KRZYSZTOF KACZMAREK

Bezpieczeństwo państwa wobec współczesnych zagrożeń

Security of the State in the Face of Contemporary Threats

Abstract

This article analyses the issue of systemic state security in the context of contemporary threats of a complex and dynamic nature. The adopted research hypothesis assumed that effective development of systemic resilience requires cooperation between public administration, the private sector, non-governmental organisations, and citizens, alongside the development of adaptive mechanisms. The study applied a literature review method, supplemented by references to the experiences of selected countries, with particular emphasis on the Finnish model. The analysis indicated the key importance of social trust, institutional flexibility, and broad cross-sectoral cooperation in shaping the long-term resilience of the state to systemic threats.

KEYWORDS: systemic security, state resilience, crisis management, adaptability

SŁOWA KLUCZOWE: bezpieczeństwo systemowe, odporność państwa, zarządzanie kryzysowe, adaptacyjność

KRZYSZTOF KACZMAREK – doktor nauk o polityce i administracji, Politechnika Koszalińska, ORCID – 0000-0001-8519-1667, e-mail: krzysztof.kaczmarek@tu.koszalin.pl

HTTPS://DOI.ORG/10.36128/PRIW.VI58.1382

1 Wstęp

Postęp w dziedzinie technologii cyfrowych sprawia, że zmieniają się niemal wszystkie aspekty funkcjonowania jednostek, społeczeństw, organizacji i państw. Ponieważ znaczna część aktywności społecznych przeniosła się do świata cyfrowego, cyberprzestrzeń redefiniuje dotychczasowe kategorie bezpieczeństwa i tworzy nowe parametry ryzyka[1]. Jednocześnie dynamika zachodzących w otoczeniu człowieka zmian powoduje, że ludzkość ma trudności w przystosowaniu się do funkcjonowania w nowym środowisku bezpieczeństwa.

Biorąc pod uwagę, że rodzaj i skala współczesnych zagrożeń wykazują tendencje ewolucyjne, a zmiany zachodzą znacznie szybciej niż kiedykolwiek wcześniej, istotne jest zaangażowanie zarówno pojedynczego obywatela, jak i innych podmiotów powołanych do realizacji określonych zadań w celu zapewnienia ciągłości istnienia i bezpieczeństwa państwa. Szczególną uwagę należy zwrócić na zapewnienie, aby wspomniana ciągłość była zachowana na każdym etapie funkcjonowania państwa, tj. w stanie pokoju, kryzysu i wojny, co z kolei jest determinowane przez utrzymanie gotowości obronnej państwa w oparciu o sprawność struktur zarówno rządowych, jak i samorządowych[2]. Dlatego też zachowanie wysokiego poziomu bezpieczeństwa jest niezbędne dla unikania zagrożeń istotnych dla prawidłowego funkcjonowania państwa i jego instytucji[3].

W tej nowej rzeczywistości szczególnego znaczenia nabiera bezpieczeństwo systemowe, rozumiane jako zdolność państwa i jego instytucji do funkcjonowania zarówno w czasie pokoju, jak i w sytuacjach kryzysowych, w tym także w obliczu konfliktu zbrojnego. Jednocześnie coraz większego znaczenia nabierają narzędzia cyfrowe, które pozwalają na automatyzację procesów administracyjnych – w tym rozwiązania oparte na sztucznej inteligencji (ang. Artificial Intelligence, dalej: AI). Chociaż narzędzie to posiada znaczny potencjał w zakresie poprawy usług publicznych, kluczowe

1 Christophe Gaie, Mirosław Karpiuk i Nicola Strizzolo, "Cybersecurity of Public Sector Institutions," *Prawo i Więź*, nr 6 (2024): 351.

2 Magdalena Bsoul-Kopowska, Aleksandra Skrabacz i Jarosław Rodzik, "The Crucial Role of Crisis Management Teams in Public Administration in the Context of COVID-19," *Polish Journal of Management Studies*, nr 1 (2022): 108.

