Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/220521

Cyber-deterrence Finlandii i państw nordyckich – model odstraszania cyfrowego a bezpieczeństwo państwa

Cyber-deterrence of Finland and the Nordic countries – a model of digital deterrence and state security

Krzysztof KACZMAREK
Politechnika Koszalińska
ORCID: 0000-0001-8519-1667
E-mail: puola1972@gmail.com

Streszczenie

Artykuł podejmuje problematykę cyber-deterrence w kontekście bezpieczeństwa państwa, koncentrując się na rozwiązaniach przyjmowanych w Finlandii oraz w pozostałych państwach nordyckich. Punktem wyjścia jest założenie, że cyberprzestrzeń stała się trwałym elementem środowiska bezpieczeństwa, a zakłócenia w tej domenie mogą bezpośrednio wpływać na funkcjonowanie administracji publicznej, usług publicznych oraz kluczowych procesów państwowych. W tym ujęciu odstraszanie w cyberprzestrzeni nie jest rozumiane wyłącznie jako reakcja na incydenty, lecz jako element szerszej strategii opartej na prewencji, odporności instytucjonalnej i ciągłości działania. Analiza pokazuje, że w Finlandii cyber-deterrence jest ściśle powiązane z koncepcją bezpieczeństwa kompleksowego i nie opiera się na logice odwetu. Zamiast tego akcentowane są zdolności państwa do identyfikowania zagrożeń, ograniczania ich skutków oraz utrzymania kontroli nad kluczowymi procesami w warunkach długotrwałej presji. Szczególna uwaga została poświęcona uwarunkowaniom społecznym i instytucjonalnym cyberbezpieczeństwa, w tym roli administracji publicznej, samorządu terytorialnego oraz współpracy międzysektorowej. W rezultacie fiński model cyber-deterrence ukazany został jako systemowy i pośredni mechanizm odstraszania, którego skuteczność wynika z odporności państwa, a nie z demonstracji siły w cyberprzestrzeni.

Słowa kluczowe

cyber-deterrence, cyberbezpieczeństwo, odporność instytucjonalna, bezpieczeństwo kompleksowe, państwa nordyckie.

Abstract

This article addresses the issue of cyber deterrence in the context of national security, focusing on solutions adopted in Finland and the other Nordic countries. The starting point is the assumption that cyberspace has become a permanent element of the security environment, and disruptions in this domain can directly impact the functioning of public administration, public services, and key state processes. In this

approach, cyber deterrence is not understood solely as a response to incidents, but as part of a broader strategy based on prevention, institutional resilience, and business continuity. The analysis shows that in Finland, cyber deterrence is closely linked to the concept of comprehensive security and is not based on the logic of retaliation. Instead, the emphasis is on the state's ability to identify threats, mitigate their effects, and maintain control over key processes under conditions of sustained pressure. Particular attention is paid to the social and institutional conditions of cybersecurity, including the role of public administration, local government, and cross-sectoral cooperation. As a result, the Finnish cyber-deterrence model was presented as a systemic and indirect deterrence mechanism whose effectiveness stems from the state's resilience, not from the demonstration of force in cyberspace.

Keywords

cyber-deterrence, cybersecurity, institutional resilience, comprehensive security, Nordic countries

Wprowadzenie

Rozwój technologii cyfrowych w istotnym stopniu zmienił warunki funkcjonowania państw oraz charakter zagrożeń, z jakimi muszą się one mierzyć, a cyberprzestrzeń stała się trwałym elementem środowiska bezpieczeństwa. Jednocześnie analizy dotyczące wszelkich form konfliktów toczących się w domenie cyfrowej muszą brać pod uwagę fakt, że w cyberprzestrzeni nie ma barier kontrolnych[1]. Istotne jest również to, że jednym z najważniejszych elementów zapewniania bezpieczeństwa w domenie cyfrowej jest prewencja[2]. Należy również brać pod uwagę, że zakłócenia w cyberprzestrzeni mogą mieć negatywny wpływ na realizację usług o znaczeniu strategicznym[3]. Jest to szczególnie istotne w przypadku państw rozwiniętych pod względem technologicznym, w których cyberataki mogą spowodować destabilizację funkcjonowania władzy publicznej[4].

W takich uwarunkowaniach szczególnego znaczenia nabiera problem odstraszania w cyberprzestrzeni, rozumianego nie tylko jako reakcja na zaistniałe incydenty, lecz jako element szerszej strategii[5]. W tym kontekście „cyber-deterrence" należy postrzegać jako zespół działań ukierunkowanych na zniechęcenie potencjalnych agresorów do podejmowania wrogich działań poprzez wzmacnianie własnych zdolności prewencyjnych i odporności instytucjonalnej[6].

