STUDIA POLITOLOGICZNE VOL. 81
DOI: 10.33896/SPolit.2026.81.14

Bartosz Maziarz[*], *Rafał Kochańczyk*[**]

Regionalna polityka bezpieczeństwa jako fundament odporności instytucjonalnej samorządu województwa wobec współczesnych zagrożeń hybrydowych

Regional Security Policy as a Foundation for the Institutional Resilience of the Voivodeship Government Against Contemporary Hybrid Threats

Słowa kluczowe: *regionalna polityka bezpieczeństwa, odporność instytucjonalna, samorząd województwa, zarządzanie kryzysowe, zagrożenia hybrydowe, infrastruktura krytyczna, ciągłość działania (COOP/BCP)*

Key words: *regional security policy, institutional resilience, voivodeship self-government, crisis management, hybrid threats, critical infrastructure, continuity of operations (COOP/BCP)*

Abstrakt: *Autorzy analizują zasadność i uwarunkowania wdrażania regionalnej polityki bezpieczeństwa przez samorządy województw w Polsce w warunkach rosnącej złożoności środowiska bezpieczeństwa. Kumulacja zagrożeń militarnych (wojna w Ukrainie), hybrydowych (dezinformacja, cyberataki, presja energetyczna, sabotaż) oraz naturalnych i klimatycznych wymusza przejście administracji regionalnej od podejścia reaktywnego do proaktywnego budowania odporności instytucjonalnej. Zastosowano jakościowe studium przypadku biura bezpieczeństwa urzędu marszałkowskiego, oparte na analizie dokumentów, obserwacji uczestniczącej i triangulacji źródeł. Przedstawiono dwufilarowy model regionalnej polityki bezpieczeństwa: (1) sieciowanie współpracy ze służbami i kluczowymi interesariuszami w regionie oraz (2) wzmacnianie odporności własnej urzędu poprzez cykliczną analizę ryzyk, rozwój kompetencji pracowników i zapewnienie zasobów umożliwiających utrzymanie ciągłości działania (COOP/BCP) w warunkach*

[*] ORCID ID: https://orcid.org/0000-0002-2190-7969; doktor nauk społecznych, adiunkt w Instytucie Nauk o Polityce i Administracji Uniwersytetu Opolskiego, Dyrektor Biura Bezpieczeństwa Urzędu Marszałkowskiego Województwa Opolskiego. E-mail: bartosz.maziarz@uni.opole.pl.

[**] ORCID ID: https://orcid.org/0000-0002-1432-1927; doktor nauk społecznych, nadinspektor Policji, Zastępca Komendanta Głównego Policji. E-mail: rafal.kochanczyk@interia.pl.

zakłóceń. Ramą integrującą jest podejście all-hazards, pozwalające projektować gotowość niezależnie od genezy zagrożenia. Wnioski mają charakter aplikacyjny i wskazują warunki transferowalności modelu do innych urzędów marszałkowskich.

Abstract: *This article examines the rationale and practical determinants for implementing regional security policies by Polish voivodeship governments under an increasingly complex threat environment. The accumulation of military threats (the war in Ukraine), hybrid threats (disinformation, cyberattacks, energy pressure, sabotage), and climate-related hazards compels regional administrations to shift from reactive crisis response to proactive institutional resilience-building. The study employs a qualitative case study of a marshal's office security bureau, using document analysis, participant observation, and source triangulation. A two-pillar model of regional security policy is proposed: (1) networking and institutionalized cooperation with regional services and key stakeholders, and (2) strengthening the office's internal resilience through cyclical risk assessment, staff capacity-building, and resources enabling continuity of operations (COOP/BCP) under disruption. The all-hazards approach serves as an integrative framework for preparedness irrespective of threat origin. The conclusions are practice-oriented and specify conditions for transferability to other regional administrations.*

Wprowadzenie

Współczesne środowisko bezpieczeństwa charakteryzuje się wysoką dynamiką i konwergencją zagrożeń, prowadzącą do erozji klasycznych dychotomii: militarne–niemilitarne, wewnętrzne–zewnętrzne, publiczne–prywatne. Z perspektywy administracji samorządowej oznacza to konieczność rozwijania zdolności do funkcjonowania w warunkach niepewności i zakłóceń o zróżnicowanej genezie.

Samorząd województwa pełni istotną rolę w systemie administracji publicznej, realizując zadania z zakresu polityki regionalnej, koordynacji usług publicznych oraz zarządzania rozwojem terytorialnym[1]. Jako podmiot zarządzający infrastrukturą i procesami o znaczeniu regionalnym, urząd marszałkowski stanowi element funkcjonalny systemu bezpieczeństwa państwa, w szczególności w obszarach koordynacji, planowania i zapewniania ciągłości działań w sytuacjach kryzysowych[2].

---

1 OECD, *Lepsze zarządzanie, planowanie i dostarczanie usług w jednostkach samorządu lokalnego w Polsce*, OECD Publishing, Paryż 2021, DOI: 10.1787/b1c061dd-pl oraz Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa, t.j. Dz.U. 2025, poz. 581.

2 P. Chrobak, *The Critical Infrastructure in the Programmes of the Civic Platform (CP, Polish: PO) of the Republic of Poland*, «Przegląd Zachodniopomorski» 2018, t. 33, nr 3, s. 63–84, DOI: 10.18276/pz.2018.3-04 oraz Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm. (Dz.U. 2024, poz. 834, 1222, 1473, 1572 i 1907).

W artykule regionalna polityka bezpieczeństwa oznacza zestaw celów, instrumentów i praktyk organizacyjnych wdrażanych przez samorząd województwa w celu: (a) ograniczania prawdopodobieństwa materializacji zagrożeń, (b) minimalizacji skutków zakłóceń oraz (c) utrzymania zdolności do realizacji funkcji publicznych w warunkach kryzysu. Polityka ta obejmuje zarówno komponent współpracy zewnętrznej (governance wielopodmiotowe), jak i komponent odporności wewnętrznej instytucji (*institutional resilience*), rozumianej jako zdolność absorpcji, adaptacji i utrzymania ciągłości działania[3].

Artykuł odpowiada na cztery pytania badawcze:

- Jakie kategorie zagrożeń determinują potrzebę regionalnej polityki bezpieczeństwa?
- Jakie elementy składają się na efektywny model tej polityki na poziomie urzędu marszałkowskiego?
- W jaki sposób podejście *all-hazards* może być operacjonalizowane w praktyce administracji samorządowej?
- Jakie implikacje praktyczne wynikają z proaktywnego budowania odporności instytucjonalnej?

Cel artykułu stanowi wykazanie, że regionalna polityka bezpieczeństwa jest niezbędnym komponentem zarządzania województwem w warunkach współczesnych zagrożeń.

Bezpieczeństwo regionalne i odporność instytucjonalna

W literaturze obserwuje się przesunięcie od wąskich ujęć bezpieczeństwa, skoncentrowanych na ochronie militarnej, ku ujęciom wielowymiarowym obejmującym czynniki ekonomiczne, społeczne, informacyjne i cybernetyczne[4]. Skuteczne zarządzanie bezpieczeństwem wymaga współdziałania różnych szczebli administracji oraz interesariuszy publicznych i prywatnych, co szczególnie dotyczy poziomu regionalnego[5].