3 Mirosław Karpiuk, Claudio Melchior i Urszula Soler, "Cybersecurity Management in the Public Service Sector," *Prawo i Więź*, nr 4 (2023): 8.

znaczenie ma jego skuteczne i bezpieczne wdrożenie[4]. W związku z tym w dobie społeczeństwa informacyjnego i państwa, którego funkcjonowanie w dużej mierze opiera się na systemach teleinformatycznych, gdzie usługi cyfrowe mają charakter powszechny, cyberbezpieczeństwo staje się szczególnie ważne[5].

Zatem zarówno struktury państwa, przedsiębiorstwa, jak i jednostki powinny zawsze brać pod uwagę wszystkie możliwe czynniki ryzyka – technologiczne, społeczne i organizacyjne, a podejście do bezpieczeństwa cyfrowego powinno być holistyczne[6].

W związku z powyższym w niniejszym artykule przyjęto hipotezę, zgodnie z którą skuteczne budowanie odporności systemowej państwa wymaga współdziałania administracji publicznej, sektora prywatnego, organizacji pozarządowych oraz obywateli, a także rozwijania mechanizmów adaptacyjnych pozwalających na elastyczne reagowanie na zmieniające się zagrożenia.

Celem artykułu jest identyfikacja i analiza kluczowych czynników kształtujących odporność systemową państwa w warunkach współczesnych wyzwań bezpieczeństwa. W szczególności zwrócono uwagę na znaczenie modelu współodpowiedzialności społecznej oraz zdolności adaptacyjnych instytucji publicznych. W pracy zastosowano metodę analizy literatury przedmiotu, uzupełnioną o odniesienia do rozwiązań funkcjonujących w wybranych państwach, w tym zwłaszcza w Finlandii, która uznawana jest za przykład rozwiniętego modelu odporności systemowej.

4 Dominik Bierecki, Christophe Gaie i Mirosław Karpiuk, "Artificial Intelligence in e-Administration," *Prawo i Więź*, nr 1 (2025): 385.

5 Mirosław Karpiuk, "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity," *Studia Iuridica Lublinensia*, nr 2 (2023): 190.

6 Krzysztof Kaczmarek, Mirosław Karpiuk i Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data," *Prawo i Więź*, nr 3 (2024): 105.

2 Wprowadzenie do problematyki bezpieczeństwa systemowego i odporności

Szybki rozwój nowych technologii informacyjno-komunikacyjnych spowodował szerokie wykorzystanie nowych narzędzi, takich jak Internet, telefonia komórkowa i AI, w różnych sferach, w tym w administracji publicznej[7]. AI jest obecnie najbardziej zaawansowanym pod względem technicznym narzędziem. W literaturze przedmiotu jest to ogólny termin obejmujący każdy rodzaj oprogramowania lub sprzętu, który obsługuje uczenie maszynowe, widzenie komputerowe, rozumienie i generowanie języka naturalnego, przetwarzanie języka naturalnego i robotykę[8]. Obecnie, dzięki możliwości analizowania danych i znajdowania wzorców o wiele szybciej, niż człowiek byłby kiedykolwiek w stanie, narzędzia AI mogą wspomagać każdy rodzaj działalności naukowej, administracyjnej, obronnej, finansowej czy marketingowej, a rozwijająca się technologia jest jednym z czynników rozwoju społeczeństwa[9].

Systemy AI mogą analizować dane o wypadkach drogowych, aby identyfikować najczęstsze przyczyny kolizji i sugerować zmiany w infrastrukturze drogowej lub oznakowaniu, które mogłyby zapobiec przyszłym wypadkom[10]. Ponadto AI może być używana do monitorowania zachowań kierowców i wykrywania niebezpiecznych sytuacji, takich jak jazda pod wpływem alkoholu lub zmęczenie kierowcy[11]. Należy jednak pamiętać, że jak każde inne narzędzie, systemy, których działanie opiera się na AI, nie są wolne od błędów. Zatem bezkrytyczne podejście do analiz przeprowadzanych przez algorytmy jest ryzykowne i stanowi czynnik ryzyka zarówno

7 Ewa Maria Włodyka, "Implementation of e-Government and Artificial Intelligence in Polish Public Administration," *TalTech Journal of European Studies*, nr 2 (2024): 120.

8 Krzysztof Kaczmarek, "Sztuczna inteligencja," w *Leksykon cyberbezpieczeństwa*, red. Katarzyna Chałubińska-Jentkiewicz (Warszawa: Akademia Sztuki Wojennej, 2024), 251 – 252.

