Krzysztof Kaczmarek
Wydział Humanistyczny
Politechnika Koszalińska
ORCID: 0000-0001-8519-1667
e-mail: krzysztof.kaczmarek@tu.koszalin.pl

Bezpieczeństwo infrastruktury krytycznej a cicha odporność instytucjonalna*

Streszczenie

Autor artykułu analizuje bezpieczeństwo infrastruktury krytycznej z punktu widzenia odporności instytucjonalnej obejmującej nie tylko rozwiązania techniczne, lecz także mniej widoczne mechanizmy funkcjonowania organizacji odpowiedzialnych za zarządzanie kryzysowe. Punktem wyjścia jest założenie, że zdolność do utrzymania podstawowych funkcji w warunkach zakłóceń wynika zarówno z formalnych procedur, jak i z praktyk działania, relacji oraz wiedzy milczącej, które w ograniczonym zakresie podlegają regulacjom i standaryzacji. Celem artykułu jest ukazanie, że ukryty wymiar odporności jest ważny dla bezpieczeństwa infrastruktury krytycznej, pomimo że jego znaczenie bywa marginalizowane w politykach bezpieczeństwa. Przyjęta hipoteza zakłada, że bezpieczeństwo infrastruktury zależy od zdolności instytucji do funkcjonowania w warunkach niepewności, zwłaszcza od „cichej odporności instytucjonalnej" ujawniającej się poza formalnymi procedurami. Zastosowaną metodą badawczą jest jakościowa analiza literatury oraz studia przypadków dotyczące wybranych sytuacji kryzysowych.

* Tekst powstał na podstawie wyników badań prowadzonych podczas stażu naukowego autora w Katedrze Prawa Administracyjnego i Nauk o Bezpieczeństwie na Wydziale Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie w 2025 roku.

Wyniki analizy pokazują, że nieformalne relacje, zdolność adaptacji, praktyczna wiedza personelu oraz lokalne sieci współpracy stanowią fundamentalny element odporności, a ich rozwój wymaga długotrwałych procesów organizacyjnych. Autor wskazuje również konieczność dalszych badań nad operacjonalizacją odporności instytucjonalnej oraz nad mechanizmami jej rozwoju w okresach braku poważnych zakłóceń.

Słowa kluczowe bezpieczeństwo infrastruktury krytycznej, odporność instytucjonalna, cicha odporność instytucjonalna, zarządzanie kryzysowe, nieformalne sieci działania

Wstęp

Punktem wyjścia dla analiz przeprowadzonych w niniejszym artykule jest przyjęcie, że odporność infrastruktury krytycznej nie zależy jedynie od jej składowych technicznych, lecz także od jej umiejscowienia w systemie społecznym, przyrodniczym czy technologicznym. Jednocześnie złożone zależności między poszczególnymi infrastrukturami powodują, że stają się one w coraz większym stopniu podatne na zakłócenia, które z łatwością mogą przenosić się między sektorami[1]. W takim ujęciu istotną rolę odgrywają utrwalone wzorce działań, relacje i zasady regulujące aktywność społeczną. To właśnie one współtworzą sieć zależności między poszczególnymi systemami infrastruktury i wpływają na to, w jakim stopniu zakłócenia się rozchodzą[2].

Dla dalszych analiz niezbędne jest również zdefiniowanie infrastruktury krytycznej. Na poziomie międzynarodowym opisuje się ją jako systemy, obiekty i sieci niezbędne do funkcjonowania gospodarki oraz zapewnienia bezpieczeństwa i dobrostanu ludności. Choć poszczególne państwa stosują odmienne definicje, wspólnym elementem pozostaje uznanie podstawowego

1 Na temat cyfrowego aspektu bezpieczeństwa infrastruktury krytycznej zob.: M. Czuryk, *Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa*, „Ius et Securitas" 2025, nr 1; C. Gaie, M. Karpiuk, A. Spaziani, *New Technologies in Public Administration*, „Ius et Securitas" 2024, nr 2; E.M. Włodyka, *Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku*, ibidem , nr 1; D. Bierecki, M. Karpiuk, C. Gaie, *Artificial Intelligence in e-Administration*, „Prawo i Więź" 2025, nr 1.

