowymi zależy od zdolności państwa do przewidywania nowych form ryzyka oraz ciągłego doskonalenia procedur bezpieczeństwa. W praktyce oznacza to konieczność regularnej aktualizacji krajowych strategii cyberbezpieczeństwa, rozwoju specjalistycznych kompetencji administracji publicznej oraz pogłębiania współpracy międzynarodowej w zakresie wymiany informacji o zagrożeniach i wspólnego reagowania na incydenty. Analiza porównawcza doświadczeń państw europejskich i Stanów Zjednoczonych potwierdza,

¹⁵ M.C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007, s. 102–118.

¹⁶ D.S. Wall, *Cybercrime: The Transformation of Crime...*, s. 55–70; S.W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012, s. 47–50.

że działania oparte na prewencji, budowaniu odporności oraz współpracy międzyinstytucjonalnej przynoszą lepsze rezultaty niż model koncentrujący się na reagowaniu po wystąpieniu ataku¹⁷.

Wyzwania związane z dostosowaniem instytucjonalnym i zarządzaniem

Postępująca cyfryzacja wymusza zmianę sposobu funkcjonowania instytucji odpowiedzialnych za bezpieczeństwo wewnętrzne. Tradycyjne modele organizacyjne, oparte na hierarchicznym podziale kompetencji oraz reagowaniu na zdarzenia po ich wystąpieniu, okazują się niewystarczające wobec zagrożeń charakteryzujących się dużą dynamiką, transgranicznością i wysokim stopniem złożoności. W literaturze podkreśla się, że skuteczność współczesnego systemu bezpieczeństwa wewnętrznego zależy od dostępnych technologii, ale przede wszystkim od zdolności instytucji do szybkiej adaptacji organizacyjnej oraz efektywnej współpracy międzysektorowej¹⁸.

Cavelty wskazuje, że jednym z najistotniejszych problemów współczesnych systemów bezpieczeństwa jest rozproszenie odpowiedzialności za cyberbezpieczeństwo. W wielu państwach kompetencje dotyczące ochrony infrastruktury krytycznej, przeciwdziałania cyberprzestępczości, ochrony danych osobowych oraz reagowania na incydenty są podzielone między administrację rządową, służby specjalne, organy ścigania i wyspecjalizowane zespoły reagowania na incydenty komputerowe (ang. *computer security incident response team*, CSIRT). Taki model zwiększa ryzyko dublowania zadań, wydłuża proces decyzyjny oraz utrudnia sprawną wymianę informacji¹⁹.

Podobne wnioski przedstawiono w raporcie OECD *Digital Security and Resilience in Critical Infrastructure and Essential Services*. Wskazano w nim, że państwa osiągające najwyższy poziom odporności cyfrowej tworzą zintegrowane systemy zarządzania bezpieczeństwem, w których odpowiedzialność poszczególnych instytucji jest jasno określona, a współpraca między nimi opiera się na wspólnych procedurach oraz regularnej wymianie informacji. Podkreślono również znaczenie strategicznego planowania oraz ciągłego doskonalenia procedur reagowania na incydenty²⁰.

Przeprowadzona analiza porównawcza pokazuje wyraźne różnice między modelami zarządzania bezpieczeństwem cyfrowym w UE i USA. W państwach

¹⁷ OECD, *Digital Security and Resilience...*, s. 34–37; *The NIST Cybersecurity Framework...*

¹⁸ M.D. Cavelty, *Cyber-Security and Threat Politics...*, s. 78–82; OECD, *Digital Security and Resilience...*, s. 39–42.

¹⁹ M.D. Cavelty, *Cyber-Security and Threat Politics...*, s. 91–95.

²⁰ OECD, *Digital Security and Resilience...*, s. 55–57.

członkowskich UE rozwój systemów cyberbezpieczeństwa opiera się przede wszystkim na harmonizacji przepisów prawa oraz współpracy prowadzonej w ramach ENISA i realizacji dyrektywy NIS 2. Państwa zobowiązano do wyznaczenia właściwych organów odpowiedzialnych za cyberbezpieczeństwo, utworzenia krajowych zespołów reagowania na incydenty oraz opracowania krajowych strategii bezpieczeństwa cyfrowego²¹.