Odporność instytucjonalna odnosi się do zdolności organizacji publicznej do utrzymania kluczowych funkcji w warunkach zakłóceń, z wykorzystaniem adapta-

[3] R. Solecki, P. Kobis, *Public administration in the face of the challenges of the COVID-19 pandemic. Experience of the Małopolska Centre for Entrepreneurship in the implementation of the Małopolska Anti-Crisis Shield*, «Eastern European Journal of Transnational Relations» 2023, t. 7, nr 1, s. 107–121, DOI: 10.15290/eejtr.2023.07.01.10 oraz OECD, *Lepsze zarządzanie*…

[4] V. Boiko, *Comparison of the Polish and Ukrainian Cybersecurity Systems*, «Teka Komisji Politologii i Stosunków Międzynarodowych» 2021, t. 14, nr 2, s. 119–137, DOI: 10.17951/teka.2019.14.2.119-137.

[5] P. Chrobak, *The Critical Infrastructure*…

cji organizacyjnej, zasobów infrastrukturalnych, kompetencji personelu oraz relacji sieciowych[6]. W kontekście urzędów marszałkowskich odporność ta obejmuje:

- zarządzanie ryzykiem i planowanie ciągłości działania,
- przygotowanie proceduralne i szkoleniowe,
- redundancję zasobów krytycznych,
- mechanizmy koordynacji z partnerami w regionie.

Istotnym komponentem jest infrastruktura krytyczna, tj. systemy i obiekty kluczowe dla bezpieczeństwa państwa i obywateli, których ciągłość działania uwarunkowana jest dostępnością energii, łączności, zasobów IT i usług logistycznych[7].

Zarządzanie kryzysowe i rola samorządu województwa

Zarządzanie kryzysowe w Polsce ma charakter wielopoziomowy i wielopodmiotowy. Samorządy terytorialne, w tym samorząd województwa, pełnią rolę nie tylko wykonawczą, lecz również koordynacyjną i planistyczną w fazach prewencji, przygotowania i reagowania na sytuacje kryzysowe[8]. Zgodnie z art. 14 ustawy o zarządzaniu kryzysowym do zadań zarządu województwa należy w szczególności kierowanie działaniami związanymi z monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń w województwie[9]. System opiera się na zasadzie subsydiarności: wyższe szczeble administracji angażują się wówczas, gdy niższe okażą się niewystarczające[10]. Samorząd województwa zajmuje pozycję strategiczną pośrednią, tj. z jednej strony koordynuje działania powiatów i gmin, z drugiej zaś współpracuje z administracją rządową i służbami centralnymi.

Zakres zadań samorządu regionalnego obejmuje zarządzanie infrastrukturą transportową, ochronę zdrowia, edukację i koordynację polityki rozwoju regionalnego. Każda z tych dziedzin posiada wymiar bezpieczeństwa. Zakłócenie funkcjonowania szpitali, sieci dróg czy systemów informatycznych urzędu może mieć bezpośrednie konsekwencje dla życia i zdrowia mieszkańców. Koordynacja między szczeblami administracji publicznej ma jednak charakter doraźny i opiera się głównie na projektach, co stanowi dodatkowy argument za budowaniem trwałych, zinstytucjonalizowanych mechanizmów współpracy[11].

---

6 OECD, *Lepsze zarządzanie*… oraz R. Solecki, P. Kobis, *Public administration*…
7 P. Chrobak, *The Critical Infrastructure*…
8 Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm.
9 Tamże.
10 OECD, *Lepsze zarządzanie*…
11 Tamże.

Doświadczenia pandemii COVID-19 dostarczyły bezprecedensowego materiału empirycznego dotyczącego zdolności adaptacyjnych polskiej administracji publicznej. Analiza działań Małopolskiego Centrum Przedsiębiorczości wykazała, że kluczową determinantą skuteczności okazała się zdolność adaptacyjna instytucji, jej gotowość do elastycznego zarządzania zasobami i utrzymania ciągłości zadań publicznych[12]. Wniosek ten potwierdza, że budowa odporności instytucjonalnej jest racjonalną odpowiedzią na ryzyko zakłóceń systemowych niezależnie od ich źródła. Wymóg ten znalazł wyraz legislacyjny w ustawie o ochronie ludności i obronie cywilnej z 2024 r., która wprost nakłada na organy administracji publicznej obowiązek podejmowania działań ukierunkowanych na zapewnienie ciągłości ich działania oraz organizowania szkoleń i ćwiczeń przygotowujących do działania na wypadek zagrożenia[13].

Zarządzanie ryzykiem w sektorze publicznym nabiera szczególnego znaczenia w kontekście postępującej cyfryzacji administracji. Analiza ryzyka IT wymaga systematycznej identyfikacji i oceny zagrożeń dla systemów informatycznych z uwzględnieniem częstotliwości i skutków ich wystąpienia[14]. Badania OECD wskazują, że główne wyzwania koordynacyjne w polskich samorządach obejmują brak formalnych mandatów, niewystarczające mechanizmy sprawozdawczości i ograniczone stosowanie pisemnych procedur[15]. Regionalna polityka bezpieczeństwa, obejmująca opracowanie i aktualizowanie planów ciągłości działania, stanowi bezpośrednią odpowiedź na te strukturalne słabości.

Cyberbezpieczeństwo jako komponent regionalnej polityki bezpieczeństwa

Wszelkie znaczące zakłócenia w funkcjonowaniu cyberprzestrzeni mają wpływ na bezpieczeństwo transgraniczne, wydajność sektora publicznego i bezpieczeństwo narodowe[16]. Samorząd województwa, zarządzający rozległą infrastrukturą regionalną i przetwarzający znaczne ilości danych wrażliwych, jest zarówno potencjalnym celem cyberataków, jak i kluczowym ogniwem regionalnego systemu cyberbezpieczeństwa.

---

12 R. Solecki, P. Kobis, *Public administration*…

13 Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907 (wejście w życie: 1 stycznia 2025 r.).

14 G. Mazur, H. Mazur, T. Mendyk-Krajewska, *Public sector risk in the context of integrated computerization*, «Ekonomiczne Problemy Usług» 2017, nr 126, s. 371–384, DOI: 10.18276/epu.2017.126/2-37.

15 OECD, *Lepsze zarządzanie*…

16 V. Boiko, *Comparison of the Polish*…

Jednostki samorządu terytorialnego są zobowiązane do bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji oraz do przeprowadzania co najmniej raz w roku audytu wewnętrznego[17]. Badania ujawniają niepokojące niedomknięcia: w 21,5% urzędów analiza ryzyka nie jest realizowana, a niespełna 12% jednostek ubezpieczyło się od ryzyka cyberataku, mimo że dla około 66% gmin cyberprzestępczość stanowi średnie lub duże zagrożenie[18]. Cyberbezpieczeństwo powinno być zatem integrowane z zarządzaniem ryzykiem i ciągłością działania urzędu, a nie traktowane jako obszar odrębny od pozostałych wymiarów bezpieczeństwa instytucjonalnego.