9 Dagmara Cholewińska, "Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia," *Ius et Securitas*, nr 1 (2025): 49.

10 Krzysztof Kaczmarek, Mirosław Karpiuk i Andrea Spaziani, "Use of Artificial Intelligence in Public Sector: Threats and Prospects," *Studia Iuridica Toruniensia*, nr 1 (2025): 34.

11 Aleksandra Skrabacz, Magdalena Bsoul-Kopowska i Bartosz Kozicki, "The Application of Artificial Intelligence in Road Traffic Management and Its Safety Improvement," *Transport Problems*, nr 4 (2024): 11.

dla osób prywatnych, jak i instytucji. Jednym z przejawów zagrożenia bezpieczeństwa publicznego może być kusząca chęć pełnej automatyzacji niektórych procesów, np. informacyjnych, przez administrację publiczną[12].

Jednocześnie należy podkreślić, że sprawne funkcjonowanie zarówno usług publicznych, jak i komercyjnych wymaga gromadzenia i wykorzystywania dużych zasobów danych, które są konieczne w dostosowaniu się do wyzwań wynikających z rozwoju i implementacji AI. Współcześnie dane te odgrywają rolę jednego z najważniejszych zasobów w procesach gospodarczych i administracyjnych[13].

Wszystkie te czynniki powodują, że współczesny świat przechodzi przemiany na szeroką skalę w niemal wszystkich obszarach relacji społecznych. Poza rewolucją informacyjną do rosnących na znaczeniu czynników ryzyka należy zaliczyć również zmiany klimatu, szybkość rozprzestrzeniania się chorób zakaźnych, antropogeniczne obciążenie środowiska oraz dematerializację znacznej części produkcji. Jednocześnie każdy element postępu technologicznego i cywilizacyjnego powoduje, że środowisko bezpieczeństwa charakteryzuje się coraz mniejszą stabilnością. Odpowiedzią na związane z tym wyzwania jest budowanie i wzmacnianie odporności, które powinno polegać na formułowaniu i wdrażaniu kierunków polityk publicznych nakierowanych na przeciwdziałanie zagrożeniom dowolnego pochodzenia i charakteru[14].

Należy jednak brać pod uwagę to, że odporność systemu to złożona koncepcja, której nie można analizować tylko z jednej perspektywy. Jest to również cecha zmienna, ponieważ po odzyskaniu przez system początkowej równowagi lub przejściu w nowy stan wymagany jest proces ciągłego dostosowywania się do nowych warunków. Zatem odporność należy traktować jako proces, a nie stan[15]. Istnieją również przykłady, które wskazują, że wymuszone sytuacjami kryzysowymi zmiany okazują się pozytywne nawet po ustąpieniu czynników zakłócających normalne funkcjonowanie.

---

12 Ewa Maria Włodyka, "Artificial Intelligence as a Supporting Tool for Local Government Decision-Making in Public Safety," *Przegląd Nauk o Obronności*, nr 17 (2024): 86.

13 Christophe Gaie, Mirosław Karpiuk i Andrea Spaziani, "Cybersecurity in France, Poland and Italy," *Studia Iuridica Lublinensia*, nr 1 (2025): 91.

14 Olga Reznikova, *National Resilience in Changing Security Environment* (Kyiv: National Institute for Strategic Studies, 2022), 7.

15 Alina Georgiana Profiroiu i Corina-Cristiana Nastacă, "What Strengthens Resilience in Public Administration Institutions?," *Eastern Journal of European Studies*, nr 12 (2021): 102.

Potrzeba budowania odporności społecznej stała się szczególnie widoczna w czasie pandemii COVID-19. Wówczas rozpoczęto wiele badań nad odpornością, zwracając szczególną uwagę na funkcjonowanie gospodarki. Wprowadzone wtedy ograniczenia spowodowały spowolnienie gospodarki globalnej. Najbardziej ucierpiały takie branże jak turystyka i usługi. Restrykcje spowodowały również, w wyniku zakłóceń w globalnych łańcuchach dostaw, spadek produkcji przemysłowej. Natomiast ówczesna sytuacja wymusiła przyśpieszoną cyfryzację handlu i usług społecznych[16].