2 C. Gim, C.A. Miller, *Institutional interdependence and infrastructure resilience*, „Current Opinion in Environmental Sustainability" 2022, nr 57, s. 1.

charakteru usług dostarczanych dzięki tej infrastrukturze, których zakłócenie wiązałoby się z poważnymi konsekwencjami społecznymi i ekonomicznymi[3]. Podobnie ujęta jest odporność, rozumiana jako zdolność systemów do absorbowania zakłóceń, odzyskiwania funkcjonalności i dostosowywania się do zmieniających się warunków z jednoczesnym ograniczeniem strat. W tym kontekście eksponuje się zarówno minimalizowanie skutków zakłóceń, jak i zdolność adaptacji do nowych wyzwań[4].

W tym kontekście wielu badaczy wskazuje na zestaw działań sprzyjających wzmacnianiu odporności infrastruktury krytycznej. Obejmują one tworzenie wielosektorowych struktur koordynacyjnych, analizę złożonych powiązań i podatności pomiędzy systemami, rozwijanie zaufania i wymiany informacji między administracją a operatorami, formułowanie realistycznych celów odpornościowych oraz dobór odpowiednich instrumentów politycznych. Dużą wagę przywiązuje się również do monitorowania wdrażanych rozwiązań i do współpracy transgranicznej[5]. Ważnym elementem badań nad poruszaną problematyką jest rozróżnienie między odpornością techniczną i organizacyjną. Pierwsza dotyczy ochrony fizycznych i technologicznych elementów infrastruktury, druga kształtuje się w obszarze zarządzania. Jednocześnie rozróżnia się cztery główne elementy odporności infrastruktury krytycznej: zdolność do przeciwstawiania się zakłóceniom, odporność strukturalną, możliwość odzyskiwania funkcjonalności oraz adaptacyjność[6].

Jednocześnie nastąpił gwałtowny wzrost popularności pojęcia „odporność". Jest ono obecne w wielu dziedzinach i dyskursach instytucjonalnych. Z jednej strony pozwala ujmować złożone zależności między wieloma czynnikami, z drugiej, stwarza ryzyko nadużywania, zwłaszcza w sytuacji braku podstaw teoretycznych. Tymczasem bez solidnych podstaw koncepcyjnych odporność może być wykorzystywana przede wszystkim jako wygodna figura

3 Więcej na temat ochrony infrastruktury krytycznej w Polsce zob. M. Karpiuk, *Właściwość samorządu terytorialnego w zakresie zapobiegania nadzwyczajnym zagrożeniom i ich skutkom*, „Ius et Administratio" 2023, nr 3.

4 *Good Governance for Critical Infrastructure Resilience*, Paryż 2019, s. 105–106.

5 H. Janeckova, *The Basis for Strengthening Organisational Resilience of Critical Transport Infrastructure Entities*, „Transportation Research Procedia" 2023, nr 74, s. 1031.

6 N. Milanova, *Institutional Resilience and Building Integrity in the Defense and Security Sector*, „Connections: The Quarterly Journal" 2020, nr 3, s. 68.

retoryczna, a nie narzędzie analityczne wspierające rozwiązywanie złożonych problemów społecznych[7].

Przedstawione powyżej ujęcia pozwalają analizować infrastrukturę krytyczną nie tylko jako zbiór obiektów wymagających ochrony, lecz przede wszystkim jako element bardziej rozbudowanego porządku instytucjonalnego. To właśnie w instytucjach – rozumianych zarówno jako struktury formalne, jak i sieci relacji oraz praktyk działania – istnieją mechanizmy, których działanie w dużym stopniu decyduje o rzeczywistej zdolności systemów do funkcjonowania w warunkach zakłóceń. Oprócz procedur, regulacji, kompetencji i uprawnień istnieją mniej widoczne, a często ważne składowe procesów. Można do nich zaliczyć sposoby podejmowania decyzji, nieformalne kanały komunikacji, relacje międzyludzkie, rutyny organizacyjne czy praktyczną wiedzę osób odpowiedzialnych za zarządzanie kryzysowe i ochronę infrastruktury krytycznej. To właśnie ten często niezauważalny aspekt decyduje, czy infrastruktura zachowuje stabilność w sytuacjach obciążenia. Na potrzeby niniejszego artykułu autor zdecydował się określić go jako „cichą odporność instytucjonalną"[8].