Jednak sposób rozumienia i realizacji cyber-deterrence zależy od uwarunkowań instytucjonalnych, politycznych, prawnych i strategicznych

[1] M. Karpiuk, Cybersecurity as an element in the planning activities of public administration, „Cybersecurity and Law" 2021, nr 1, s. 50.
[2] M. Czuryk, Activities of the Local Government During a State of Natural Disaster, „Studia Iuridica Lublinensia" 2021, nr 4, s. 122.
[3] M. Czuryk, The legal status of digital service providers in the national cybersecurity system, „Cybersecurity and Law" 2024, nr 1, s.. 40.
[4] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, Cybersecurity in the Visegrad Group Countries, Maribor 2023, s. 1.
[5] M. Banasik, L. Chojnowski, Rywalizacja strategiczna w cyberprzestrzeni i jej konsekwencje dla bezpieczeństwa międzynarodowego, „Przegląd Geopolityczny" 2024, nr 48, s. 82-84.
[6] T. Zieliński, Odstraszanie w cyberprzestrzeni. Rola sztucznej inteligencji w budowaniu odporności, atrybucji i skoordynowanej odpowiedzi między domenami, „Cybersecurity and Law" 2025, nr 1, s. 6-9.

poszczególnych państw[7]. Oznacza to, że odstraszanie w cyberprzestrzeni nie przyjmuje jednej, uniwersalnej postaci, lecz jest kształtowane przez specyfikę systemu bezpieczeństwa państwa, strukturę administracji publicznej oraz relacje pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyfrowe[8]. W konsekwencji analiza cyber-deterrence wymaga podejścia uwzględniającego kontekst państwowy i pozwalającego identyfikować odmienne modele funkcjonowania odstraszania cyfrowego. W tym ujęciu Finlandia stanowi szczególnie użyteczny punkt odniesienia, ponieważ rozwiązania przyjęte w jej dokumentach rządowych konsekwentnie łączą cyberbezpieczeństwo z koncepcją bezpieczeństwa kompleksowego oraz z utrzymaniem kluczowych funkcji państwa i społeczeństwa[9]. Wyraża się to zarówno w zaktualizowanej strategii cyberbezpieczeństwa na lata 2024–2035[10], jak i w dokumentach porządkujących system przygotowania państwa, w których cyberprzestrzeń traktowana jest jako element środowiska bezpieczeństwa wymagający koordynacji międzysektorowej[11].

Celem artykułu jest identyfikacja i analiza modeli cyber-deterrence funkcjonujących w Finlandii oraz w pozostałych państwach nordyckich w kontekście bezpieczeństwa państwa. Jednocześnie przyjęcie perspektywy porównawczej pozwala następnie ocenić, w jakim stopniu podobne założenia oraz mechanizmy organizacyjne występują w tych państwach i jakie różnice ujawniają się na poziomie strategii. Takie zestawienie pozwala odróżnić elementy specyficzne dla Finlandii od rozwiązań, które mogą mieć charakter szerszego wzorca regionalnego.

Społeczne i instytucjonalne uwarunkowania cyberbezpieczeństwa państwa

W celu uporządkowania dalszych rozważań należy wskazać podstawowe uwarunkowania społeczne i instytucjonalne, które mają wpływ na cyberbezpieczeństwo w administracji publicznej.

Funkcjonowanie administracji publicznej w warunkach transformacji cyfrowej zależy od kompetencji[12], rozumianych jako zestaw umiejętności i postaw umożliwiających pracę w środowisku cyfrowym, w tym wykorzystywanie danych i narzędzi cyfrowych w realizacji zadań publicznych[13]. W praktyce przekłada się to nie tylko na sprawność obsługi procesów administracyjnych, lecz również na zdolność instytucji do adaptacji do zmieniających się wymagań organizacyjnych

[7] J. Burton, Cyber Deterrence: A Comprehensive Approach?, s. 16, https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf [dostęp: 13.12.2025].

[8] E. D. Borghard, S.W. Lonergan, Deterrence by denial in cyberspace, „Journal of Strategic Studies„ 2023, no. 3, s. 536-562.

[9] Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös, Helsinki 2025, s. 97.

[10] Suomen kyberturvallisuus strategia 2024–2035, Helsinki 2024, https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/fe013d31-1fc0-4d23-b121-9acb09215ec8/content [dostęp: 13.12.2025].

[11] Kyberturvallisuusstrategian toimeenpanosuunnitelma, https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/action-plans/FI_ACTION_PLAN_2024_fi.pdf [dostęp: 13.12. 2025].