Współczesne środowisko bezpieczeństwa wymaga, aby systemowa odporność państwa była budowana w oparciu o zintegrowane podejście, w którym kluczową rolę odgrywają rozwój technologiczny, organizacja struktur administracyjnych oraz zdolność społeczeństwa i jednostek do współpracy i adaptacji.

3 Główne obszary i filary bezpieczeństwa systemowego państwa

Bezpieczeństwo systemowe obejmuje budowanie odporności zarówno na zagrożenia bezpośrednie (katastrofy naturalne, wypadki komunikacyjne, awarie technologiczne, ataki terrorystyczne, działania wojenne, epidemie), jak i pośrednie (zmiany klimatyczne, degradacja środowiska, długofalowe skutki różnego rodzaju skażeń, kryzysy zdrowotne o podłożu cywilizacyjnym). Zagrożenia te mogą również prowadzić do poważnych konsekwencji dla życia i zdrowia, kumulując skutki i zwiększając ryzyko destabilizacji systemu[17].

W tym kontekście istotne jest również bezpieczeństwo ekologiczne, które należy rozumieć jako zapewnienie warunków do istnienia i rozwoju

16 Sergiu Gherghina, Clara Volintiru i Throstur Olaf Sigurjonsson, "Making a Difference: The Effects of Institutional Resilience in Society During COVID19," *European Political Science*, nr 1 (2022): 428.

17 Mirosław Karpiuk, "Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)," *Studia Iuridica Lublinensia*, nr 1 (2019): 185.

istot ludzkich i innych gatunków biologicznych[18]. Istotnym elementem odporności jest także zapewnienie neutralności światopoglądowej instytucji i struktur państwa, co w reżimach demokratycznych sprzyja stabilności społecznej i minimalizowaniu napięć mogących potencjalnie destabilizować system[19].

Kolejnym kluczowym elementem bezpieczeństwa systemowego jest zaufanie społeczne wobec grup dyspozycyjnych, które mają możliwość skutecznego działania tylko wtedy, gdy ich działania spotykają się z akceptacją obywateli. To jednak wymaga, aby media i społeczeństwa, zwłaszcza na szczeblu lokalnym, uważnie monitorowały działania członków tych grup, głośno potępiając wszelkie powodowane przez nich naruszenia norm prawnych i zwyczajowych[20].

Do niemilitarnych podstaw bezpieczeństwa systemowego można zaliczyć:

- bezpieczeństwo polityczne, które odnosi się do ochrony suwerenności państwa i jego systemu politycznego oraz zapewnienia społeczeństwu ochrony przed bezprawnymi zagrożeniami wewnętrznymi i zewnętrznymi. Obejmuje ono zarówno bezpieczeństwo państwa, jak i wewnętrzne oraz działania organów ścigania;
- bezpieczeństwo ekonomiczne, które dotyczy nie tylko ochrony zdolności gospodarki do zaspokajania potrzeb ludności, ale również stopnia, w jakim państwo i obywatele mają możliwość samodzielnego podejmowania decyzji ekonomicznych. Obejmuje także ochronę majątku narodowego i wolności gospodarczej przed zagrożeniami zewnętrznymi i presją polityczną. W jego zakres wchodzą polityka gospodarcza, działania niektórych służb państwowych oraz międzynarodowe umowy handlowe i finansowe;
- bezpieczeństwo energetyczne i zasobów naturalnych, które najczęściej definiuje się jako stopień dostępu państwa i jego obywateli do

18 Jarosław Kostrubiec, Mirosław Karpiuk i Dominik Tyrawa, "The Status of Municipal Government in the Sphere of Ecological Security," *Hungarian Journal of Legal Studies*, nr 2 (2024): 165.

19 Małgorzata Czuryk, "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd," *Studia z Prawa Wyznaniowego*, nr 27 (2024): 158.