W związku z tym celem artykułu jest analiza znaczenia ukrytych i nieformalnych mechanizmów instytucjonalnych dla funkcjonowania infrastruktury krytycznej w warunkach zakłóceń, ze szczególnym uwzględnieniem ich wpływu na zdolność do utrzymania ciągłości działania. Zgodnie z przyjętą hipotezą odporność infrastruktury krytycznej zależy nie tylko od formalnych procedur zarządzania i rozwiązań technicznych, lecz także od nieformalnych relacji, kontaktów międzyludzkich, praktyk i kompetencji instytucjonalnych. Przeprowadzone analizy zostały przeprowadzone na podstawie studiów przypadku oraz wyników najnowszych badań nad odpornością infrastruktury krytycznej w różnych państwach.

7 M.Z.Y. Tan, *Resilience is a dirty word: misunderstood, and how we can truly build it*, „Critical Care" 2022, nr 26, s. 1.

8 Określenie „cicha odporność instytucjonalna" nawiązuje do rozwijanych w literaturze przedmiotu koncepcji odporności instytucjonalnej oraz odporności infrastruktury krytycznej. Por.: N. Milanova, op. cit.; J. Gonçalves, S. Spolaor, L. Lebedeva, *Institutional resilience and crisis governance in the EU: insights from the Lisbon Metropolitan Experience*, „Frontiers in Political Science" 2025, nr 7; S. Keele, L. Coenen, *The Role of Public Policy in Critical Infrastructure Resilience. Research Report*, Londyn 2019, https://www.resilienceshift.org/wp-content/uploads/2019/04/ResilienceShift-Role-of-Public-Policy-FINAL-1.pdf [dostęp: 6.12.2025].

Instytucjonalne ujęcia odporności infrastruktury krytycznej

Pojęcie „odporność" przyjmowane w badaniach nad infrastrukturą krytyczną obejmuje nie tylko zdolność systemów do ograniczania negatywnych skutków zakłóceń, lecz także mechanizmy pozwalające na utrzymanie ciągłości działania w razie ich wystąpienia[9]. W tym kontekście czynniki instytucjonalne służą wyjaśnianiu, w jaki sposób struktury organizacyjne, procedury i praktyki działania wpływają na zdolność systemów do zachowania ciągłości działania w sytuacji znacznego, spowodowanego zakłóceniami, obciążenia. Dlatego analiza odporności instytucjonalnej koncentruje się na identyfikacji tych elementów systemu, które są odpowiedzialne za adaptację i utrzymanie podstawowych funkcji infrastruktury krytycznej[10].

Współczesne podejścia do badań nad odpornością infrastruktury krytycznej w coraz większym stopniu uwzględniają elementy instytucjonalne. Przykładem są wyniki badań przeprowadzonych w sektorze energetycznym w Malawi. Pokazały one, że odporność operatorów zależy od pięciu podstawowych zdolności: prewencyjnej, antycypacyjnej, absorpcyjnej, adaptacyjnej oraz transformacyjnej[11]. Wyniki badań operatorów infrastruktury krytycznej w Nowej Zelandii pokazały, że poziom odporności organizacyjnej w znacznej mierze zależy od zdolności do współpracy międzyinstytucjonalnej, systematycznego uczenia się na podstawie wcześniejszych zakłóceń oraz regularnego testowania procedur w warunkach symulowanych kryzysów[12]. Do podobnych wniosków upoważniają wyniki badań przeprowadzonych w Austrii. Wynika z nich, że odporność instytucjonalna zależy nie tylko od formalnych uprawnień poszczególnych organów, lecz również od gęstości sieci powiązań między nimi oraz od jakości partycypatywnych mechanizmów oceny i doskonalenia

9 *Good Governance for Critical Infrastructure Resilience*…, s. 22–24.

10 X. Zhao, Y. Liu ,W. Jiang, D. Wei, *Study on the Factors Influencing and Mechanisms Shaping the Institutional Resilience of Mega Railway Construction Projects*, „Sustainability" 2023, nr 10, s. 2–5.

11 J.N. Chivunga, Z. Lin, R. Blanchard, *Critical infrastructure organisational resilience assessment: A case study of Malawi's power grid operator*, „The Electricity Journal" 2024, nr 37, s. 12–14.

12 C. Brown, E. Seville, J. Vargo, *Measuring the organizational resilience of critical infrastructure providers*, „International Journal of Critical Infrastructure Protection" 2017, nr 18, s. 46–47.

procedur[13]. Natomiast wyniki analiz miejskich systemów w Niemczech dowodzą, że odporność instytucjonalna jest ograniczana przez wysoki poziom fragmentacji instytucji, niejasne podziały odpowiedzialności oraz trudności w koordynacji działań w sytuacjach przekraczających uprawnienia pojedynczych podmiotów[14].