[12] A. Bencsik, M. Karpiuk, N. Strizzolo, Information Society Services and their Cybersecurity, „Cybersecurity and Law” 2024, nr 1, s. 259.

[13] M. Burtscher, S. Piano, B. Welby, Developing skills for digital government: A review of good practices across OECD governments, „OECD Social, Employment and Migration Working Papers” 2024, nr 303, s. 13.

i technologicznych[14]. Jednocześnie poziom kompetencji cyfrowych w społeczeństwie pozostaje zróżnicowany, co wpływa na warunki korzystania z usług publicznych oraz na skalę wyzwań stojących przed instytucjami, które te usługi projektują i świadczą[15].

W tym kontekście szczególnie istotne są działania samorządu terytorialnego jako poziomu administracji operującego dużą ilością danych obywateli oraz prowadzącego liczne działania oparte na systemach teleinformatycznych[16]. Z perspektywy bezpieczeństwa informacyjnego kluczowe znaczenie ma fakt, że instytucje publiczne są narażone na szereg zagrożeń takich jak nieuprawniony dostęp do danych i naruszenia ich poufności, przy czym skala szkód może dotyczyć dużej liczby osób[17]. Przykładem ryzyka związanego z przetwarzaniem danych w sektorze publicznym jest przypadek naruszenia dotyczącego jednostki samorządu Helsinek[18]. W ujęciu analitycznym oznacza to, że cyberbezpieczeństwo instytucji samorządowych należy rozpatrywać nie tylko w kategoriach narzędzi technicznych, lecz także w perspektywie procesów zarządzania informacją, kontroli dostępu oraz dojrzałości organizacyjnej.

Jednocześnie niezbędne jest uwzględnienie faktu, że cyfryzacja administracji napotyka bariery o charakterze infrastrukturalnym, kompetencyjnym i organizacyjnym, które wpływają na tempo i jakość wdrożeń[19]. W badaniach porównawczych dotyczących cyfrowej transformacji sektora publicznego podkreśla się, że powodzenie reform zależy od fundamentów instytucjonalnych, w tym zdolności do prowadzenia polityk cyfrowych w sposób spójny oraz zorientowany na użytkownika[20]. W wymiarze praktycznym wyzwania te uwidaczniają się również na poziomie jednostek administracji lokalnej, gdzie analizuje się luki kompetencyjne i potrzeby rozwoju umiejętności z zakresu cyberbezpieczeństwa wśród pracowników administracji publicznej[21].

Zidentyfikowane uwarunkowania społeczne i instytucjonalne stanowią punkt odniesienia dla dalszej analizy rozwiązań przyjmowanych na poziomie państwowym, w których cyberbezpieczeństwo jest integrowane z szerszym systemem bezpieczeństwa i zarządzania kryzysowego.

---

[14] 2023 OECD Digital Government Index, s.7, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/2023-oecd-digital-government-index_b11e8e8e/1a89ed5e-en.pdf [dostęp: 14.12.2025].

[15] C. Gai, M. Karpiuk, A. Spaziani, New Technologies in Public Administration, „Ius et Securitas" 2024, nr 2, s. 50.

[16] E. M. Włodyka, Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa, „Cybersecurity and Law" 2022, nr. 1, s. 218.

[17] I. Bakatsis, Enisa Sectorial Threat Landscape. Public Administration, s. 35-37, https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Public%20Administration%20TL%202024_0.pdf [dostęp: 14.12.2025].

[18] Data breach targeting the City of Helsinki in 2024, https://www.turvallisuustutkinta.fi/material/sites/otkes/otkes/mvyzc49g6/P2024_Helsinki_Investigation_report.pdf [dostęp: 14.12.2025].

[19] E. M. Włodyka, Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku, „Ius et Securitas" 2024, nr 1, s. 72.

[20] Digital Government Index. 2019 Results, „OECD Public Governance Policy Papers" 2019, nr 3, s. 10-13.

[21] R. Yoshinov, M. Kotseva, A. Madzharov, N. Chehlarova, Implying cybersecurity skills for public administration employees, „Environment. Technology. Resources. Rezekne, Latvia Proceedingsof the 15th International Scientific and Practical Conference" 2024, nr 4, s. 301.