Bezpieczeństwo publiczne i współpraca wielopodmiotowa

Badania dotyczące bezpieczeństwa publicznego na poziomie lokalnym konsekwentnie akcentują, że skuteczność działań zależy od trwałych mechanizmów koordynacji między służbami i instytucjami, a nie od doraźnych reakcji na izolowane incydenty[19]. Analiza działalności Straży Miejskiej Poznania wykazała, że podejście systemowe przynosi trwałe rezultaty, podczas gdy brak kontynuacji dobrych rozwiązań i dostrzeganie problemu wyłącznie przez pryzmat zaistniałych incydentów uniemożliwia pozytywne zmiany w obszarze bezpieczeństwa publicznego[20].

Współpraca wielopodmiotowa napotyka na bariery instytucjonalne, finansowe i organizacyjne[21]. Infrastruktura krytyczna, systemy kluczowe dla bezpieczeństwa państwa i obywateli, stanowi wspólny mianownik różnych podmiotów systemu bezpieczeństwa regionalnego[22]. Jej ochrona przekracza możliwości pojedynczego podmiotu i wymaga skoordynowanego działania administracji samorządowej, służb mundurowych i podmiotów prywatnych. Obowiązki urzędów marszałkowskich w tym zakresie precyzuje ustawa o zarządzaniu kryzysowym, nakładając na zarząd województwa zadania zwią-

17 S. Kańduła, J. Przybylska, A. Kaczyńska, *Transformacja cyfrowa samorządu gminnego w Polsce*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2023, DOI: 10.18559/978-83-8211-166-8.

18 Tamże.

19 P. Antkowiak, A. Radzioch, *Działalność Straży Miejskiej Miasta Poznania w latach 2015–2019*, «Przegląd Politologiczny» 2020, t. 25, nr 2, s. 113–126, DOI: 10.14746/pp.2020.25.2.8.

20 W. Jarczewski, P. Bogdalski, *Social Determinants of Crime and Hatred Incidents at Mass Sports Events in Poland*, «Przegląd Strategiczny» 2019, nr 12, s. 209–228, DOI: 10.14746/ps.2019.1.14.

21 M. Żak-Skwierczyńska, *Bariery we współpracy jednostek samorządu terytorialnego miejskich obszarów funkcjonalnych. Przykład województwa łódzkiego*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2018, DOI: 10.18778/8142-522-3.

22 P. Chrobak, *The Critical Infrastructure*…

zane z ochroną infrastruktury krytycznej i planowaniem ciągłości działania natomiast ustawa o ochronie ludności i obronie cywilnej uzupełnia ten obowiązek o wymóg planowania ewakuacji ludności i przygotowania warunków do zachowania ciągłości łańcucha dostaw[23].

Metodologia

Badanie przeprowadzono w paradygmacie jakościowym, stosując studium przypadku (case study) jako strategię badawczą umożliwiającą analizę złożonych zjawisk instytucjonalnych w ich naturalnym kontekście[24]. Jednostką analizy było biuro bezpieczeństwa urzędu marszałkowskiego rozumiane jako węzeł koordynacji działań bezpieczeństwa i odporności instytucjonalnej.

Zastosowano trzy komplementarne techniki badawcze:

1. Analiza dokumentów (desk research): przegląd regulacji, dokumentów strategicznych i procedur wewnętrznych dotyczących bezpieczeństwa, ryzyka i ciągłości działania.
2. Obserwacja uczestnicząca: wgląd w praktyki planistyczne, szkoleniowe i mechanizmy koordynacji.
3. Triangulacja źródeł: porównywanie ustaleń z dokumentów i obserwacji w celu zwiększenia wiarygodności wniosków[25].

Procedura analityczna polegała na kategoryzacji danych w układzie odpowiadającym pytaniom badawczym oraz na rekonstrukcji mechanizmów działań, tj. w jaki sposób sieciowanie współpracy przekłada się na skrócenie czasu reakcji i jak zasoby energetyczne oraz szkolenia zwiększają zdolność do utrzymania funkcji krytycznych.

Ograniczenia badania: wyniki mają charakter idiograficzny i dotyczą jednego przypadku, co ogranicza możliwość generalizacji statystycznej. Obserwacja uczestnicząca może implikować ryzyko stronniczości interpretacyjnej. Z tego względu wnioski formułowano jako propozycje transferowalne warunkowo (*transferability*), zależne od kontekstu zasobów, struktury organizacyjnej i profilu ryzyk innych urzędów[26].

---

[23] Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm. oraz Ustawa o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907.

[24] P. Ciesiółka, *Systemy monitorowania rewitalizacji w gminach województwa wielkopolskiego*, «Rozwój Regionalny i Polityka Regionalna» 2019, nr 48, s. 37–55, DOI: 10.14746/rrpr.2019.48.03.

[25] Tamże.

[26] M. Żak-Skwierczyńska, *Bariery we współpracy*…

Analiza współczesnych zagrożeń jako przesłanek regionalnej polityki bezpieczeństwa

Wojna w Ukrainie: ciągłość działania i odporność infrastrukturalna

Pełnoskalowa inwazja Federacji Rosyjskiej na Ukrainę zapoczątkowana 24 lutego 2022 roku dostarczyła bezprecedensowego materiału empirycznego dotyczącego odporności instytucji publicznych i infrastruktury krytycznej w warunkach konfliktu zbrojnego[27]. Konflikt uwidocznił, że nowoczesna wojna nie ogranicza się do działań kinetycznych, lecz obejmuje systematyczne uderzenia w infrastrukturę energetyczną, telekomunikacyjną i administracyjną, których celem jest paraliż funkcji państwowych i podważenie morale społeczeństwa[28].

Szczególnie wymowne są doświadczenia ukraińskiej infrastruktury energetycznej. Systematyczne ataki rosyjskie na sieć elektroenergetyczną (jesień 2022, zima 2022–2023) doprowadziły do masowych przerw w dostawach energii. Jednocześnie ukraiński sektor energetyczny wykazał zdumiewającą odporność, pracownicy sektora komunalnego zapewniali funkcjonowanie i szybkie odtwarzanie infrastruktury krytycznej[29]. Lekcja jest jednoznaczna: zdolność do utrzymania i szybkiego odtwarzania funkcji krytycznych w warunkach ataków na infrastrukturę energetyczną stanowi warunek konieczny przetrwania instytucji publicznych w konflikcie zbrojnym.

Ukraiński przykład potwierdza, że ciągłość działania administracji ma fundamentalne znaczenie strategiczne: zachowanie stabilności systemów finansowych, bankowych i logistycznych zaopatrzenia bezpośrednio wpływa na zdolność do prowadzenia działań obronnych i utrzymania morale społeczeństwa[30]. Dla polskich samorządów województw oznacza to, że planowanie ciągłości działania powinno uwzględniać scenariusze długotrwałych przerw w zasilaniu i zakłóceń łączności[31]. Analiza zarządzania przyjęciem uchodźców wojennych z Ukrainy we Wrocławiu wykazała, że skuteczność reagowania kryzysowego była wynikiem doraźnej improwizacji, a nie jakości istniejącego

[27] A. Badawi, *Unraveling the Russian-Ukrainian Conflict: Geopolitical Dynamics, Religious Tensions*, «Wschód Europy. Studia Humanistyczno-Społeczne» 2024, t. 10, nr 1, s. 11–34, DOI: 10.17951/we.2024.10.1.11-34.