Model amerykański opiera się na zarządzaniu ryzykiem oraz partnerstwie administracji publicznej z sektorem prywatnym. Ramy zarządzania cyberbezpieczeństwem opracowane przez NIST obejmują pięć podstawowych etapów: identyfikację zagrożeń, ochronę zasobów, wykrywanie incydentów, reagowanie oraz odbudowę zdolności operacyjnych. Rozwiązanie to jest szeroko wykorzystywane zarówno przez administrację federalną, jak i przedsiębiorstwa zarządzające infrastrukturą krytyczną²².

Istotnym elementem transformacji instytucjonalnej pozostaje rozwój kompetencji pracowników odpowiedzialnych za bezpieczeństwo. Henock Mulugeta Melaku zwraca uwagę, że skuteczność systemów cyberbezpieczeństwa zależy w równym stopniu od stosowanych technologii i od poziomu specjalistycznej wiedzy personelu. W praktyce oznacza to konieczność prowadzenia systematycznych szkoleń, rozwijania umiejętności z zakresu analizy danych, informatyki śledczej oraz zarządzania incydentami bezpieczeństwa. Niedobór wysoko wykwalifikowanych specjalistów stanowi obecnie jedno z najczęściej wskazywanych ograniczeń rozwoju krajowych systemów cyberbezpieczeństwa²³.

Coraz większego znaczenia nabiera również współpraca między administracją publiczną a sektorem prywatnym. Znaczna część infrastruktury krytycznej, obejmująca systemy energetyczne, telekomunikacyjne, finansowe oraz transportowe, pozostaje własnością prywatnych przedsiębiorstw. Ochrona tych zasobów wymaga zatem stworzenia mechanizmów umożliwiających bieżącą wymianę informacji o zagrożeniach, prowadzenie wspólnych ćwiczeń oraz opracowywania jednolitych procedur reagowania. Doświadczenia państw skandynawskich oraz Holandii pokazują, że dzięki rozwiniętym partnerstwom publiczno-prywatnym można szybciej zidentyfikować zagrożenia i skuteczniej ograniczać skutki incydentów cybernetycznych²⁴.

²¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa...

²² *The NIST Cybersecurity Framework...*

²³ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework*, „Journal of Cybersecurity and Privacy” 2023, t. 3, nr 3, s. 347–350. <https://doi.org/10.3390/jcp3030017>.

²⁴ OECD, *Digital Security and Resilience...*, s. 51–53.

Przegląd literatury wskazuje również, że transformacja instytucjonalna nie może ograniczać się do wdrażania nowych technologii. Równie istotne jest budowanie kultury organizacyjnej sprzyjającej współpracy, wymianie wiedzy oraz ciągłemu doskonaleniu procedur bezpieczeństwa. Organizacje charakteryzujące się wysokim poziomem elastyczności organizacyjnej skuteczniej adaptują się do zmieniającego się środowiska zagrożeń niż instytucje funkcjonujące według sztywnych, hierarchicznych modeli zarządzania²⁵.

Podsumowując, można stwierdzić, że rozwój bezpieczeństwa wewnętrznego wymaga kompleksowej modernizacji instytucji publicznych. Obejmuje ona inwestycje w nowoczesne technologie, reformę struktur organizacyjnych, rozwój kompetencji pracowników, budowę trwałych mechanizmów współpracy z sektorem prywatnym oraz systematyczne doskonalenie procedur zarządzania ryzykiem. Analiza porównawcza doświadczeń państw UE i Stanów Zjednoczonych wskazuje, że najwyższą skuteczność osiągają systemy bezpieczeństwa łączące nowoczesne rozwiązania technologiczne z efektywnym zarządzaniem instytucjonalnym oraz jasno określonym podziałem odpowiedzialności²⁶.

Prawne i etyczne aspekty bezpieczeństwa wewnętrznego w erze cyfrowej

Transformacja cyfrowa spowodowała konieczność dostosowania obowiązujących regulacji prawnych dotyczących bezpieczeństwa wewnętrznego do zagrożeń w cyberprzestrzeni. Rozwój technologii informacyjnych umożliwił instytucjom publicznym wykorzystywanie narzędzi opartych na analizie dużych zbiorów danych, monitorowaniu sieci teleinformatycznych oraz automatyzacji procesów decyzyjnych. Jednocześnie rozwiązania te wywołały dyskusję dotyczącą granic ingerencji państwa w prawa i wolności jednostki. W literaturze przedmiotu podkreśla się, że skuteczność działań podejmowanych na rzecz bezpieczeństwa wewnętrznego powinna pozostawać w zgodzie z zasadą państwa prawa oraz standardami ochrony praw człowieka²⁷.