Przedstawione powyżej ujęcia instytucjonalne i wyniki badań wskazują, że poza formalnymi strukturami odporność infrastruktury krytycznej zależy również od wielu mechanizmów i praktyk, które nie zawsze są widoczne w oficjalnych procedurach, ale mają ważne znaczenie dla zdolności funkcjonowania systemów w warunkach zakłóceń.

Ukryty wymiar instytucjonalnej odporności infrastruktury krytycznej

Jednym z istotnych wniosków płynących z badań nad odpornością organizacyjną jest to, że jej ważna część bazuje na nieformalnych relacjach i wiedzy milczącej, rzadko odzwierciedlanych w formalnych strukturach zarządzania. Autorzy literatury przedmiotu często wskazują, że w sytuacjach zakłóceń to nieformalne sieci powiązań doradczych umożliwiają szybkie podejmowanie decyzji, tym samym stają się jednym z głównych elementów odporności instytucjonalnej[15]. Jednocześnie wyniki badań nad operacjami ratowniczymi na Morzu Północnym wskazują, że główną rolę w utrzymaniu sprawności systemów odgrywa wiedza milcząca personelu, jego doświadczenie i *know-how*, które nie są zapisane w procedurach, ale determinują sposób interpretowania sygnałów ostrzegawczych oraz koordynowania działań w czasie rzeczywistym[16].

13 P. Abduragimova, B.D. Fath, C.G.H. Katzmair, *Participatory approach for assessing institutional resilience: a case study of crises in Austria*, „Environment, Development and Sustainability" 2022, nr 25, s. 9221–9223.

14 J. Monstadt, M. Schmidt, *Urban resilience in the making? The governance of critical infrastructures in German cities*, „Urban Studies" 2019, nr 11.

15 X. Jin, D. Yang, W. Sun, L. Xu, *Building a Resilient Organization Through Informal Networks: Examining the Role of Individual, Structural, and Attitudinal Factors in Advice-Seeking Tie Formation*, „Systems" 2025, nr 4, s. 14–15.

16 R. Steen, G. Haakonsen, T.J. Steiro, *Patterns of Learning: A Systemic Analysis of Emergency Response Operations in the North Sea through the Lens of Resilience Engineering*, „Infrastructures" 2023, nr 2, s. 14–16.

W ostatnich latach zostały opracowane metody, które umożliwiają operacjonalizację odporności instytucjonalnej. Jako przykład można podać metodę ASOR (A Systemic Approach to Organisational Resilience – systemowe podejście do odporności organizacyjnej) pozwalającą na systematyczną ocenę czynników takich jak zarządzanie ryzykiem, innowacyjność organizacji czy szkolenia personelu. Umożliwia to identyfikację słabych punktów i planowanie odpowiednich działań podnoszących odporność operatorów infrastruktury krytycznej[17]. Dzięki temu odporność przestaje mieć charakter deklaratywny i być jedynie zbiorem procedur, staje się mierzalnym zestawem warunków funkcjonowania organizacji, wymagającym ciągłego monitorowania, a nie tylko reakcji po awarii[18].

Niewidoczna strona instytucjonalnej odporności infrastruktury krytycznej wiąże się również z tym, w jaki sposób organizacje kształtują swoją kulturę działania w warunkach niepewności. Badania nad tzw. organizacjami wysokiej niezawodności pokazują, że zdolność do utrzymania funkcjonalności w sytuacji nieoczekiwanych zdarzeń polega na zbiorowej uważności przejawiającej się m.in. w stałej koncentracji na drobnych sygnałach niepowodzenia i unikaniu upraszczania ich interpretacji, wrażliwości na przebieg działań operacyjnych oraz gotowości do odwoływania się do wiedzy fachowej niezależnie od formalnej hierarchii[19]. Tego typu praktyki organizacyjne trudno w pełni uchwycić w klasycznych planach zarządzania kryzysowego. Tymczasem to one w dużej mierze decydują o tym, czy instytucje odpowiedzialne za infrastrukturę krytyczną potrafią szybko wykrywać i korygować błędy, zanim przerodzą się one w poważne zakłócenia. Zbieżne wnioski formułuje się w badaniach nad miejską „codzienną odpornością", w których podkreśla się, że zdolność do radzenia sobie z zagrożeniami rozwija się stopniowo w toku rutynowych interakcji między służbami, administracją i innymi podmiotami, czyli w przestrzeni praktyk rzadko znajdujących bezpośrednie odzwierciedlenie

17 D. Rehak, *Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic*, „Safety Science" 2020, nr 123, s. 3–6.

18 Z. Dvorak, N. Chovancikova, J. Bruk, M, Hromada, *Methodological Framework for Resilience Assessment of Electricity Infrastructure in Conditions of Slovak Republic*, „International Journal of Environmental Research and Public Health" 2021, nr 16, s. 24–26.