[28] M. Hordiichuk i in., *How the Information Warfare Turns Into Full-Scale Military Aggression: the Experience of Ukraine*, «Przegląd Strategiczny» 2024, nr 17, s. 13–38, DOI: 10.14746/ps.2024.1.1.

[29] Tamże.

[30] Tamże.

[31] P. Chrobak, *The Critical Infrastructure*…

systemu, co podkreśla wartość proaktywnego budowania gotowości instytucjonalnej[32].

Zagrożenia hybrydowe: cyberataki, dezinformacja i sabotaż

Zagrożenia hybrydowe charakteryzują się łączeniem instrumentów militarnych i niemilitarnych przy zachowaniu niejednoznaczności sprawstwa[33]. Federacja Rosyjska konsekwentnie stosuje wojnę hybrydową, dążąc do uzyskania przewagi poprzez hybrydyzację zarówno strony walczącej, jak i przestrzeni konfliktu, jego genezy i natury[34]. Analiza rosyjskich „środków aktywnych" wskazuje, że metody te obejmują cyberataki na infrastrukturę krytyczną, w 2015 r. na ukraińskiego operatora energetycznego Prykarpattyaoblenerho, w 2016 r. na Skarb Państwa Ukrainy i Ministerstwo Finansów, a w 2018 r. wirus NotPetya wyrządził globalne szkody[35].

Cyberbezpieczeństwo sektora energetycznego stanowi szczególnie wrażliwy obszar. Blackout w zachodniej Ukrainie w 2016 roku był cyberatakiem o wymiarze międzynarodowym, demonstrującym zdolność zakłócenia dostaw energii poprzez działania w cyberprzestrzeni[36]. Polityka cyberbezpieczeństwa krajów Grupy Wyszehradzkiej, w tym Polski, ewoluuje w odpowiedzi na te zagrożenia[37]. Nowa Strategia Bezpieczeństwa Narodowego RP z 2020 roku uwzględnia zjawisko hybrydowości i operacje w cyberprzestrzeni[38].

Dezinformacja i operacje informacyjne stanowią kolejny kluczowy wymiar zagrożeń hybrydowych. Rosyjska propaganda antyukraińska, stosująca wszystkie metody propagandy i fałszowania faktów, jest produkowana i rozpowszechniana do różnych grup docelowych, w tym obywateli krajów zachod-

---

32 M. Błaszczyk i in., *Governance agility in reception of war refugees from Ukraine: The case of Wrocław, Poland*, «Social Policy and Administration» 2023, t. 57, nr 7, s. 1289–1303, DOI: 10.1111/spol.12934.

33 M. Orzechowski, *Wojna hybrydowa jako przejaw neoimperialnego ekspansjonizmu w strategii politycznej Federacji Rosyjskiej wobec Ukrainy*, «Teka Komisji Politologii i Stosunków Międzynarodowych» 2018, t. 13, nr 2, s. 71–88, DOI: 10.17951/teka.2018.13.2.71-88.

34 Tamże.

35 D. Dubov i in., *„Active Measures" of the USSR Against the USA: Old Soviet Games in the New Geopolitical Reality*, «Przegląd Strategiczny» 2020, nr 13, s. 57–80, DOI: 10.14746/ps.2020.1.4.

36 K. Konaszczuk, *Zagrożenia cyberbezpieczeństwa sektora ropy naftowej, gazu ziemnego i energii elektrycznej w kontekście ewolucji technologicznej*, «Studia Iuridica Lublinensia» 2021, t. 30, nr 3, s. 261–280, DOI: 10.17951/sil.2021.30.3.261-280.

37 M. Górka, *Cybersecurity in the V4 Policy in 2011–2022*, «Środkowoeuropejskie Studia Polityczne» 2022, nr 4, s. 5–28, DOI: 10.14746/ssp.2022.4.1.

38 A. Sobczak, *The New National Security Strategy of the Republic of Poland*, [w:] *National Security Strategies in a Comparative Perspective*, Wydawnictwo Naukowe Scholar, Warszawa 2021, DOI: 10.4467/25444972SMZP.21.001.13843.

nich[39]. Wymaga to od polskich instytucji publicznych budowania odporności informacyjnej. Doświadczenia ukraińskiej polityki informacyjnej w warunkach wojennych, mobilizacja obywateli, zmniejszenie paniki, zwiększenie krytycyzmu wobec fałszywych informacji potwierdzają, że sprawna komunikacja kryzysowa jest kluczowym elementem odporności instytucjonalnej[40]. Rekomendacje dla Polski wskazują na konieczność niezawodności komunikacji jako jednego z kluczowych elementów odporności narodowej[41].

Niepewność transatlantycka jako czynnik presji na zdolności własne

Zmienność polityki transatlantyckiej i wahania zaangażowania USA w bezpieczeństwo europejskie tworzą środowisko strategicznej niepewności z bezpośrednimi implikacjami dla planowania bezpieczeństwa na wszystkich szczeblach administracji. Analiza konfliktu rosyjsko-ukraińskiego wskazuje, że tylko przy użyciu relacji handlowych nie jest możliwe zapewnienie pokoju, a od Unii Europejskiej coraz mocniej wymaga się większego wkładu w jej własne bezpieczeństwo[42]. Dla polskich samorządów województw oznacza to, że nie mogą zakładać nieograniczonej dostępności zewnętrznego wsparcia operacyjnego i logistycznego w sytuacji kryzysu.

Szczyt NATO w Warszawie (2016) wskazał, że tylko ściśle skoordynowane wysiłki cywilów i wojska zapewniają skuteczną odporność. Komunikat Szczytu stwierdza, że „gotowość cywilna jest centralnym filarem odporności sojuszników i krytycznym czynnikiem umożliwiającym zbiorową obronę Sojuszu"[43]. Samorządy województw jako podmioty cywilne zarządzające infrastrukturą regionalną, są integralnym elementem systemu gotowości cywilnej NATO. Ich zdolność do funkcjonowania w kryzysie jest zatem nie tylko kwestią lokalną, lecz elementem szerszej architektury bezpieczeństwa sojuszniczego.

---

39 M. Hordiichuk i in., *How the Information Warfare*… oraz О. Шевченко, A. Yalovets, *Anti-Ukrainian narratives of Russia in the global information space*, «Wschód Europy. Studia Humanistyczno-Społeczne» 2023, t. 9, nr 2, s. 11–28, DOI: 10.17951/we.2023.9.2.11-28.

40 Н. Карпчук, *Information and Communication Policy in Wartime: the Case of Ukraine*, «Historia i Polityka» 2022, nr 41(48), s. 9–24, DOI: 10.12775/HiP.2022.022.

41 A. Nowak, *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, «Roczniki Nauk Społecznych» 2022, t. 14 (50), nr 3, s. 5–26, DOI: 10.18290/rns.2016.44.3-5.

42 S. Tankovsky, *Economic Opportunities or Integrational Challenges – The Case Study of Ukraine, rozprawa doktorska*, Corvinus University of Budapest, Budapest 2023.