Nordycki model odstraszania w cyberprzestrzeni

Próby przenoszenia klasycznych koncepcji odstraszania na grunt cyberprzestrzeni napotykają na istotne ograniczenia, które w praktyce państwowej szybko ujawniają swoje konsekwencje. Jednym z nich pozostaje problem ustalenia odpowiedzialności za prowadzone działania, zwłaszcza w sytuacjach, gdy operacje cyfrowe realizowane są w sposób pośredni lub z wykorzystaniem podmiotów niepaństwowych[22]. W takich przypadkach atrybucja przestaje być jedynie zagadnieniem analitycznym, a staje się warunkiem podejmowania decyzji o charakterze politycznym i strategicznym[23]. Brak jednoznaczności w tym zakresie utrudnia formułowanie reakcji, które mogłyby pełnić funkcję odstraszającą, i osłabia wiarygodność komunikacji państwa wobec potencjalnych przeciwników[24].

Na tym tle szczególnie interesujące są rozwiązania przyjmowane w Finlandii oraz w pozostałych państwach nordyckich, gdzie odstraszanie w cyberprzestrzeni nie jest ujmowane jako odrębny instrument reakcji, ale jako element szerszego systemu bezpieczeństwa państwa[25]. W państwach tych zagadnienia atrybucji, komunikacji strategicznej oraz odporności instytucjonalnej są powiązane z koncepcją bezpieczeństwa kompleksowego, zakładającą ciągłość funkcjonowania administracji, gospodarki i społeczeństwa również w warunkach presji poniżej progu konfliktu zbrojnego[26]. W efekcie cyber-deterrence nie opiera się wyłącznie na groźbie odwetu, lecz na sygnalizowaniu zdolności do identyfikowania zagrożeń, ograniczania ich skutków oraz utrzymania kontroli nad kluczowymi procesami państwowymi[27].

W modelach przyjmowanych w Finlandii oraz w pozostałych państwach nordyckich takie podejście prowadzi do zmiany sposobu rozumienia odstraszania w cyberprzestrzeni. Nie jest ono budowana poprzez deklaracje odwetu, lecz poprzez zdolność państwa do funkcjonowania w warunkach zakłóceń bez utraty kontroli nad procesami decyzyjnymi i administracyjnymi[28]. W praktyce oznacza to, że cyber-deterrence jest oceniane nie na podstawie pojedynczych reakcji na incydenty, lecz przez pryzmat stabilności działania instytucji publicznych oraz przewidywalności zachowań państwa w sytuacjach długotrwałej presji zewnętrznej[29].

---

[22] S. Jeż, Przestępczość cybernetyczna jako metoda adaptacji Koreańskiej Republiki Ludowo-Demokratycznej do reżimu sankcyjnego, „Przegląd Bezpieczeństwa Wewnętrznego” 2025, nr 33, s. 150.

[23] F. J. Egloff, M. Smeets, Publicly attributing cyber attacks: a framework, „Journal of Strategic Studies” 2023, no. 3, s. 504-505.

[24] J. R. Lindsay, Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, „Journal of Cybersecurity” 2015, nr 1, s. 54-58.

[25] M. Keinonen, The Concept of Comprehensive Security as a Tool for Cyber Deterrence, „Proceedings of the 22nd European Conference on Cyber Warfare and Security” 2023, nr 1, s. 568-569.

[26] J. Wrange, R. Bengtsson, D. Brommesson, Resilience through total defence: Towards a shared security culture in the Nordic–Baltic region?, „European Journal of International Security” 2024, nr 4, s. 512-514.

[27] E. Lonergan, M. Montgomery, What is the Future of Cyber Deterrence?, „Review of International Affairs” 2021, no. 2, s. 61-62.

[28] M. Keinonen, Cyber Deterrence of a Small State, „National Defence University Research Publications” 2025, no. 70, s. 4-5.

[29] A. Longo, A. A. Ardebili, A. Lazari, A. Ficarella, Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks, „Electronics” 2025, no. 8, s. 29-30.

Wspólną cechą podejść rozwijanych w państwach nordyckich jest traktowanie cyberbezpieczeństwa jako obszaru powiązanego z odpornością państwa, a nie jako wyizolowanej domeny technicznej[30]. W dokumentach strategicznych akcentuje się ochronę „kluczowych" lub „żywotnych" funkcji społeczeństwa (administracji, usług publicznych i infrastruktury krytycznej) oraz zdolność do utrzymania ich działania w warunkach zakłóceń[31].

Przesuwa to środek ciężkości z samej reakcji na incydent na zarządzanie ryzykiem, gotowość i ciągłość działania. W tym ujęciu istotne staje się praktykowane w państwach nordyckich budowanie rozwiązań przekrojowych takich jak koordynacja między resortami i agencjami, współpraca z operatorami usług kluczowych i sektorem prywatnym, rozwijanie jednolitych wymogów dla administracji publicznej oraz ćwiczenia i procedury wspólnego reagowania. Z perspektywy cyber-deterrence oznacza to, że odstraszanie jest w tych państwach wzmacniane przez przewidywalny, systemowy charakter przygotowań – przeciwnik otrzymuje sygnał nie tylko o zdolności do identyfikacji i ograniczania skutków zakłóceń, ale także o spójności instytucjonalnej i odporności procesów decyzyjnych, które uniemożliwiają lub utrudniają osiągnięcie celów atakujących.