20 Aleksandra Skrabacz, "Migrations as a Challenge for Dispositional Groups in Polish and European Comparative Perspectives," *Journal of Eastern Europe Research in Business and Economics*, Article ID 290391 (2021): 5.

zasobów takich jak ropa naftowa, gaz, woda czy surowce mineralne. Precyzyjniej można je określić jako swobodny dostęp do tych zasobów, kształtowany przez mechanizmy rynkowe, bez ingerencji ze strony innych państw czy podmiotów politycznych bądź wojskowych;

- bezpieczeństwo wewnętrzne obejmujące szereg funkcji związanych z ochroną państwa na jego własnym terytorium. Obejmuje ono m.in. ochronę lotnisk i portów, zabezpieczenie granic, bezpieczeństwo transportu, kontrolę imigracji oraz inne powiązane obszary;
- cyberbezpieczeństwo, które odnosi się do ochrony infrastruktury teleinformatycznej państwa i obywateli, w tym systemów komputerowych i przetwarzania danych, przed szkodliwą ingerencją z zewnątrz lub z wewnątrz kraju. Obejmuje ono zarówno obronę narodową i bezpieczeństwo wewnętrzne, jak i działania organów ścigania;
- bezpieczeństwo humanitarne, które jest koncepcją rozwijaną głównie w ramach Organizacji Narodów Zjednoczonych (dalej: ONZ) po zakończeniu zimnej wojny. Obejmuje ona ochronę ludzi przed głodem, chorobami, represjami i destabilizacją codziennego życia. Z czasem koncepcja ta została rozszerzona i obecnie zawiera również bezpieczeństwo ekonomiczne, środowiskowe, żywnościowe, zdrowotne, osobiste, wspólnotowe, polityczne oraz ochronę kobiet i mniejszości. Jej charakterystyczną cechą jest unikanie tradycyjnego ujęcia bezpieczeństwa jako problemu militarnego pomiędzy państwami i skupianie się na społecznych i ekonomicznych przyczynach zagrożeń oraz na międzynarodowej odpowiedzialności za ochronę ludności przed przemocą. Koncepcja ta ma być realizowana i nadzorowana przez ONZ;
- bezpieczeństwo środowiskowe, które jest pojęciem wieloznacznym. Tradycyjnie wiązano je z przeciwdziałaniem konfliktom wywoływanym przez problemy środowiskowe, takie jak niedobory wody, zakłócenia w dostępie do energii czy zmiany klimatyczne, przy czym zakładano, że mają one charakter transgraniczny i mogą prowadzić do sporów między państwami. Nowsze podejście traktuje ochronę środowiska i klimatu jako cel sam w sobie, uznając degradację środowiska spowodowaną działalnością człowieka za zagrożenie równoważne klasycznym zagrożeniom bezpieczeństwa narodowego. W przeszłości klęski żywiołowe nie były uznawane za element bezpieczeństwa narodowego, jednak wraz z popularyzacją idei zmian

klimatycznych i globalnego ocieplenia stają się one istotnym komponentem debaty o bezpieczeństwie międzynarodowym[21].

Budowanie bezpieczeństwa systemowego opiera się na wszystkich wymienionych filarach przy jednoczesnym budowaniu odporności jednostek i społeczności lokalnych. Równocześnie nie jest to stan, a ciągły proces polegający na dostosowywaniu się do dynamicznie zmieniającego się otoczenia.

4 Budowanie odporności systemowej w praktyce: model fiński jako punkt odniesienia

W większości badań nad budowaniem odporności systemowej punktem odniesienia jest Finlandia, która jest uznawana za lidera w zakresie przygotowania na sytuacje kryzysowe[22]. Państwo to wypracowało model, w którym szeroko angażuje się różne grupy społeczne, instytucje i podmioty gospodarcze w działania na rzecz bezpieczeństwa. Takie podejście pozwoliło Finlandii lepiej radzić sobie z dynamicznie zmieniającymi się warunkami zewnętrznymi i nowymi zagrożeniami.

Współczesne zagrożenia często mają charakter złożony i wielowymiarowy, dlatego nie da się ich skutecznie neutralizować wyłącznie siłami administracji centralnej. Efektywne działania wymagają współpracy administracji rządowej, samorządów, służb ratowniczych, sektora prywatnego, organizacji społecznych oraz samych obywateli. Model, w którym bezpieczeństwo staje się wspólną odpowiedzialnością wielu podmiotów, zwiększa

21 Kim R. Holmes, "What Is National Security?," w *Index of U.S. Military Strength*, red. Dakota L. Wood (Washington, D.C.: The Heritage Foundation, 2015), 19 – 20, https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf? [dostęp: 30.10.2025].