19 K.E. Weick, K.M. Sutcliffe, *Managing the Unexpected: Sustained Performance in a Complex World*, Hoboken 2015, s. 44–48.

w dokumentach strategicznych[20]. Tym samym mechanizmy te pozostają poza standardowymi ujęciami formalnymi, choć w praktyce to one mogą warunkować prawidłowe funkcjonowanie infrastruktury krytycznej w przypadku zakłóceń.

Instytucjonalne ujęcie odporności infrastruktury krytycznej: studia przypadków

Przedstawione analizy koncepcji odporności instytucjonalnej wymagają uzupełnienia poprzez odniesienie do konkretnych przykładów pokazujących, w jaki sposób rozwija się ona w praktyce funkcjonowania infrastruktury krytycznej. Wybrane studia przypadków ilustrują różne sposoby reagowania instytucji na zakłócenia oraz ujawniają znaczenie elementów nieformalnych.

W lipcu 2021 roku w dolinie rzeki Ahr, w kraju związkowym Nadrenia-Palatynat w zachodnich Niemczech, doszło do powodzi, podczas której zostały uszkodzone elementy infrastruktury krytycznej, w tym sieci energetyczne, drogi, mosty oraz linie kolejowe. Skutkowało to wielodniowymi przerwami w dostawach energii elektrycznej, odcięciem od świata wielu miejscowości oraz poważnymi ograniczeniami w funkcjonowaniu podstawowych usług publicznych. W takich warunkach szczególnego znaczenia nabrały nieformalne mechanizmy współpracy między służbami ratowniczymi, lokalną administracją i operatorami infrastruktury, które pozwalały na koordynację działań i przywracanie funkcjonalności szybciej niż wynikało to ze standardowych procedur. Jednocześnie okazało się, że problemy w przepływie informacji i opóźnienia w ogłaszaniu alarmu przyczyniły się do zwiększenia strat oraz utrudniły działania ratownicze. Mimo że Europejski System Informowania o Powodziach (EFAS) sygnalizował możliwe zagrożenie już kilka dni wcześniej, decyzja o ogłoszeniu alarmu została podjęta dopiero po wystąpieniu zjawiska, co uwidoczniło ograniczenia formalnych procedur. W rezultacie to lokalne, nieformalne struktury wsparcia okazały się najważniejsze w pierwszej fazie reagowania, co potwierdza znaczenie ukrytego potencjału odporności

20 J. Coaffee, D.M. Wood, P. Rogers, *The everyday resilience of the city: How cities respond to terrorism and disaster*, Berlin 2008, s. 219–230.

instytucjonalnej w sytuacjach, w których jest wymagana natychmiastowa reakcja[21].

Interesująco przedstawiają się również sytuacje kryzysowe, w których cechy cichej odporności można uchwycić w praktycznym działaniu instytucji odpowiedzialnych za infrastrukturę krytyczną. W maju 2021 roku w Stanach Zjednoczonych Ameryki doszło do cyberataku typu *ransomware* na systemy Colonial Pipeline, operatora jednej ze strategicznych magistrali przesyłowych paliw płynnych, łączącej rafinerie na wybrzeżu Zatoki Meksykańskiej z głównymi rynkami wschodniego wybrzeża państwa[22]. W reakcji na atak przedsiębiorstwo prewencyjnie wstrzymało pracę rurociągu na kilka dni, co doprowadziło do zakłóceń w dostawach benzyny, diesla i paliwa lotniczego, lokalnych niedoborów oraz wzrostu cen paliw w licznych stanach na wschodzie kraju. Incydent ujawnił silne uzależnienie bezpieczeństwa energetycznego od pojedynczego operatora infrastruktury oraz słabości dotychczasowego, w dużej mierze dobrowolnego systemu regulacji bezpieczeństwa cyfrowego w sektorze paliw. W odpowiedzi po raz pierwszy władze federalne wprowadziły wiążące dyrektywy bezpieczeństwa dla operatorów rurociągów, nakładające obowiązek wyznaczenia całodobowego koordynatora cyberbezpieczeństwa, niezwłocznego raportowania incydentów oraz przeprowadzenia oceny podatności i opracowania planów działań naprawczych i awaryjnych[23]. Przypadek Colonial Pipeline pokazuje, że odporność instytucjonalna infrastruktury krytycznej kształtuje się nie tylko na poziomie pojedynczych przedsiębiorstw, lecz także w relacjach między regulatorem, agencjami odpowiedzialnymi za bezpieczeństwo i sektorem prywatnym, a zdolność do szybkiego tworzenia i wdrażania nowych zasad regulacyjnych staje się istotnym składnikiem „cichej" odporności instytucjonalnej również wobec zagrożeń o charakterze cyfrowym.