Specyfika cyber-deterrence Finlandii

Specyfika cyber-deterrence Finlandii wynika z odmiennego sposobu myślenia o bezpieczeństwie państwa niż ten, który dominuje w innych krajach. W fińskim ujęciu odstraszanie w cyberprzestrzeni nie zostało wyodrębnione jako samodzielny element polityki ani przypisane wyłącznie do struktur technicznych lub wojskowych[32]. Zamiast tego zostało ono włączone w szerszy model bezpieczeństwa kompleksowego, obejmujący funkcjonowanie administracji publicznej na każdym szczeblu, gospodarki, badań naukowych oraz społeczeństwa w warunkach zakłóceń i w sytuacjach kryzysowych[33].

Jednym z elementów wyraźnie odróżniających Finlandię od innych państw jest sposób organizacji współpracy między podmiotami odpowiedzialnymi za bezpieczeństwo. Cyberbezpieczeństwo nie jest tam traktowane jako domena jednego resortu, lecz jako obszar wymagający stałej koordynacji między administracją rządową, samorządem terytorialnym, operatorami usług kluczowych oraz sektorem prywatnym[34]. W praktyce oznacza to, że działania mające znaczenie odstraszające są rozproszone pomiędzy różne instytucje, ale jednocześnie osadzone w spójnym systemie[35]. Na tle innych państw charakterystyczne jest również to, że fińskie cyber-deterrence nie opiera się na komunikowaniu gotowości do odwetu. Zdolność odstraszania budowana jest

---

30 Kyberturvallisuus ja kybertoimintaympäristö, https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto [dostęp: 14.12.2025].

31 L. Jauhiainen, S. Schiffling, Comparing the resilience objectives of Finnish comprehensive security model and the NATO baseline requirements for resilience, „Journal of Military Studies" 2025, no. 1, s. 2-3.

32 Kyberturvallisuuden palvelut ja yhteistyöverkostot, https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2024/kyberturvallisuuden-palvelut-ja-yhteistyoverkostot [dostęp: 14.12.2025].

33 What is comprehensive security?, https://turvallisuuskomitea.fi/en/comprehensive-security/ [dostęp: 14.12.2025].

34 Digitoimiston yhteistyöryhmät, https://vm.fi/yhteistyoryhmat [dostęp: 14.12.2025].

35 Digitaalinen turvallisuus ja kyberturvallisuus, https://www.kuntaliitto.fi/kuntajohtaminen-ja-digitalisaatio/digitaalinen-turvallisuus [dostęp: 14.12.2025].

raczej poprzez wykazywanie odporności instytucjonalnej i zdolności do utrzymania ciągłości działania administracji publicznej[36].

Odrębność fińskiego podejścia widoczna jest także w sposobie rozwijania narzędzi wspierających orientację sytuacyjną w cyberprzestrzeni. Rozwiązania te są projektowane z myślą o szerokim gronie użytkowników, a nie wyłącznie o wąskich strukturach eksperckich[37]. Pozwala to na wcześniejsze identyfikowanie zagrożeń oraz lepszą synchronizację działań między instytucjami publicznymi a podmiotami odpowiedzialnymi za realizację usług o znaczeniu krytycznym. W wielu innych państwach podobne funkcje pozostają rozproszone lub ograniczone do struktur technicznych, co utrudnia osiągnięcie efektu systemowego. Natomiast w porównaniu z innymi państwami nordyckimi Finlandia wyróżnia się konsekwencją w traktowaniu cyberbezpieczeństwa jako elementu długofalowej polityki przygotowań społeczeństwa. Cyber-deterrence nie jest tam postrzegane jako zestaw narzędzi reagowania na incydenty, lecz jako rezultat trwałego procesu wzmacniania zdolności instytucjonalnych[38]. Takie podejście sprzyja zmniejszeniu poziomu podatności państwa na wrogie działania w cyberprzestrzeni.