²⁵ Tamże.

²⁶ OECD, *Digital Security and Resilience...*, s. 55–58; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, s. 341–344; *The NIST Cybersecurity Framework...*

²⁷ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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); M.D. Cavelti, *Cyber-Security and Threat Politics...*

Podstawowym aktem prawnym regulującym ochronę danych osobowych w państwach UE jest *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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)* (dalej: rozporządzenie RODO). Regulacja ta ustanawia zasady legalności, przejrzystości, minimalizacji danych oraz ograniczenia celu ich przetwarzania. Z perspektywy bezpieczeństwa wewnętrznego oznacza to, że organy publiczne mogą wykorzystywać dane osobowe wyłącznie w zakresie niezbędnym do realizacji ustawowych zadań oraz z zachowaniem zasady proporcjonalności. Rozporządzenie RODO nie ogranicza możliwości prowadzenia działań związanych z bezpieczeństwem państwa, jednak nakłada obowiązek zapewnienia odpowiednich zabezpieczeń technicznych i organizacyjnych chroniących prawa obywateli.

Drugim istotnym elementem europejskiego systemu prawnego jest dyrektywa NIS 2. W porównaniu z wcześniejszą dyrektywą NIS²⁸ rozszerzono katalog podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa oraz zaostrzono wymagania dotyczące zarządzania ryzykiem, zgłaszania incydentów oraz odpowiedzialności kierownictwa organizacji. Rozwiązania te odzwierciedlają zmianę podejścia – od reagowania na incydenty do systemowego budowania odporności państwa i infrastruktury krytycznej²⁹.

Istotne znaczenie dla współpracy międzynarodowej ma również konwencja Rady Europy o cyberprzestępczości zwana konwencją budapesztańską³⁰. Dokument ten ujednolicił podstawowe definicje przestępstw komputerowych oraz stworzył ramy współpracy między organami ścigania różnych państw. Jak wskazuje Susan Brenner, skuteczne zwalczanie cyberprzestępczości wymaga harmonizacji regulacji prawnych, ponieważ sprawcy często wykorzystują różnice między krajowymi systemami prawnymi. Konwencja budapesztańska pozostaje podstawowym instrumentem współpracy międzynarodowej w zakresie ścigania przestępstw popełnianych z wykorzystaniem technologii informacyjnych.

W Polsce podstawę systemu cyberbezpieczeństwa stanowi ustawa o krajowym systemie cyberbezpieczeństwa³¹ implementująca rozwiązania przyjęte

²⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

²⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa...

³⁰ Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.; S.W. Brenner, *Cybercrime and the Law...*, s. 48–50.

³¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

na poziomie UE. Ustawa określa kompetencje administracji publicznej, operatorów usług kluczowych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT MON, CSIRT NASK oraz CSIRT GOV). Jej celem jest zapewnienie sprawnego wykrywania incydentów, koordynacji działań naprawczych oraz wymiany informacji między instytucjami odpowiedzialnymi za bezpieczeństwo państwa.

Coraz większe znaczenie zyskują również regulacje dotyczące wykorzystania sztucznej inteligencji. Przyjęty przez Unię Europejską AI Act³² wprowadza klasyfikację systemów sztucznej inteligencji według poziomu ryzyka oraz określa obowiązki podmiotów wdrażających rozwiązania o wysokim stopniu oddziaływania społecznego. W kontekście bezpieczeństwa wewnętrznego oznacza to konieczność zapewnienia przejrzystości działania algorytmów wykorzystywanych m.in. do analizy zagrożeń, monitorowania przestrzeni publicznej czy wspomagania procesów decyzyjnych służb odpowiedzialnych za bezpieczeństwo.

Aspekty prawne są ściśle związane z problematyką etyczną. Rozwój systemów monitoringu, analityki predykcyjnej oraz sztucznej inteligencji zwiększa możliwości zapobiegania zagrożeniom, ale jednocześnie rodzi ryzyko naruszenia prawa do prywatności oraz wystąpienia dyskryminacji algorytmicznej. Cavelty podkreśla, że przyzwolenie społeczne na wykorzystywanie nowoczesnych technologii w celu zapewnienia bezpieczeństwa zależy od przejrzystości procedur, możliwości kontroli działań administracji oraz skutecznych mechanizmów odwoławczych. Obywatele są bardziej skłonni akceptować zwiększony zakres działań państwa, jeżeli mają pewność, że ingerencja odbywa się na podstawie prawa i podlega niezależnemu nadzorowi³³.