W analizie odporności instytucjonalnej istotne znaczenie mają także prywatne relacje międzyludzkie, które ujawniają się w sytuacjach kryzysowych, jako czynnik warunkujący zdolność do działania poza formalnymi

21 *Ahrtal unter Wasser. Chronik einer Katastrophe*, https://reportage.wdr.de/chronik-ahrtal-hochwasser-katastrophe [dostęp: 7.12.2025].

22 *Case study 2: the Colonial Pipeline ransomware attack*, https://www.futurelearn.com/info/courses/security-by-design/0/steps/390473 [dostęp: 7.12.2025].

23 *Cyber Case Study: Colonial Pipeline Ransomware Attack*, https://insurica.com/blog/colonial-pipeline-ransomware-attack/ [dostęp: 7.12.2025].

procedurami. Dobrym przykładem znaczenia prywatnych kontaktów międzyludzkich dla funkcjonowania infrastruktury krytycznej jest doświadczenie Japonii po trzęsieniu ziemi w Kobe w 1995 roku. W dzielnicach, w których istniały gęste sieci sąsiedzkie, *machizukuri*[24] oraz lokalne organizacje pozarządowe, szybciej przywracano podstawowe usługi, skuteczniej gaszono pożary, organizowano tymczasowe punkty zaopatrzenia w wodę i energię oraz sprawniej negocjowano z władzami przebieg odbudowy[25]. Badania Daniela Aldricha pokazują, że to właśnie gęstość nieformalnych więzi, takich jak relacje między sąsiadami, właścicielami małych firm i lokalnymi liderami, najlepiej tłumaczy tempo „powrotu do życia" poszczególnych dzielnic, podczas gdy obiektywna skala zniszczeń czy poziom zamożności miały mniejsze znaczenie[26]. Przykład ten pokazuje, że spontanicznie tworzone sieci doradcze i wsparcia pozwalają wspólnie planować odbudowę, mobilizować zewnętrzne zasoby oraz korygować błędy w formalnych planach i procedurach, co stanowi przykład cichej odporności instytucjonalnej zakorzenionej w prywatnych relacjach międzyludzkich.

Zakończenie

Wyniki przeprowadzonych w artykule analiz potwierdzają, że odporność infrastruktury krytycznej nie może być interpretowana wyłącznie jako efekt działań technicznych i organizacyjnych, lecz stanowi wynik wielowarstwowych procesów instytucjonalnych, w dużej mierze nieujmowanych w formalnych procedurach. Natomiast wnioski płynące z badań studiów przypadków wskazują, że w sytuacjach kryzysowych decydujące znaczenie mają nieformalne sieci współpracy, wiedza milcząca, doświadczenie oraz zdolność przekraczania

24 Machizukuri – japońskie pojęcie oznaczające oddolne, partycypacyjne kształtowanie miasta i lokalnej przestrzeni oparte na sieci współpracy między mieszkańcami, lokalnymi organizacjami, małymi przedsiębiorstwami i samorządem, tzw. miękka infrastruktura. Więcej zob. M. Christchurch, *Community led opportunity for renewal – Kobe earthquake recovery 1995–2000*, https://medium.com/making-christchurch/community-led-opportunity-for-renewal-kobe-earthquake-recovery-1995-2000-e43025c9f406 [dostęp: 8.12.2025].

25 *Network for Citizen-centered Restoration Projects in Kobe*, https://tm19950117.jp/en/interview/2786/ [dostęp: 8.12.2025].