W rezultacie fiński model cyber-deterrence różni się od wielu innych rozwiązań tym, że jego skuteczność nie wynika z potencjału eskalacyjnego, lecz z ograniczania możliwości osiągnięcia celów przez podmiot oddziałujący. Odstraszanie ma tu charakter pośredni i systemowy, a jego podstawą pozostaje spójność instytucjonalna oraz zdolność państwa do funkcjonowania w warunkach zakłóceń, a nie demonstracja siły w cyberprzestrzeni. Jednak jedną z najważniejszych cech fińskiego modelu cyber-deterrence jest społeczna świadomość realności istnienia zagrożeń cyfrowych. Powoduje to, że mieszkańcy Finlandii są w o wiele mniejszym stopniu podatni na szerokorozumiane zagrożenia cyfrowe już na poziomie jednostek.

Podsumowanie

Przeprowadzone w artykule analizy pozwalają potwierdzić, że cyber-deterrence w Finlandii i państwach nordyckich funkcjonuje w odmiennym paradygmacie niż klasyczne, znane z domeny militarnej, modele. Zamiast akcentowania zdolności eskalacyjnych lub komunikowania gotowości do odwetu, odstraszanie w cyberprzestrzeni opiera się tam na długofalowym wzmacnianiu odporności instytucjonalnej, spójności organizacyjnej oraz zdolności państwa do utrzymania ciągłości kluczowych funkcji w warunkach zakłóceń. Tym samym zrealizowany został cel artykułu, jakim była identyfikacja i analiza modeli cyber-deterrence funkcjonujących w Finlandii i państwach nordyckich w kontekście bezpieczeństwa państwa.

Wyniki analizy wskazują, że cyberbezpieczeństwo nie może być rozpatrywane w oderwaniu od szerszych procesów społecznych i gospodarczych zachodzących w warunkach dynamicznej transformacji cyfrowej. Postęp

[36] National Cyber Security Centre Finland, https://kyberturvallisuuskeskus.fi/en [dostęp: 14.12.2025].

[37] Havainnointi ja avunanto, https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto [dostęp: 15.12.2025].

[38] Cyber Security Strategy implementation plan published – cybersecurity integrated into comprehensive security, https://defmin.fi/en/-/1410829/cyber-security-strategy-implementation-plan-published-cybersecurity-integrated-into-comprehensive-security#1ea71de4 [dostęp: 15.12. 2025].

w dziedzinie technologii informacyjno-komunikacyjnych prowadzi do jakościowych zmian również na rynku pracy, co stało się szczególnie widoczne w okresie pandemii COVID-19, kiedy część dotychczasowych profesji traciła znaczenie, a jednocześnie pojawiało się zapotrzebowanie na nowe kompetencje cyfrowe[39]. Zjawiska te wpływają bezpośrednio na funkcjonowanie administracji publicznej oraz na sposób świadczenia usług publicznych, zwiększając jednocześnie znaczenie bezpieczeństwa systemów teleinformatycznych.

W państwach demokratycznych szczególnym obszarem podatności pozostają procesy wyborcze, które w warunkach cyfryzacji stają się potencjalnym celem oddziaływań zewnętrznych[40]. Zagrożenia te dotyczą nie tylko samego przebiegu kampanii wyborczych, lecz również integralności systemów wykorzystywanych do liczenia głosów i zarządzania procesem wyborczym. W tym kontekście cyberbezpieczeństwo nabiera znaczenia ustrojowego, a jego brak może prowadzić do podważenia zaufania społecznego do instytucji państwa.

Analiza potwierdza również, że zapewnienie bezpieczeństwa pozostaje podstawowym zadaniem państwa, niezależnie od zmieniających się form zagrożeń[41]. Współczesne społeczeństwa, funkcjonujące w warunkach rosnącej globalizacji i przyspieszonego tempa zmian technologicznych, muszą dostosowywać się do nowych norm, wartości[42]. Zagrożenia i konflikty stanowią trwały element życia społecznego oraz funkcjonowania państw[43], przy czym w środowisku cyfrowym przybierają one formy trudniejsze do jednoznacznej identyfikacji i reakcji.

W tym kontekście cyberbezpieczeństwo staje się kluczowym warunkiem sprawnego funkcjonowania zarówno administracji publicznej, jak i społeczności lokalnych[44]. Rosnące uzależnienie od technologii informacyjnych sprawia, że zakłócenia w cyberprzestrzeni mogą bezpośrednio wpływać na realizację usług publicznych oraz funkcjonowanie infrastruktury krytycznej[45]. Dotyczy to w szczególności współczesnych miast, których działanie w coraz większym stopniu opiera się na zintegrowanych systemach cyfrowych, narażonych na cyberataki i awarie o charakterze systemowym[46].