Analiza porównawcza wskazuje wyraźne różnice między podejściem europejskim i amerykańskim. W UE pierwszeństwo przyznaje się ochronie praw podstawowych, prywatności oraz kontroli przetwarzania danych osobowych. W USA większy nacisk położono na efektywność działań operacyjnych służb odpowiedzialnych za bezpieczeństwo narodowe, pozostawiając przy tym szerszy zakres kompetencji instytucjom zajmującym się przeciwdziałaniem zagrożeniom. Różnice te wynikają z odmiennych tradycji prawnych i konstytucyjnych. Oba modele zmierzają jednak do zachowania równowagi między skutecznością działań w zakresie bezpieczeństwa a ochroną praw obywatelskich³⁴.

³² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

³³ M.D. Cavelty, *Cyber-Security and Threat Politics...*, s. 91–93.

³⁴ Tamże, s. 91–95.

Przegląd literatury oraz obowiązujących regulacji prowadzi do wniosku, że rozwój bezpieczeństwa wewnętrznego w erze cyfrowej wymaga równoczesnego doskonalenia instrumentów prawnych i standardów etycznych. Nowoczesne technologie mogą znacznie zwiększać skuteczność instytucji odpowiedzialnych za bezpieczeństwo, jednak ich wykorzystanie powinno odbywać się w granicach wyznaczonych przez zasadę proporcjonalności, legalności i odpowiedzialności. Tylko zachowanie równowagi pomiędzy ochroną bezpieczeństwa państwa a poszanowaniem praw jednostki pozwala budować trwałe zaufanie społeczne i zapewnić skuteczność systemu bezpieczeństwa wewnętrznego³⁵.

Technologia jako narzędzie bezpieczeństwa wewnętrznego

Rozwój technologii cyfrowych istotnie zmienił sposób realizacji zadań związanych z zapewnieniem bezpieczeństwa wewnętrznego. Nowoczesne rozwiązania informatyczne nie pełnią już funkcji wyłącznie wspomagającej działalność instytucji publicznych, lecz stały się jednym z podstawowych elementów planowania, monitorowania zagrożeń i reagowania na nie. Jak podkreślają Clarke i Knake, współczesne bezpieczeństwo państwa w coraz większym stopniu jest uzależnione od zdolności do skutecznego wykorzystania technologii informacyjnych zarówno w działaniach prewencyjnych, jak i operacyjnych³⁶.

Jednym z najważniejszych kierunków rozwoju pozostaje wykorzystanie analizy danych oraz sztucznej inteligencji. Współczesne systemy bezpieczeństwa przetwarzają ogromne ilości informacji pochodzących z monitoringu, sieci teleinformatycznych, rejestrów administracyjnych oraz otwartych źródeł informacji (ang. *open-source intelligence*, OSINT). Zastosowanie algorytmów uczenia maszynowego umożliwi identyfikację nietypowych zachowań, przewidywanie potencjalnych zagrożeń oraz wspomaganie procesów decyzyjnych. Melaku wskazuje, że rozwiązania oparte na sztucznej inteligencji zwiększają skuteczność zarządzania cyberbezpieczeństwem pod warunkiem, że funkcjonują w ramach odpowiednio zaprojektowanego systemu zarządzania ryzykiem oraz podlegają stałemu nadzorowi ekspertów³⁷.

³⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r...; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych...; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji...

³⁶ R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat...*, s. 12–28.

³⁷ H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, s. 348–350.

Istotną rolę odgrywają również technologie wspierające monitorowanie infrastruktury krytycznej. Systemy automatycznej detekcji zagrożeń pozwalają na bieżące analizowanie funkcjonowania sieci energetycznych, transportowych, telekomunikacyjnych oraz finansowych. Raport *ENISA Threat Landscape 2023* wskazuje, że szybkie wykrywanie nieprawidłowości znacznie ogranicza skutki ataków ransomware oraz innych incydentów wymierzonych w infrastrukturę państwa. Z tego względu coraz większy nacisk kładzie się na rozwój systemów wczesnego ostrzegania oraz automatyzację procedur reagowania³⁸.