43 B. Madlovics, B. Magyar, *Ukraine's Patronal Democracy and the Russian Invasion*, CEU Press, Budapest–New York 2023, DOI: 10.7829/9789633675533.

Zagrożenia naturalne i klimatyczne: uzasadnienie podejścia *all-hazards*

Rosnąca częstotliwość i intensywność ekstremalnych zjawisk pogodowych, powodzi, susz, wichur, długotrwałych mrozów, zwiększa ryzyko zakłóceń infrastrukturalnych mogących paraliżować funkcjonowanie instytucji publicznych w sposób analogiczny do skutków zagrożeń militarnych i hybrydowych. Podejście *all-hazards* umożliwia budowę zdolności horyzontalnych użytecznych zarówno w kryzysach naturalnych, jak i hybrydowych czy militarnych[44]. Koncepcja ryzyka jako funkcji prawdopodobieństwa i skutku zdarzeń wskazuje, że inwestycje w zasoby o szerokim spektrum zastosowań mają wyższą oczekiwaną wartość redukcji ryzyka niż zasoby dedykowane jednemu scenariuszowi kryzysowemu[45]. Zarówno konflikty zbrojne, jak i katastrofy naturalne wymagają podobnych zdolności adaptacyjnych i odtworzeniowych[46].

Model regionalnej polityki bezpieczeństwa: studium przypadku Biura Bezpieczeństwa Urzędu Marszałkowskiego Województwa Opolskiego

Umocowanie organizacyjne i struktura modelu

Biuro Bezpieczeństwa Urzędu Marszałkowskiego Województwa Opolskiego, stanowi wyspecjalizowaną jednostkę organizacyjną odpowiedzialną za koordynację działań w obszarze bezpieczeństwa i odporności urzędu marszałkowskiego. Jego umocowanie w strukturze urzędu odzwierciedla rosnące znaczenie problematyki bezpieczeństwa i sprzyja instytucjonalizacji bezpieczeństwa jako stałego obszaru zarządzania, a nie działania ad hoc. Podstawę prawną działania tej jednostki tworzą przepisy ustawy o samorządzie województwa, przyznające samorządowi województwa szeroką autonomię organizacyjną w zakresie tworzenia wewnętrznych struktur urzędu marszałkowskiego[47] oraz ustawy o zarządzaniu kryzysowym, nakładającej na zarząd województwa obowiązki w zakresie opracowywania i aktualizacji planów zarządzania kryzysowego, analizy zagrożeń i koordynacji działań z organami administracji rządowej[48]. Samorząd regionalny realizuje coraz szerszy zakres zadań z zakresu

44 P. Chrobak, *The Critical Infrastructure*…

45 G. Mazur i in., *Public sector risk*…

46 I. Krawczyk-Sokołowska, *Zrównoważony rozwój w zarządzaniu*, [w:] *Zrównoważony rozwój w zarządzaniu*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023, DOI: 10.15611/pn.2023.532.07.

47 Ustawa o samorządzie województwa, t.j. Dz.U. 2025 poz. 581.

48 Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023 poz. 122 ze zm.

infrastruktury i usług publicznych, co oznacza, że jego sprawne funkcjonowanie w kryzysie ma bezpośredni wpływ na jakość życia mieszkańców[49].

W praktyce Biuro Bezpieczeństwa pełni cztery wzajemnie uzupełniające się funkcje:

- analityczną – systematyczna ocena ryzyk i zagrożeń dla ciągłości działania urzędu;
- koordynacyjną – budowanie i utrzymywanie sieci współpracy ze służbami regionu;
- szkoleniową – budowa kompetencji personelu w zakresie zachowania w sytuacjach kryzysowych;
- logistyczno-zasobową – zapewnienie zasobów materialnych umożliwiających realizację funkcji krytycznych w kryzysie.

Na podstawie analizy przypadku proponuje się dwufilarowy model regionalnej polityki bezpieczeństwa:

- Filar I – sieciowanie współpracy regionalnej (mechanizmy koordynacji i interoperacyjności ze służbami i interesariuszami regionu),
- Filar II – odporność wewnętrzna urzędu (ryzyko–kompetencje–zasoby–ciągłość działania).

Oba filary są wzajemnie uzupełniające. Filar I zapewnia zdolność do koordynacji z zewnętrznymi podmiotami systemu bezpieczeństwa, natomiast Filar II gwarantuje zdolność do samodzielnego funkcjonowania urzędu w warunkach zakłócenia normalnego trybu pracy.

Filar I: Sieciowanie współpracy ze służbami i interesariuszami regionu

Pierwszy filar obejmuje budowę trwałych relacji roboczych z kluczowymi podmiotami systemu bezpieczeństwa w regionie: Policją, Państwową Strażą Pożarną (PSP), Strażą Graniczną (SG), Państwowym Ratownictwem Medycznym (PRM), jednostkami Sił Zbrojnych, operatorami infrastruktury krytycznej i jednostkami samorządu niższych szczebli. Sieciowanie wykracza poza formalne procedury i obejmuje budowanie nieformalnych kanałów komunikacji, wzajemne poznanie procedur poszczególnych służb oraz wypracowanie wspólnych protokołów działania w sytuacjach kryzysowych.

W ujęciu operacyjnym sieciowanie obejmuje cztery kluczowe elementy:

1. regularne kanały kontaktu i wymiany informacji – formalne (spotkania robocze, protokoły współpracy) i nieformalne;
2. uzgodnienia dotyczące ról i odpowiedzialności w scenariuszach kryzysowych;

[49] OECD, *Lepsze zarządzanie…*

3. cykliczne ćwiczenia i testy procedur identyfikujące luki w planach reagowania;
4. uzgadnianie standardów komunikacji i priorytetów działań zapewniające interoperacyjność.

Skuteczność bezpieczeństwa publicznego zależy od sprawnej koordynacji między służbami[50]. Podejście systemowe i długofalowe jest bardziej efektywne niż reakcje incydentalne[51]. Doświadczenia zarządzania przyjęciem uchodźców wojennych we Wrocławiu potwierdzają, że elastyczność i „wspólnota wyższego celu" umożliwiają skuteczne reagowanie kryzysowe, ale zarazem wskazują, że opierała się ona na doraźnej improwizacji, a nie jakości istniejącego systemu, co podkreśla wartość proaktywnego budowania sieci współpracy przed materializacją kryzysu[52]. Bariery instytucjonalne i finansowe utrudniają trwałą współpracę między jednostkami samorządu terytorialnego, Biuro Bezpieczeństwa UMWO, posiadające formalny mandat i stałe zasoby, może pełnić rolę katalizatora przełamującego te bariery[53].

Filar II: Wzmacnianie odporności urzędu (*internal resilience*)

Cykliczna analiza ryzyk i potrzeb *(risk governance)*

Podstawą odporności instytucjonalnej jest systematyczna identyfikacja i analiza ryzyk. Ocena obejmuje co najmniej trzy grupy zagrożeń:

- klęski żywiołowe i zdarzenia klimatyczne,
- przerwy w dostawie energii i zakłócenia infrastrukturalne,
- zagrożenia związane z konfliktem zbrojnym i presją hybrydową – zgodnie z zasadą *all-hazards*[54].