Przeprowadzone rozważania prowadzą do wniosku, że transformacja cyfrowa nie powinna ograniczać się do rozbudowy infrastruktury technicznej ani do doraźnych modernizacji systemów informatycznych[47]. Skuteczne cyber-

[39] E. M. Włodyka, Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim, „Acta Politica Polonica" 2021, nr 2, s. 91.

[40] E. M. Włodyka, Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce, [w:] Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe, red. M. Karpiuk, Warszawa 2024, s. 116.

[41] M. Czuryk, Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1, s. 6.

[42] D. Cholewińska, Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia, „Ius et Securitas" 2025, nr 1, s. 49.

[43] A. Pieczywok, Wirtualna przestrzeń edukacji człowieka, „Ius et Securitas" 2025, nr 1, s. 54.

[44] P. Krauze-Maślankowska, D. Majewicz, Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland, „Ius et Securitas" 2025, nr 2, s. 56.

[45] M. Karpiuk, Crisis management vs. cyber threat, "Sicurezza, terrorismo e società" 2022, nr 16 s. 121.

[46] N. Moch, W. Wereda, Management of Urban Security and New Technologies, „European Research Studies Journal" 2024, no. 4, s. 1319.

[47] V. Constantinov, M. Karpiuk, N. Strizzolo, Cybersecurity Incidents as Threats to National and International Security, „Ius et Securitas" 2025, nr 2, s. 7.

deterrence wymaga spójnych, długofalowych decyzji strategicznych, stabilnych ram instytucjonalnych oraz koordynacji działań między różnymi szczeblami administracji i sektorami gospodarki. Przypadek Finlandii pokazuje, że włączenie cyberbezpieczeństwa w model bezpieczeństwa kompleksowego może skutecznie ograniczać podatność państwa na presję zewnętrzną, nawet w warunkach narastających zagrożeń poniżej progu konfliktu zbrojnego.

Z perspektywy dalszych badań zasadne wydaje się pogłębienie analiz porównawczych obejmujących inne państwa europejskie, w szczególności te, które deklarują wdrażanie podejścia odpornościowego w cyberprzestrzeni, lecz realizują je w odmiennych uwarunkowaniach instytucjonalnych. Interesującym kierunkiem badawczym pozostaje również empiryczna ocena skuteczności cyber-deterrence opartego na odporności w kontekście konkretnych incydentów oraz długotrwałych kampanii oddziaływań niekinetycznych.

Bibliografia

2023 OECD Digital Government Index, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/2023-oecd-digital-government-index_b11e8e8e/1a89ed5e-en.pdf [dostęp: 14.12.2025].

Bakatsis I., Enisa Sectorial Threat Landscape. Public Administration, https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Public%20 Administration%20TL%202024_0.pdf [dostęp: 14.12.2025].

Banasik M., Chojnowski L., Rywalizacja strategiczna w cyberprzestrzeni i jej konsekwencje dla bezpieczeństwa międzynarodowego, „Przegląd Geopolityczny" 2024, nr 48.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., Cybersecurity in the Visegrad Group Countries, Maribor 2023.

Bencsik A., Karpiuk M., Strizzolo N, Information Society Services and their Cybersecurity, „Cybersecurity and Law" 2024, nr 1.

Borghard E. D., Lonergan S. W., Deterrence by denial in cyberspace, „Journal of Strategic Studies„ 2023, nr 3.

Burton J., Cyber Deterrence: A Comprehensive Approach?, https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf [dostęp: 13.12.2025].

Burtscher M., Piano S., Welby B., Developing skills for digital government: A review of good practices across OECD governments, „OECD Social, Employment and Migration Working Papers" 2024, no. 303.

Cholewińska D., Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia, „Ius et Securitas" 2025, nr 1.

Constantinov V., Karpiuk M., Strizzolo, N. Cybersecurity Incidents as Threats to National and International Security, „Ius et Securitas" 2025, nr 2.

Cyber Security Strategy implementation plan published – cybersecurity integrated into comprehensive security, https://defmin.fi/ en/-/1410829/cyber-security-strategy-implementation-plan-published-cybersecurity-integrated-into-comprehensive-security#1ea71de4 [dostęp: 15.12.2025].

Czuryk M., Activities of the Local Government During a State of Natural Disaster, „Studia Iuridica Lublinensia" 2021, nr 4.

Czuryk M., The legal status of digital service providers in the national cybersecurity system, „Cybersecurity and Law" 2024, nr 1.

Czuryk M., Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1.

Data breach targeting the City of Helsinki in 2024, https://www.turvallisuustutkinta.fi/material/sites/otkes/otkes/mvyzc49g6/P2024_ Helsinki_Investigation_report.pdf [dostęp: 14.12.2025].