22 Aino Ruggiero, Wojciech D. Piotrowicz i Lijo John, "Enhancing Societal Resilience Through the Whole-of-Society Approach to Crisis Preparedness: Complex Adaptive Systems Perspective – The Case of Finland," *International Journal of Disaster Risk Reduction*, nr 114 (2024): 2.

elastyczność i efektywność całego systemu[23]. Zaangażowanie szerokiego grona uczestników życia publicznego umożliwia lepsze wykorzystanie ich doświadczeń i zasobów. Przykładowo organizacje pozarządowe mogą wspierać działania pomocowe wobec osób starszych czy wymagających opieki, podczas gdy sektor prywatny dysponuje infrastrukturą i zasobami technicznymi, które w określonych sytuacjach można wykorzystać w działaniach kryzysowych lub odbudowie. Takie szerokie partnerstwo wzmacnia gotowość państwa i społeczeństwa do reagowania na nieprzewidziane sytuacje. Istotne znaczenie ma również poziom zaufania społecznego do instytucji publicznych. Obywatele, którzy dostrzegają sens i przejrzystość działań władz, są bardziej skłonni akceptować wprowadzane ograniczenia w sytuacjach kryzysowych i chętniej podejmują współpracę. Zaufanie nie buduje się jednak samoistnie. Wymaga systematycznej pracy, uczciwego informowania o działaniach państwa, a także umiejętności przyznawania się do błędów i ich korygowania. Zatem stabilność systemu zależy w dużej mierze właśnie od wiarygodności władzy publicznej. Odporność instytucjonalna to nie tylko formalne procedury i gotowe plany kryzysowe. W praktyce sytuacje kryzysowe często wymuszają podejmowanie decyzji w warunkach niepełnej wiedzy i szybko zmieniających się okoliczności[24]. Dlatego tak ważna jest zdolność elastycznego reagowania i dostosowywania działań do aktualnych potrzeb. Same plany są niezbędne, ale system musi być przygotowany na ich modyfikowanie, gdy wymaga tego rzeczywistość. Znaczenie ma również edukacja obywatelska. Osoby świadome zagrożeń i zasad postępowania w sytuacjach nadzwyczajnych są lepiej przygotowane do odpowiedzialnego działania i współpracy z instytucjami publicznymi. Działania edukacyjne powinny być prowadzone zarówno w ramach systemu oświaty, jak i w przestrzeni publicznej poprzez kampanie informacyjne i szkolenia. Dzięki temu społeczeństwo nie tylko ogranicza własną podatność na dezinformację czy panikę, ale także staje się aktywnym uczestnikiem działań ochronnych.

Nie można też pominąć rosnącego znaczenia bezpieczeństwa cyfrowego. Funkcjonowanie państwa i gospodarki coraz silniej opiera się na systemach informatycznych, a zakłócenia w tej sferze mogą prowadzić do destabilizacji

23 Josephine Adekola, Denis Fischbacher-Smith i Moira Fischbacher-Smith, "Inherent Complexities of a Multi-Stakeholder Approach to Building Community Resilience," *International Journal of Disaster Risk Science*, nr 11 (2022): 43.

24 Roman Krawczyński, "Bezpieczeństwo w kontekście osobowości osób zarządzających w sytuacjach kryzysowych," *Colloquium*, nr 3 (2012): 186.

całych sektorów. Dlatego rozwijanie kompetencji w obszarze cyberbezpieczeństwa oraz szybkie wykrywanie i neutralizowanie zagrożeń w tej przestrzeni staje się dziś nieodłącznym elementem odporności systemowej.

Model fiński bywa analizowany także przez pryzmat teorii systemów złożonych adaptacyjnych. Podejście to zakłada, że w złożonym układzie instytucji i społeczeństwa powstają dynamiczne powiązania i zależności, których skutków nie da się zawsze przewidzieć[25]. Siła systemu zależy wtedy od jakości współpracy, sprawnej wymiany informacji i gotowości do dostosowywania się do nowych warunków. Dzięki temu system nie jest sztywny, lecz uczy się, dostosowuje i rozwija w odpowiedzi na kolejne wyzwania.