Obowiązek opracowania Planu Zarządzania Kryzysowego Województwa, obejmującego charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, spoczywa na Zarządzie Województwa z mocy ustawy o zarządzaniu kryzysowym[55]. Ustawa o ochronie ludności i obronie cywilnej rozszerza ten obowiązek, nakładając na organy administracji publicznej zadanie przeprowadzania oceny ryzyka i planowania działań ochronnych w ramach zintegrowanego systemu ochrony ludności[56]. Zarządzanie ryzykiem zakłada analizę prawdopodobieństwa i skutków zdarzeń, a projektowanie działań redukujących

50 P. Antkowiak, A. Radzioch, *Działalność Straży Miejskiej*…
51 W. Jarczewski, P. Bogdalski, *Social Determinants*…
52 M. Błaszczyk i in., *Governance agility*…
53 M. Żak-Skwierczyńska, *Bariery we współpracy*…
54 P. Chrobak, *The Critical Infrastructure*…
55 Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm.
56 Ustawa o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907.

ryzyko musi mieć charakter ciągły[57]. Identyfikowanie i monitorowanie ryzyka dostarcza kadrze kierowniczej informacji o kierunkach doskonalenia kontroli zarządczej[58].

Cykliczna analiza ryzyk jest szczególnie istotna wobec niepokojących niedomknięć: w 21,5% urzędów analiza ryzyka nie jest realizowana[59]. Deficyt ten oznacza, że instytucja nie jest w stanie adekwatnie przygotować się na zagrożenia, których nie zidentyfikowała. Biuro Bezpieczeństwa UMWO, realizując cykliczną analizę ryzyk, wypełnia tę lukę i tworzy podstawę dla racjonalnego planowania inwestycji w bezpieczeństwo.

Redundancja energetyczna i tryb pracy w degradacji

Z doświadczeń ukraińskich wynika jednoznacznie, że energia elektryczna i łączność stanowią warunek konieczny funkcjonowania nowoczesnej administracji publicznej. Odporność ukraińskiego sektora energetycznego była możliwa dzięki wcześniejszemu przygotowaniu, w tym posiadaniu planów awaryjnych i zdolności do szybkiego przywracania funkcji krytycznych[60]. Rekomendacje dla Polski podkreślają konieczność posiadania planów awaryjnych oraz odpowiednio zabezpieczonych sieci elektroenergetycznych[61].

W badanym przypadku wdrożono wielowarstwowy system redundancji energetycznej sfinansowany ze środków OLiOC: agregaty prądotwórcze o zróżnicowanej mocy (w tym jednostka wysokiej mocy rzędu 100 kVA/kW) zapewniają zasilanie kluczowych systemów urzędu, w tym systemów informatycznych i łączności. Systemy infrastruktury krytycznej obejmują sieci łączności i telekomunikacyjne jako jeden z kluczowych elementów, a ich ciągłość w warunkach braku zasilania sieciowego jest warunkiem koniecznym efektywnego zarządzania kryzysowego[62]. Uzupełnienie stanowią banki energii, oświetlenie awaryjne oraz powerbanki dla pracowników. Zestaw tych rozwiązań tworzy zdolność do pracy w trybie degradacji, utrzymania minimalnych procesów i komunikacji, w warunkach długotrwałych zakłóceń[63].

57 G. Mazur i in., *Public sector risk*…
58 S. Kańduła i in., *Transformacja cyfrowa*…
59 Tamże.
60 M. Hordiichuk i in., *How the Information Warfare*…
61 A. Nowak, *Budowa odporności*…
62 P. Chrobak, *The Critical Infrastructure*…
63 A. Nowak, *Budowa odporności*…

Rozwój kompetencji personelu jako „warstwa odporności"

Odporność instytucji publicznych jest w znaczącym stopniu determinowana przez kompetencje, nawyki i zdolności adaptacyjne personelu. Doświadczenia pandemii COVID-19 wykazały, że kluczową determinantą skuteczności była zdolność adaptacyjna instytucji jako wypadkowa kompetencji i gotowości konkretnych pracowników do działania w warunkach stresu i niepewności[64]. Obowiązek organizowania szkoleń i ćwiczeń z zakresu ochrony ludności i obrony cywilnej, skierowanych do pracowników administracji publicznej, wynika wprost z ustawy o ochronie ludności i obronie cywilnej[65].

Szkolenia pracowników obejmują cztery kluczowe obszary:

1. procedury ewakuacji i zachowania w zdarzeniach nagłych: budowanie nawyków i odruchów działania w warunkach stresu;
2. podstawy komunikacji kryzysowej: zasady informowania i korzystania z alternatywnych kanałów komunikacji przy awarii systemów podstawowych;
3. świadomość zagrożeń hybrydowych: rozpoznawanie dezinformacji, phishingu i innych form ataków cybernetycznych i socjotechnicznych;
4. elementy bezpieczeństwa fizycznego i organizacyjnego: postępowanie z informacjami wrażliwymi i ochrona dostępu do systemów.

Pracownicy urzędów stanowią pierwszą linię obrony przed atakami cybernetycznymi ukierunkowanymi na czynnik ludzki. Szkolenia z zakresu świadomości cyberzagrożeń budują „ludzką zaporę" uzupełniającą techniczne środki bezpieczeństwa. Zarówno samorząd, jak i jego pracownicy muszą być przygotowani na wprowadzenie nowych rozwiązań i przejść odpowiednie szkolenia – regularność szkoleń jest równie ważna jak ich treść[66].

Zasoby i wyposażenie kryzysowe jako instrument ciągłości działania

Zapewnienie zasobów kryzysowych stanowi materialny wymiar odporności instytucjonalnej. W badanym przypadku zakup wyposażenia obejmuje trzy kategorie zasobów:

1. Zasoby energetyczne (agregaty prądotwórcze, banki energii, oświetlenie awaryjne, systemy łączności internetowej): zapewniają ciągłość zasilania kluczowych systemów urzędu; uzasadnione zarówno z perspektywy zagrożeń naturalnych, jak i hybrydowych.

---

64 R. Solecki, P. Kobis, *Public administration*…

65 Ustawa o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907.

66 S. Kańduła i in., *Transformacja cyfrowa*…

2. Zasoby osobiste personelu (powerbanki, ubrania ochronne): umożliwiają utrzymanie łączności i podstawowego bezpieczeństwa pracowników w różnych scenariuszach kryzysowych.
3. Zasoby długotrwałego funkcjonowania (śpiwory, łóżka polowe): umożliwiają całodobowe dyżurowanie kluczowego personelu w sytuacjach kryzysowych wymagających ciągłej obecności.

Dobór wyposażenia odzwierciedla zasadę *all-hazards*, tj. każdy z zakupionych zasobów ma charakter wielofunkcyjny i jest użyteczny w różnych scenariuszach kryzysowych. Ta wielofunkcyjność zwiększa efektywność inwestycji w bezpieczeństwo, zapewniając gotowość na różne scenariusze przy ograniczonych nakładach finansowych.