Digitaalinen turvallisuus ja kyberturvallisuus, https://www.kuntaliitto.fi/kuntajohtaminen-ja-digitalisaatio/digitaalinen-turvallisuus [dostęp: 14.12.2025].
Digital Government Index. 2019 Results, „OECD Public Governance Policy Papers" 2019, no. 3.
Digitoimiston yhteistyöryhmät, https://vm.fi/yhteistyoryhmat [dostęp: 14.12.2025].
Egloff F. J., Smeets M., Publicly attributing cyber attacks: a framework, „Journal of Strategic Studies" 2023, no. 3.
Gai C., Karpiuk M., Spaziani A., New Technologies in Public Administration, „Ius et Securitas" 2024, nr 2.
Havainnointi ja avunanto, https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto [dostęp: 15.12.2025].
Jauhiainen L., Schiffling S., Comparing the resilience objectives of Finnish comprehensive security model and the NATO baseline requirements for resilience, „Journal of Military Studies" 2025, no. 1.
Jeż S., Przestępczość cybernetyczna jako metoda adaptacji Koreańskiej Republiki Ludowo-Demokratycznej do reżimu sankcyjnego, „Przegląd Bezpieczeństwa Wewnętrznego" 2025, nr 33.
Karpiuk M., Crisis management vs. cyber threat, „Sicurezza, terrorismo e società" 2022, no. 16.
Karpiuk M., Cybersecurity as an element in the planning activities of public administration, „Cybersecurity and Law" 2021, nr 1.
Keinonen M., Cyber Deterrence of a Small State, „National Defence University Research Publications" 2025, no. 70.
Keinonen M., The Concept of Comprehensive Security as a Tool for Cyber Deterrence, „Proceedings of the 22nd European Conference on Cyber Warfare and Security" 2023, no. 1.
Krauze-Maślankowska P., Majewicz D., Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland, „Ius et Securitas" 2025, nr 2.
Kyberturvallisuuden palvelut ja yhteistyöverkostot, https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2024/kyberturvallisuuden-palvelut-ja-yhteistyoverkostot [dostęp: 14.12.2025].
Kyberturvallisuus ja kybertoimintaympäristö, https://um.fi/kyberturvallisuus-ja-kybertoimintaympariston [dostęp: 14.12.2025].
Kyberturvallisuusstrategian toimeenpanosuunnitelma, https://www. enisa.europa.eu/sites/default/files/ncss-map/strategies/action-plans/FI_ACTION_PLAN_2024_fi.pdf [dostęp: 13.12.2025].
Lindsay J. R., Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, „Journal of Cybersecurity" 2015, no. 1.
Lonergan E., Montgomery M., What is the Future of Cyber Deterrence?, „Review of International Affairs" 2021, no. 2.
Longo A., Ardebili A. A., Lazari A., Ficarella A., Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks, „Electronics" 2025, no. 8.
Moch N., Wereda W., Management of Urban Security and New Technologies, „European Research Studies Journal" 2024, no. 4.
National Cyber Security Centre Finland, https://kyberturvallisuuskeskus.fi/en [dostęp: 14.12.2025].
Pieczywok A., Wirtualna przestrzeń edukacji człowieka, „Ius et Securitas" 2025, nr 1.
Suomen kyberturvallisuus strategia 2024–2035, Helsinki 2024, https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/fe013d31-1fc0-4d23-b121-9acb09215ec8/content [dostęp: 13.12.2025].
What is comprehensive security?, https://turvallisuuskomitea.fi/en/comprehensive-security/ [dostęp: 14.12.2025].
Włodyka E. M., Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim, „Acta Politica Polonica" 2021, nr 2.

Włodyka E. M., Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa, „Cybersecurity and Law" 2022, nr 1.

Włodyka E. M., Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku, „Ius et Securitas" 2024, nr 1.

Włodyka E.M., Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce, [w:] M. Karpiuk (red.), Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe, Warszawa 2024.

Wrange J., Bengtsson R., Brommesson D., Resilience through total defence: Towards a shared security culture in the Nordic–Baltic region?, „European Journal of International Security" 2024, no. 4.

Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös, Helsinki 2025.

Yoshinov R., Kotseva M., Madzharov A., Chehlarova N., Implying cybersecurity skills for public administration employees, „Environment. Technology. Resources. Rezekne, Latvia Proceedingsof the 15th International Scientific and Practical Conference" 2024, nr 4.

Zieliński T., Odstraszanie w cyberprzestrzeni. Rola sztucznej inteligencji w budowaniu odporności, atrybucji i skoordynowanej odpowiedzi między domenami, „Cybersecurity and Law" 2025, nr 1.