5 Wnioski

Przeprowadzone rozważania potwierdzają hipotezę postawioną we wstępie, zgodnie z którą skuteczne budowanie odporności systemowej państwa wymaga współdziałania administracji publicznej, sektora prywatnego, organizacji pozarządowych oraz obywateli, przy jednoczesnym rozwijaniu mechanizmów adaptacyjnych umożliwiających elastyczne reagowanie na zmienne zagrożenia. Zarówno analiza literatury, jak i odniesienie do praktycznych doświadczeń, w tym w szczególności do modelu fińskiego, pozwalają dostrzec znaczenie szerokiego, wielosektorowego podejścia do bezpieczeństwa.

Współczesne środowisko bezpieczeństwa charakteryzuje się dużą dynamiką i wielowymiarowością, dlatego budowanie odporności musi mieć charakter ciągłego procesu dostosowawczego. Kluczowe znaczenie mają tu nie tylko formalne struktury i procedury, ale również zaufanie społeczne, jakość edukacji obywatelskiej, rozwój kompetencji cyfrowych oraz otwartość instytucji państwowych na współpracę z różnymi podmiotami życia publicznego. Rekomendacją na przyszłość pozostaje dalszy rozwój zintegrowanych modeli zarządzania bezpieczeństwem, w których odporność systemowa będzie kształtowana nie tylko przez państwo, ale również

25 Tamara Galkina i Irina Atkova, "Effectual Networks as Complex Adaptive Systems: Exploring Dynamic and Structural Factors of Emergence," *Entrepreneurship Theory and Practice*, nr 5 (2020): 987.

przez aktywne uczestnictwo obywateli, organizacji pozarządowych i sektora prywatnego. Warto również prowadzić dalsze badania nad adaptacyjnym charakterem takich systemów, uwzględniającym coraz większe znaczenie zagrożeń o charakterze cyfrowym, klimatycznym i hybrydowym. W warunkach narastającej niepewności właśnie elastyczność i umiejętność współdziałania różnych podmiotów mogą stać się podstawą długoterminowego bezpieczeństwa państwa i jego obywateli.

Bibliografia

Adekola, Josephine, Denis Fischbacher-Smith i Moira Fischbacher-Smith. "Inherent Complexities of a Multi-Stakeholder Approach to Building Community Resilience." *International Journal of Disaster Risk Science*, nr 11 (2022): 32 – 45. https://doi.org/10.1007/s13753-020-00246-1.

Bierecki, Dominik, Christophe Gaie i Mirosław Karpiuk. "Artificial Intelligence in e-Administration." *Prawo i Więź*, nr 1 (2025): 383 – 407. https://doi.org/10.36128/PRIW.VI54.1201.

Bsoul-Kopowska, Magdalena, Aleksandra Skrabacz i Jarosław Rodzik. "The Crucial Role of Crisis Management Teams in Public Administration in the Context of COVID-19." *Polish Journal of Management Studies*, nr 1 (2022): 107 – 131. http://dx.doi.org/10.17512/pjms.2022.25.1.07.

Cholewińska, Dagmara. "Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia." *Ius et Securitas*, nr 1 (2025): 41 – 52.

Czuryk, Małgorzata. "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd." *Studia z Prawa Wyznaniowego*, nr 27 (2024): 151 – 163. https://doi.org/10.31743/spw.17518.

Gaie, Christophe, Mirosław Karpiuk i Andrea Spaziani. "Cybersecurity in France, Poland and Italy." *Studia Iuridica Lublinensia*, nr 1 (2025): 73 – 95. http://dx.doi.org/10.17951/sil.2025.34.1.73-95.

Gaie, Christophe, Mirosław Karpiuk i Nicola Strizzolo. "Cybersecurity of Public Sector Institutions." *Prawo i Więź*, nr 6 (2024): 347 – 362. https://doi.org/10.36128/PRIW.VI53.1129.

Galkina, Tamara i Irina Atkova. "Effectual Networks as Complex Adaptive Systems: Exploring Dynamic and Structural Factors of Emergence." *Entrepreneurship Theory and Practice*, nr 5 (2020): 964 – 995. https://doi.org/10.1177/1042258719879670.