Przykładem praktycznego wykorzystania technologii są krajowe i sektorowe centra operacji bezpieczeństwa (ang. *security operations centres*), których zadaniem jest całodobowe monitorowanie sieci teleinformatycznych oraz analiza pojawiających się zagrożeń. Funkcjonowanie takich jednostek umożliwia skrócenie czasu wykrywania incydentów oraz szybszą koordynację działań naprawczych.

Unia Europejska i Stany Zjednoczone mają odmienne podejście do wykorzystania technologii. Państwa unijne równolegle rozwijają technologię i system regulacyjny, akcentując ochronę danych osobowych oraz bezpieczeństwo infrastruktury krytycznej. W USA większy nacisk położono na współpracę administracji federalnej z sektorem prywatnym oraz rozwój innowacyjnych technologii opracowywanych przez przedsiębiorstwa technologiczne. Model amerykański sprzyja szybkiemu wdrażaniu nowych rozwiązań, europejski natomiast zapewnia silniejsze mechanizmy nadzoru prawnego nad ich stosowaniem³⁹.

Postępująca automatyzacja procesów bezpieczeństwa przynosi jednak również nowe wyzwania. Coraz większe uzależnienie administracji publicznej od systemów informatycznych powoduje, że awaria lub skuteczny cyberatak mogą prowadzić do zakłócenia funkcjonowania wielu sektorów jednocześnie. Libicki podkreśla, że wzrost poziomu cyfryzacji zwiększa zarówno efektywność działania instytucji publicznych, jak i skalę potencjalnych konsekwencji wynikających z naruszenia bezpieczeństwa systemów informatycznych. Oznacza to konieczność projektowania rozwiązań zapewniających odporność, redundancję oraz możliwość szybkiego odtworzenia funkcji krytycznych po wystąpieniu incydentu⁴⁰.

W literaturze zwraca się również uwagę na znaczenie współpracy między środowiskiem naukowym, administracją publiczną oraz sektorem prywatnym. Dynamiczny rozwój technologii powoduje, że instytucje odpowiedzialne za bezpieczeństwo nie są w stanie samodzielnie opracowywać wszystkich innowacyjnych

³⁸ *ENISA Threat Landscape 2023...*, s. 47–51.

³⁹ Tamże; *The NIST Cybersecurity Framework...*; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych...

⁴⁰ M.C. Libicki, *Conquest in Cyberspace...*, s. 102–106.

rozwiązań. OECD wskazuje, że partnerstwa obejmujące uczelnie, instytuty badawcze oraz przedsiębiorstwa technologiczne sprzyjają szybszemu wdrażaniu nowych narzędzi analitycznych, poprawiają jakość zarządzania ryzykiem oraz zwiększają poziom odporności cyfrowej państwa⁴¹.

Przegląd literatury prowadzi do wniosku, że technologia stanowi obecnie jeden z najważniejszych instrumentów zapewnienia bezpieczeństwa wewnętrznego. Jej skuteczność zależy jednak od sposobu integracji z rozwiązaniami organizacyjnymi, prawnymi i kadrowymi. Samo wdrażanie nowych systemów informatycznych nie gwarantuje zwiększenia poziomu bezpieczeństwa. Decydujące znaczenie ma stworzenie spójnego modelu zarządzania, w którym rozwiązania technologiczne wspierają proces podejmowania decyzji, pozostając jednocześnie pod kontrolą odpowiednich procedur prawnych i kompetentnego personelu. Analiza doświadczeń państw UE i Stanów Zjednoczonych potwierdza, że najwyższą skuteczność osiągają systemy łączące rozwój technologii z inwestycjami w kapitał ludzki, współpracę międzyinstytucjonalną oraz systematyczną ocenę ryzyka⁴².