26 D.P. Aldrich, *The power of people: social capital's role in recovery from the 1995 Kobe earthquake*, „Natural Hazards" 2011, nr 3, s. 607–608.

sztywnych granic instytucjonalnych. Przypadki te potwierdzają, że instytucjonalne zdolności adaptacyjne ujawniają się najczęściej nie w warunkach pełnej zgodności z procedurami, lecz w sytuacjach odstępstwa od nich, co wskazuje na istnienie praktyk działania niewidocznych w standardowych modelach zarządzania kryzysowego. Jednocześnie przedstawione przykłady pokazują, że cicha odporność instytucjonalna jest trudna do uchwycenia w klasycznych narzędziach analitycznych. Wprawdzie można wskazać rosnące znaczenie tej problematyki w literaturze oraz praktyce zarządzania bezpieczeństwem infrastruktury krytycznej, ale jej operacjonalizacja wciąż bazuje na fragmentarycznych koncepcjach. W tym sensie przeprowadzone rozważania potwierdzają hipotezę badawczą dotyczącą ograniczeń analizy odporności, która pomija ukryte elementy instytucjonalne lub traktuje je jako czynnik drugorzędny.

Uzyskane wyniki mają również znaczenie praktyczne. Oznacza to, że działania państwa na rzecz wzmacniania bezpieczeństwa infrastruktury krytycznej powinny obejmować nie tylko rozwój systemów ochrony technicznej, lecz także projektowanie mechanizmów ułatwiających wymianę informacji, tworzenie trwałych relacji między administracją publiczną a operatorami oraz wzmacnianie uprawnień instytucji odpowiedzialnych za koordynację międzysektorową[27]. Szczególnego znaczenia nabierają działania podejmowane pomiędzy okresami kryzysów, w czasie braku poważnych zakłóceń funkcjonowania instytucji, kiedy kształtują się praktyki decydujące o późniejszej zdolności reagowania.

Wskazane w artykule wnioski otwierają przestrzeń do dalszych badań dotyczących porównania cichej odporności instytucjonalnej z uwzględnieniem systemów prawa, struktur administracyjnych i modeli koordynacji państwa z sektorem prywatnym. Takie badania mogłyby dostarczyć pogłębionej wiedzy na temat instytucjonalnych czynników stabilności, które pozostają słabo rozpoznane zarówno w literaturze, jak i praktyce zarządzania bezpieczeństwem infrastruktury krytycznej. Warto również rozwijać metody umożliwiające empiryczne badanie cichej odporności oraz identyfikowanie jej ograniczeń, zwłaszcza w sytuacjach, w których praktyki nieformalne wchodzą w konflikt z obowiązującymi regulacjami.

27 A. Pieczywok, *Złożoność zagrożeń egzystencji człowieka – wybrane zagadnienia*, „Ius et Securitas" 2024, nr 1, s. 7.

Bibliografia

Abduragimova P., Fath B.D., Katzmair C.G.H, *Participatory approach for assessing institutional resilience: a case study of crises in Austria*, „Environment, Development and Sustainability" 2022, nr 25.

Ahrtal unter Wasser. Chronik einer Katastrophe, https://reportage.wdr.de/chronik-ahrtal-hochwasser-katastrophe [dostęp: 7.12.2025].

Aldrich D.P., *The power of people: social capital's role in recovery from the 1995 Kobe earthquake*, „Natural Hazards" 2011, nr 3.

Bierecki D., Karpiuk M., Gaie C., *Artificial Intelligence in e-Administration*, „Prawo i Więź" 2025, nr 1.

Brown C., Seville E., Vargo J., *Measuring the organizational resilience of critical infrastructure providers*, „International Journal of Critical Infrastructure Protection" 2017, nr 18.

Case study 2: the Colonial Pipeline ransomware attack, https://www.futurelearn.com/info/courses/security-by-design/0/steps/390473 [dostęp: 7.12.2025].

Chivunga J.N., Lin Z., Blanchard R., *Critical infrastructure organisational resilience assessment: A case study of Malawi's power grid operator*, „The Electricity Journal" 2024, nr 37.

Christchurch M., *Community led opportunity for renewal – Kobe earthquake recovery 1995–2000*, https://medium.com/making-christchurch/community-led-opportunity-for-renewal-kobe-earthquake-recovery-1995-2000-e43025c9f406 [dostęp: 8.12.2025].

Coaffee J., Wood D.M., Rogers P., *The everyday resilience of the city: How cities respond to terrorism and disaster*, Berlin 2008.