Gherghina, Sergiu, Clara Volintiru i Throstur Olaf Sigurjonsson. "Making a Difference: The Effects of Institutional Resilience in Society During COVID19." *European Political Science*, nr 1 (2022): 426 – 435. https://doi.org/10.1057/s41304-022-00380-y.

Holmes, Kim R. "What Is National Security?" W *Index of U.S. Military Strength*, red. Dakota L. Wood, 17 – 26. Washington, D.C.: The Heritage Foundation, 2015. https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf?.

Kaczmarek, Krzysztof, Mirosław Karpiuk i Andrea Spaziani. "Use of Artificial Intelligence in Public Sector: Threats and Prospects." *Studia Iuridica Toruniensia*, nr 1 (2025): 29 – 48. http://dx.doi.org/10.12775/SIT.2025.002.

Kaczmarek, Krzysztof, Mirosław Karpiuk i Claudio Melchior. "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data." *Prawo i Więź*, nr 3 (2024): 103 – 121. https://doi.org/10.36128/PRIW.VI50.907.

Kaczmarek, Krzysztof. "Sztuczna inteligencja." W *Leksykon cyberbezpieczeństwa*, red. Katarzyna Chałubińska-Jentkiewicz, 250 – 252. Warszawa: Akademia Sztuki Wojennej, 2024.

Karpiuk, Mirosław, Claudio Melchior i Urszula Soler. "Cybersecurity Management in the Public Service Sector." *Prawo i Więź*, nr 4 (2023): 7 – 27. https://doi.org/10.36128/PRIW.VI47.751.

Karpiuk, Mirosław. "Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)." *Studia Iuridica Lublinensia*, nr 1 (2019): 185 – 194. http://dx.doi.org/10.17951/sil.2019.28.1.185-194.

Karpiuk, Mirosław. "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity." *Studia Iuridica Lublinensia*, nr 2 (2023): 189 – 201. http://dx.doi.org/10.17951/sil.2023.32.2.189-201.

Kostrubiec, Jarosław, Mirosław Karpiuk i Dominik Tyrawa. "The Status of Municipal Government in the Sphere of Ecological Security." *Hungarian Journal of Legal Studies*, nr 2 (2024): 164 – 181. https://doi.org/10.1556/2052.2024.00510.

Krawczyński, Roman. "Bezpieczeństwo w kontekście osobowości osób zarządzających w sytuacjach kryzysowych." *Colloquium*, nr 3 (2012): 185 – 210.

Profiroiu, Alina Georgiana i Corina-Cristiana Nastacă. "What Strengthens Resilience in Public Administration Institutions?" *Eastern Journal of European Studies*, nr 12 (2021): 100 – 125. https://doi.org/10.47743/ejes-2021-SI05.

Reznikova, Olga. *National Resilience in Changing Security Environment*. Kyiv: National Institute for Strategic Studies, 2022.

Ruggiero, Aino, Wojciech D. Piotrowicz i Lijo John. "Enhancing Societal Resilience Through the Whole-of-Society Approach to Crisis Preparedness:

Complex Adaptive Systems Perspective – The Case of Finland." *International Journal of Disaster Risk Reduction*, nr 114 (2024): 1 – 17. https://doi.org/10.1016/j.ijdrr.2024.104944.

Skrabacz, Aleksandra, Magdalena Bsoul-Kopowska i Bartosz Kozicki. "The Application of Artificial Intelligence in Road Traffic Management and Its Safety Improvement." *Transport Problems*, nr 4 (2024): 5 – 16. http://dx.doi.org/10.20858/tp.2024.19.4.01.

Skrabacz, Aleksandra. "Migrations As a Challenge for Dispositional Groups in Polish and European Comparative Perspectives." *Journal of Eastern Europe Research in Business and Economics*, Article ID 290391 (2021): 1 – 14. http://dx.doi.org/10.5171/2021.290391.

Włodyka, Ewa Maria. "Artificial Intelligence as a Supporting Tool for Local Government Decision-Making in Public Safety." *Przegląd Nauk o Obronności*, nr 17 (2024): 80 – 91. https://doi.org/10.37055/pno/185616.

Włodyka, Ewa Maria. "Implementation of e-Government and Artificial Intelligence in Polish Public Administration." *TalTech Journal of European Studies*, nr 2 (2024): 118 – 136. https://doi.org/10.2478/bjes-2024-0019.