Kontekst międzynarodowy i perspektywa porównawcza

Współczesne bezpieczeństwo wewnętrzne nie może być analizowane wyłącznie z perspektywy pojedynczego państwa. Rozwój technologii cyfrowych spowodował, że zagrożenia coraz częściej mają charakter transgraniczny, a ich skutki wykraczają poza granice jurysdykcji krajowych. Cyberprzestępczość, kampanie dezinformacyjne czy ataki na infrastrukturę krytyczną są prowadzone z wykorzystaniem globalnych sieci teleinformatycznych, co powoduje, że skuteczne przeciwdziałanie wymaga ścisłej współpracy międzynarodowej. Jak zauważa Kello, cyberprzestrzeń stała się nowym środowiskiem rywalizacji strategicznej, w którym granice między bezpieczeństwem wewnętrznym i zewnętrznym stopniowo się zacierają⁴³.

Pomimo różnic organizacyjnych systemy europejski i amerykański opierają się na podobnych założeniach strategicznych. W obu przypadkach kluczowe znaczenie mają: rozwój krajowych strategii cyberbezpieczeństwa, budowanie odporności infrastruktury krytycznej, doskonalenie systemów wymiany informacji oraz rozwój kompetencji specjalistycznych. Różnice dotyczą natomiast sposobu realizacji tych celów. W państwach UE większy nacisk położono na harmonizację

⁴¹ OECD, *Digital Security and Resilience...*, s. 34–39.

⁴² Tamże; H.M. Melaku, *A Dynamic and Adaptive Cybersecurity Governance Framework...*, s. 327–331; *The NIST Cybersecurity Framework...*

⁴³ L. Kello, *The virtual weapon and international order...*, s. 45–62.

przepisów prawa i ochronę praw podstawowych, a w USA na elastyczność organizacyjną oraz partnerstwo publiczno-prywatne⁴⁴.

Znaczącą rolę w międzynarodowym systemie bezpieczeństwa odgrywa również Organizacja Traktatu Północnoatlantyckiego (NATO). Po uznaniu cyberprzestrzeni za domenę działań operacyjnych NATO rozwija wspólne zdolności w zakresie przeciwdziałania zagrożeniom cybernetycznym, prowadzi ćwiczenia z udziałem państw członkowskich oraz wspiera wymianę doświadczeń dotyczących ochrony infrastruktury krytycznej. Rozwiązania te zwiększają zdolność państw do reagowania na incydenty o charakterze transgranicznym oraz sprzyjają ujednolicaniu procedur bezpieczeństwa⁴⁵.

Coraz większe znaczenie mają również działania prowadzone przez Organizację Narodów Zjednoczonych oraz Radę Europy. Konwencja budapeszteńska stworzyła podstawy współpracy organów ścigania w zakresie zwalczania cyberprzestępczości, a eksperckie grupy ONZ opracowują rekomendacje dotyczące odpowiedzialnego zachowania państw w cyberprzestrzeni⁴⁶. Chociaż dokumenty te nie eliminują wszystkich różnic między krajowymi systemami prawnymi, to przyczyniają się do stopniowej harmonizacji standardów międzynarodowych oraz ułatwiają współpracę w zakresie ścigania sprawców przestępstw komputerowych.

Analiza porównawcza dokumentów prowadzi do wniosku, że skuteczność systemów bezpieczeństwa wewnętrznego zależy nie od przyjęcia jednego uniwersalnego modelu organizacyjnego, lecz od umiejętnego dostosowania rozwiązań do uwarunkowań krajowych przy jednoczesnym wykorzystaniu doświadczeń międzynarodowych. Wspólnym elementem wszystkich analizowanych modeli, czyli unijnego i amerykańskiego, pozostaje rozwój współpracy międzyinstytucjonalnej, budowanie odporności infrastruktury krytycznej, systematyczna wymiana informacji o zagrożeniach oraz ciągłe doskonalenie kompetencji specjalistycznych. Przegląd literatury potwierdza, że państwa aktywnie uczestniczące w międzynarodowych sieciach współpracy osiągają wyższy poziom odporności na zagrożenia cyfrowe oraz skuteczniej reagują na incydenty o charakterze transgranicznym⁴⁷.

⁴⁴ OECD, *Digital Security and Resilience...*, s. 34–58; ENISA *Threat Landscape 2023...*; The NIST Cybersecurity Framework...

⁴⁵ A. Kozłowski, *Operacje NATO w cyberprzestrzeni*, CyberDefence24, 3 VI 2019 r., https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [dostęp: 11 IX 2026].

⁴⁶ Konwencja Rady Europy o cyberprzestępczości...; United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021, s. 57–59.