Wkład modelu: instytucjonalizacja prewencji i interoperacyjności

Przedstawiony model wnosi wartość poprzez przełożenie ogólnych postulatów odporności na konkretne instrumenty organizacyjne: sieciowanie współpracy, cykliczną analizę ryzyk, rozwój kompetencji oraz zapewnienie zasobów ciągłości działania. W porównaniu z podejściami reaktywnymi model wzmacnia przygotowanie instytucji przed materializacją zagrożenia, ograniczając koszty reorganizacji w trakcie kryzysu[67]. Zamiast koncentrować się na jednym wymiarze bezpieczeństwa, Biuro Bezpieczeństwa UMWO realizuje zintegrowaną politykę obejmującą wszystkie kluczowe wymiary gotowości kryzysowej. Podejście to odpowiada na złożoność zagrożeń hybrydowych łączących elementy militarne, cybernetyczne, informacyjne i energetyczne[68].

Bezpieczeństwo jako inwestycja w ciągłość działania (COOP/BCP)

W sektorze publicznym koszty zakłóceń obejmują nie tylko straty bezpośrednie (przerwanie realizacji zadań), lecz również koszty reputacyjne i społeczne (spadek zaufania, opóźnienia w usługach, koszty odtwarzania systemów). W świetle koncepcji ryzyka jako funkcji prawdopodobieństwa i skutku zdarzeń inwestycje w odporność należy interpretować jako instrument redukcji

[67] R. Solecki, P. Kobis, *Public administration*…

[68] M. Orzechowski, *Wojna hybrydowa*…; A. Nowak, *Budowa odporności*…; M. Hordiichuk i in., *How the Information Warfare*…

ryzyka i ochrony ciągłości działania, a nie jako wydatki „dodatkowe"[69]. Argument ten jest szczególnie istotny przy zagrożeniach niskoprawdopodobnych, lecz wysokoskutkowych takich jak długotrwały blackout lub poważny incydent cybernetyczny.

Rekomendacje dla Polski wskazują, że odporność stanowi fundament odstraszania i obrony[70]. Inwestycje w bezpieczeństwo instytucjonalne mają zatem zarówno wartość operacyjną (zapewnienie ciągłości działania), jak i strategiczną (odstraszanie potencjalnych agresorów poprzez demonstrację gotowości). Samorząd województwa przygotowany na różne scenariusze kryzysowe jest mniej podatny na destabilizację i tym samym mniej atrakcyjnym celem działań hybrydowych.

Transferowalność i warunki replikacji modelu

Model może być replikowany przez inne samorządy województw, jednak jego skuteczność zależy od trzech warunków:

- dopasowania do profilu ryzyk regionalnych: województwa różnią się ekspozycją na różne typy zagrożeń (powodzie, infrastruktura przemysłowa, węzły transportowe, bliskość granicy), co wymaga dostosowania analizy ryzyk i doboru zasobów kryzysowych;
- umocowania organizacyjnego: skuteczność biura bezpieczeństwa zależy od formalnego mandatu, dostępu do kierownictwa urzędu i adekwatnych zasobów;
- minimalnego poziomu zasobów i kompetencji: wdrożenie wymaga zarówno nakładów finansowych na wyposażenie kryzysowe, jak i kompetencji organizacyjnych do realizacji szkoleń i budowania sieci współpracy.

Bariery instytucjonalne i finansowe utrudniające trwałą współpracę między jednostkami samorządu terytorialnego mogą być przełamywane poprzez formalizację współpracy (protokoły, porozumienia), budowanie kultury bezpieczeństwa w regionie oraz dzielenie się doświadczeniami między urzędami marszałkowskimi[71]. Urząd marszałkowski może pełnić rolę lidera i katalizatora budowania odporności w całym regionie, inspirując podobne działania na poziomie powiatów i gmin.

[69] G. Mazur i in., *Public sector risk*…
[70] A. Nowak, *Budowa odporności*…
[71] M. Żak-Skwierczyńska, *Bariery we współpracy*…

Ograniczenia i kierunki dalszych badań

Ograniczenia wynikają z zastosowanego studium przypadku oraz z braku ilościowych miar skuteczności, takich jak czas odtwarzania procesów, poziom gotowości personelu mierzony testami czy wskaźniki dojrzałości ciągłości działania. W dalszych badaniach zasadne byłoby:

- porównanie kilku urzędów marszałkowskich (multiple-case study) w celu identyfikacji czynników różnicujących skuteczność regionalnych polityk bezpieczeństwa;
- wprowadzenie wskaźników dojrzałości ciągłości działania i cyberodporności umożliwiających benchmarking;
- ocena efektywności szkoleń i ćwiczeń w ujęciu przed–po;
- analiza kosztów i korzyści inwestycji w bezpieczeństwo instytucjonalne w perspektywie długoterminowej.

Wnioski i rekomendacje

Wnioski

1. Złożoność współczesnych zagrożeń (militarne, hybrydowe, naturalne) wymusza na samorządach województw rozwijanie odporności instytucjonalnej jako stałego komponentu zarządzania.
2. Dwufilarowy model (sieciowanie + odporność własna urzędu) stanowi spójną odpowiedź organizacyjną na ryzyka regionalne.
3. Podejście all-hazards umożliwia projektowanie zdolności horyzontalnych (energia, łączność, procedury, kompetencje) użytecznych w wielu scenariuszach.
4. Nakłady na bezpieczeństwo należy traktować jako inwestycję w ciągłość działania instytucji i redukcję kosztów zakłóceń[72].
5. Czynnik ludzki (kompetencje, nawyki, świadomość zagrożeń) jest równorzędny wobec zasobów materialnych[73].

Rekomendacje

1. Powołać lub wzmocnić biuro bezpieczeństwa jako jednostkę odpowiedzialną za regionalną politykę bezpieczeństwa i odporność urzędu, korzystając

[72] G. Mazur i in., *Public sector risk*…
[73] S. Kańduła i in., *Transformacja cyfrowa*…

z autonomii organizacyjnej przyznanej samorządowi województwa przez ustawę o samorządzie województwa[74].

2. Wdrożyć cykliczną analizę ryzyk all-hazards, obejmującą ryzyka naturalne, technologiczne, hybrydowe i militarne, realizując ustawowy obowiązek opracowania i aktualizacji Planu Zarządzania Kryzysowego Województwa oraz oceny ryzyka wymaganej przepisami ustawy o ochronie ludności i obronie cywilnej[75].
3. Zinstytucjonalizować współpracę ze służbami poprzez stałe fora wymiany informacji, wspólne ćwiczenia i protokoły interoperacyjności.
4. Zapewnić redundancję energetyczną i łączności dla utrzymania funkcji krytycznych urzędu w warunkach zakłóceń.
5. Uzupełnić zasoby kryzysowe o elementy umożliwiające długotrwałą pracę w trybie degradacji.
6. Zrealizować program szkoleń i ćwiczeń obejmujący procedury kryzysowe, komunikację, cyberhigienę i rozpoznawanie operacji wpływu, wypełniając obowiązek wynikający z ustawy o ochronie ludności i obronie cywilnej[76].
7. Opracować i testować plan ciągłości działania (COOP/BCP) z regularnymi przeglądami i aktualizacjami, jako element Planu Zarządzania Kryzysowego Województwa[77].
8. Udostępniać dobre praktyki powiatom i gminom (efekt kaskadowy), budując spójność odporności w regionie.