Cyber Case Study: Colonial Pipeline Ransomware Attack, https://insurica.com/blog/colonial-pipeline-ransomware-attack/ [dostęp: 7.12.2025].

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

Dvorak Z., Chovancikova N., Bruk J., Hromada M,, *Methodological Framework for Resilience Assessment of Electricity Infrastructure in Conditions of Slovak Republic*, „International Journal of Environmental Research and Public Health" 2021, nr 16.

Gaie C., Karpiuk M., Spaziani A., *New Technologies in Public Administration*, „Ius et Securitas" 2024, nr 2.

Gim C., Miller C.A., *Institutional interdependence and infrastructure resilience*, „Current Opinion in Environmental Sustainability" 2022, nr 57.

Gonçalves J., Spolaor S., Lebedeva L., *Institutional resilience and crisis governance in the EU: insights from the Lisbon Metropolitan Experience*, „Frontiers in Political Science" 2025, nr 7.

Good Governance for Critical Infrastructure Resilience, Paryż 2019.

Janeckova H., *The Basis for Strengthening Organisational Resilience of Critical Transport Infrastructure Entities*, „Transportation Research Procedia" 2023, nr 74.

Jin X., Yang D., Sun W., Xu L., *Building a Resilient Organization Through Informal Networks: Examining the Role of Individual, Structural, and Attitudinal Factors in Advice-Seeking Tie Formation*, „Systems" 2025, nr 4.

Karpiuk M., *Właściwość samorządu terytorialnego w zakresie zapobiegania nadzwyczajnym zagrożeniom i ich skutkom*, „Ius et Administratio" 2023, nr 3.
Keele S., Coenen L., *The Role of Public Policy in Critical Infrastructure Resilience. Research Report*, London 2019, https://www.resilienceshift.org/wp-content/uploads/2019/04/ResilienceShift-Role-of-Public-Policy-FINAL-1.pdf [dostęp: 6.12.2025].
Milanova N., *Institutional Resilience and Building Integrity in the Defense and Security Sector*, „Connections: The Quarterly Journal" 2020, nr 3.
Monstadt J., Schmidt M., *Urban resilience in the making? The governance of critical infrastructures in German cities*, „Urban Studies" 2019, nr 11.
Network for Citizen-centered Restoration Projects in Kobe, https://tm19950117.jp/en/interview/2786/ [dostęp: 8.12.2025].
Pieczywok A., *Złożoność zagrożeń egzystencji człowieka – wybrane zagadnienia*, „Ius et Securitas" 2024, nr 1.
Rehak D., *Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic*, „Safety Science" 2020, nr 123.
Steen R., Haakonsen G., Steiro T.J., *Patterns of Learning: A Systemic Analysis of Emergency Response Operations in the North Sea through the Lens of Resilience Engineering*, „Infrastructures" 2023, nr 2.
Tan M.Z.Y., *Resilience is a dirty word: misunderstood, and how we can truly build it*, „Critical Care" 2022, nr 26.
Weick K.E., Sutcliffe K.M., *Managing the Unexpected: Sustained Performance in a Complex World*, Hoboken 2015.
Włodyka E.M., *Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku*, „Ius et Securitas" 2024, nr 1.
Zhao X., Liu Y. ,Jiang W., Wei D., *Study on the Factors Influencing and Mechanisms Shaping the Institutional Resilience of Mega Railway Construction Projects*, „Sustainability" 2023, nr 10.

Critical Infrastructure Security and the Silent Institutional Resilience

Abstract

The article examines critical infrastructure security from the perspective of institutional resilience, which encompasses not only technical solutions but also the less visible mechanisms shaping the functioning of organisations responsible for crisis management. The point of departure is the assumption that the ability to maintain essential functions under disruptive conditions results not only from formal procedures, but also from practices of action, relationships, and tacit knowledge which remain only partially regulated and standardised. The aim of the article is to demonstrate that the hidden dimension of resilience remains central to critical infrastructure security, despite being frequently marginalised in security policies.

The working hypothesis assumes that infrastructure security depends on the capacity of institutions to operate under uncertainty, and particularly on silent institutional resilience, which manifests itself beyond formal procedures. The research method applied is a qualitative analysis of the literature combined with case studies of selected crisis situations. The findings indicate that informal relations, adaptive capacity, practical staff knowledge and local cooperation networks constitute a key component of resilience, and their development requires long-term organisational processes.

Key words critical infrastructure security, institutional resilience, silent institutional resilience, crisis management, informal networks of action