⁴⁷ OECD, *Digital Security and Resilience...*, s. 51–54; ENISA *Threat Landscape 2023...*; The NIST Cybersecurity Framework...

Podsumowanie i wnioski

Przeprowadzona analiza literatury przedmiotu, aktów prawnych oraz dokumentów strategicznych potwierdza, że postępująca cyfryzacja prowadzi do zasadniczej zmiany sposobu postrzegania bezpieczeństwa wewnętrznego. Współczesne zagrożenia coraz rzadziej mają charakter wyłącznie lokalny lub fizyczny, a coraz częściej obejmują cyberprzestrzeń, infrastrukturę krytyczną oraz środowisko informacyjne. W konsekwencji bezpieczeństwo wewnętrzne należy rozumieć jako system zdolny do identyfikowania, ograniczania i neutralizowania zagrożeń istniejących równocześnie w wymiarze technologicznym, organizacyjnym, prawnym i społecznym.

Analiza dorobku naukowego Barry'ego Buzana, Myriam Dunn Cavelty, Richarda Clarke'a, Roberta Knake'a, Lucasa Kello oraz Davida S. Walla i innych badaczy wskazuje, że rozwój technologii cyfrowych doprowadził do rozszerzenia zakresu odpowiedzialności instytucji bezpieczeństwa. Ochrona porządku publicznego obejmuje obecnie również zapewnienie bezpieczeństwa infrastruktury cyfrowej, ochronę danych, przeciwdziałanie dezinformacji oraz budowanie odporności społeczeństwa na zagrożenia informacyjne. Oznacza to odejście od tradycyjnego modelu bezpieczeństwa skoncentrowanego na reagowaniu po wystąpieniu zagrożenia na rzecz modelu opartego na zarządzaniu ryzykiem i wzmacnianiu odporności.

Przegląd literatury pozwala również stwierdzić, że skuteczność systemu bezpieczeństwa wewnętrznego zależy od stopnia integracji działań prowadzonych przez administrację publiczną, sektor prywatny oraz środowisko naukowe. Szczegółne znaczenie ma ochrona infrastruktury krytycznej, która w większości państw pozostaje w znacznej części własnością podmiotów prywatnych. Doświadczenia państw europejskich oraz Stanów Zjednoczonych pokazują, że rozwinięte partnerstwa publiczno-prywatne umożliwiają skuteczniejszą wymianę informacji o zagrożeniach, szybsze reagowanie na incydenty oraz bardziej efektywne zarządzanie ryzykiem.

Państwa UE i Stany Zjednoczone realizują odmienne modele organizacji bezpieczeństwa cyfrowego. Model europejski koncentruje się na harmonizacji regulacji prawnych, ochronie praw podstawowych oraz budowaniu wspólnych standardów cyberbezpieczeństwa. Model amerykański większy nacisk kładzie na zarządzanie ryzykiem, elastyczność organizacyjną oraz współpracę administracji z sektorem prywatnym.

Analiza aktów prawnych wskazuje, że rozwój bezpieczeństwa wewnętrznego wymaga równoczesnego doskonalenia regulacji dotyczących ochrony danych osobowych, cyberbezpieczeństwa oraz wykorzystania sztucznej inteligencji. Unijne rozporządzenie RODO, dyrektywa NIS 2, konwencja budapesztańska oraz AI Act tworzą komplementarne ramy prawne umożliwiające prowadzenie działań na rzecz bezpieczeństwa przy jednoczesnym poszanowaniu praw i wolności obywatelskich.

Oznacza to konieczność zachowania równowagi między skutecznością działań służb odpowiedzialnych za bezpieczeństwo a ochroną prywatności, przejrzystością działania administracji oraz odpowiedzialnością za podejmowane decyzje.

Na podstawie przeprowadzonej analizy można sformułować następujące wnioski:

1. Cyfryzacja trwale zmieniła charakter bezpieczeństwa wewnętrznego, rozszerzając jego zakres o ochronę cyberprzestrzeni, w tym systemów obsługujących infrastrukturę krytyczną oraz bezpieczeństwa informacyjnego.
2. Największym wyzwaniem dla współczesnych systemów bezpieczeństwa pozostaje zdolność instytucji do szybkiego dostosowywania struktur organizacyjnych i procedur do dynamicznie zmieniającego się środowiska zagrożeń.
3. Skuteczność ochrony bezpieczeństwa wewnętrznego zależy od współpracy administracji publicznej, sektora prywatnego oraz środowiska naukowego, szczególnie w zakresie ochrony infrastruktury krytycznej i wymiany informacji o zagrożeniach.
4. Nowoczesne technologie, w tym sztuczna inteligencja, analiza dużych zbiorów danych oraz automatyzacja procesów bezpieczeństwa, zwiększają możliwości instytucji odpowiedzialnych za bezpieczeństwo, jednak wykorzystanie tych technologii wymaga odpowiednich gwarancji prawnych i etycznych.
5. Najwyższą skuteczność osiągają systemy łączące rozwój technologiczny z efektywnym zarządzaniem, jasnym podziałem kompetencji oraz rozbudowaną współpracą międzynarodową.

Bezpieczeństwo wewnętrzne w erze cyfrowej wymaga podejścia interdyscyplinarnego, łączącego wiedzę z zakresu nauk o bezpieczeństwie, prawa, nauk o zarządzaniu oraz technologii informacyjnych. Dalszy rozwój systemów bezpieczeństwa będzie uzależniony od zdolności państw do wdrażania innowacyjnych rozwiązań technologicznych przy jednoczesnym zachowaniu standardów demokratycznego państwa prawa i ochrony praw człowieka.

Na podstawie przeprowadzonej analizy autor zauważa również kierunki dalszych badań dotyczących wpływu sztucznej inteligencji na funkcjonowanie instytucji bezpieczeństwa, oceny skuteczności wdrażania dyrektywy NIS 2 w państwach UE oraz porównania krajowych modeli budowania odporności cyfrowej. Wiedza na ten temat może dostarczyć istotnych rekomendacji dla praktyki funkcjonowania administracji publicznej oraz dalszego doskonalenia krajowych systemów bezpieczeństwa wewnętrznego.

Bibliografia

- Brenner S.W., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012.
- Buzan B., Wæver O., Wilde J. de, *Security: A New Framework for Analysis*, London 1998.
- Cavelty M.D., *Cyber-Security and Threat Politics. US efforts to secure the information age*, London–New York 2009.
- Clarke R.A., Knake R.K., *Cyber War: The Next Threat to National Security and What to Do about It*, New York 2010.
- Kello L., *The virtual weapon and international order*, New Haven–London 2017.
- Libicki M.C., *Conquest in Cyberspace. National Security and Information Warfare*, Cambridge 2007.
- Melaku H.M., *A Dynamic and Adaptive Cybersecurity Governance Framework*, „Journal of Cybersecurity and Privacy” 2023, t. 3, nr 3, s. 327–350. <https://doi.org/10.3390/jcp3030017>.
- United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 14 July 2021.
- Wall D.S., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge 2007.

Źródła internetowe

- ENISA *Threat Landscape 2023*, European Union Agency for Cybersecurity, October 2023, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf> [dostęp: 11 VIII 2026].
- Kozłowski A., *Operacje NATO w cyberprzestrzeni*, CyberDefence24, 3 VI 2019 r., https://cyberdefence24.pl/polityka-i-prawo/operacje-nato-w-cyberprzestrzeni#goog_rewarded [dostęp: 11 IX 2026].
- OECD, *Digital Security and Resilience in Critical Infrastructure and Essential Services*, April 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf? [dostęp: 11 VIII 2026].
- The NIST Cybersecurity Framework (CSF) 2.0*, February 2024, <https://nvlpubs.nist.gov/nist-pubs/CSWP/NIST.CSWP.29.pdf> [dostęp: 17 VIII 2026].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

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) – (Dz. Urz. UE L 333/80 z 27 XII 2022 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19 VII 2016 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) – (Dz. Urz. UE L 2024/1689 z 12 VII 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 119/1 z 4 V 2016 r.).

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (DzU z 2015 r. poz. 728).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2018 r. poz. 1560, ze zm.).

Michał Antoniuk

Ukończył studia na Uniwersytecie Warszawskim oraz podyplomowe studia w Akademii Sztuki Wojennej. Zawodowo związany z administracją publiczną, obecnie pełni służbę w Ministerstwie Obrony Narodowej, gdzie realizuje zadania z obszaru bezpieczeństwa. Jego zainteresowania naukowe i zawodowe obejmują geopolitykę oraz zarządzanie projektami.

Kontakt: antonek@o2.pl