Zakończenie

Regionalna polityka bezpieczeństwa powinna być traktowana jako komponent nowoczesnego zarządzania województwem, a nie jako zadanie incydentalne. W warunkach zagrożeń hybrydowych, klimatycznych i infrastrukturalnych utrzymanie ciągłości działania administracji regionalnej wymaga zarówno sieciowej współpracy, jak i wewnętrznej odporności organizacyjnej. Zaproponowany model dwufilarowy stanowi praktyczną propozycję operacjonalizacji podejścia *all-hazards* w urzędzie marszałkowskim i może stanowić punkt odniesienia dla innych regionów – przy zachowaniu wymogu adaptacji do lokalnego profilu ryzyk i zasobów.

---

74 Ustawa o samorządzie województwa, t.j. Dz.U. 2025, poz. 581.

75 Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm.; Ustawa o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907.

76 Ustawa o ochronie ludności i obronie cywilnej, Dz.U. 2024, poz. 1907.

77 Ustawa o zarządzaniu kryzysowym, t.j. Dz.U. 2023, poz. 122 ze zm.

Bibliografia

Antkowiak P., Radzioch A., *Działalność Straży Miejskiej Miasta Poznania w latach 2015–2019*, «Przegląd Politologiczny» 2020, t. 25, nr 2, DOI: 10.14746/pp.2020.25.2.8.

Badawi A., *Unraveling the Russian-Ukrainian Conflict: Geopolitical Dynamics, Religious Tensions*, «Wschód Europy. Studia Humanistyczno-Społeczne» 2024, t. 10, nr 1, DOI: 10.17951/we.2024.10.1.11-34.

Błaszczyk M. i in., *Governance agility in reception of war refugees from Ukraine: The case of Wrocław, Poland*, «Social Policy and Administration» 2023, t. 57, nr 7, DOI: 10.1111/spol.12934.

Boiko V., *Comparison of the Polish and Ukrainian Cybersecurity Systems*, «Teka Komisji Politologii i Stosunków Międzynarodowych» 2021, t. 14, nr 2, DOI: 10.17951/teka.2019.14.2.119-137.

Chrobak P., *The Critical Infrastructure in the Programmes of the Civic Platform (CP, Polish: PO) of the Republic of Poland*, «Przegląd Zachodniopomorski» 2018, t. 33, nr 3, DOI: 10.18276/pz.2018.3-04.

Ciesiółka P., *Systemy monitorowania rewitalizacji w gminach województwa wielkopolskiego*, «Rozwój Regionalny i Polityka Regionalna» 2019, nr 48, DOI: 10.14746/rrpr.2019.48.03.

Dubov D. i in., *„Active Measures" of the USSR Against the USA: Old Soviet Games in the New Geopolitical Reality*, «Przegląd Strategiczny» 2020, nr 13, DOI: 10.14746/ps.2020.1.4.

Geppert M., Konieczny P., *Analysis of Potential Threats to the Critical Infrastructure of the 31st Tactical Air Base, in the Context of the Security of the Poznan Agglomeration*, «Przegląd Strategiczny» 2024, nr 17, DOI: 10.14746/ps.2024.1.10.

Górka M., *Cybersecurity in the V4 Policy in 2011–2022*, «Środkowoeuropejskie Studia Polityczne» 2022, nr 4, DOI: 10.14746/ssp.2022.4.1.

Hordiichuk M. i in., *How the Information Warfare Turns Into Full-Scale Military Aggression: the Experience of Ukraine*, «Przegląd Strategiczny» 2024, nr 17, DOI: 10.14746/ps.2024.1.1.

Jarczewski W., Bogdalski P., *Social Determinants of Crime and Hatred Incidents at Mass Sports Events in Poland*, «Przegląd Strategiczny» 2019, nr 12, DOI: 10.14746/ps.2019.1.14.

Kańduła S., Przybylska J., Kaczyńska A., *Transformacja cyfrowa samorządu gminnego w Polsce*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2023, DOI: 10.18559/978-83-8211-166-8.

Konaszczuk K., *Zagrożenia cyberbezpieczeństwa sektora ropy naftowej, gazu ziemnego i energii elektrycznej w kontekście ewolucji technologicznej*, «Studia Iuridica Lublinensia» 2021, t. 30, nr 3, DOI: 10.17951/sil.2021.30.3.261-280.

Krawczyk-Sokołowska I., *Zrównoważony rozwój w zarządzaniu*, [w:] *Zrównoważony rozwój w zarządzaniu*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023, DOI: 10.15611/pn.2023.532.07.

Madlovics B., Magyar B., *Ukraine's Patronal Democracy and the Russian Invasion*, CEU Press, Budapest–New York 2023, DOI: 10.7829/9789633675533.

Mazur G., Mazur H., Mendyk-Krajewska T., *Public sector risk in the context of integrated computerization*, «Ekonomiczne Problemy Usług» 2017, nr 126, DOI: 10.18276/epu.2017.126/2-37.

Nowak A., *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, «Roczniki Nauk Społecznych» 2022, t. 14(50), nr 3, DOI: 10.18290/rns.2016.44.3-5.

Orzechowski M., *Wojna hybrydowa jako przejaw neoimperialnego ekspansjonizmu w strategii politycznej Federacji Rosyjskiej wobec Ukrainy*, «Teka Komisji Politologii i Stosunków Międzynarodowych» 2018, t. 13, nr 2, DOI: 10.17951/teka.2018.13.2.71-88.

Sobczak A., *The New National Security Strategy of the Republic of Poland,* [w:] *National Security Strategies in a Comparative Perspective*, Wydawnictwo Naukowe Scholar, Warszawa 2021, DOI: 10.4467/25444972SMZP.21.001.13843.

Solecki R., Kobis P., *Public administration in the face of the challenges of the COVID-19 pandemic*, «Eastern European Journal of Transnational Relations» 2023, t. 7, nr 1, DOI: 10.15290/eejtr.2023.07.01.10.

Tankovsky S., *Economic Opportunities or Integrational Challenges – The Case Study of Ukraine*, rozprawa doktorska, Corvinus University of Budapest, Budapest 2023.

Willa R., Płonka M., *European Union in the Face of Russian Aggression against Ukraine (2014–2023)*, «Historia i Polityka» 2024, nr 47(54), DOI: 10.12775/HiP.2024.001.

Żak-Skwierczyńska M., *Bariery we współpracy jednostek samorządu terytorialnego miejskich obszarów funkcjonalnych. Przykład województwa łódzkiego*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2018, DOI: 10.18778/8142-522-3.

Карпчук Н. (Karpchuk N.), *Information and Communication Policy in Wartime: the Case of Ukraine*, «Historia i Polityka» 2022, nr 41(48), DOI: 10.12775/HiP.2022.022.

Шевченко О. (Shevchenko O.), Yalovets A., *Anti-Ukrainian narratives of Russia in the global information space*, «Wschód Europy, Studia Humanistyczno-Społeczne» 2023, t. 9, nr 2, DOI: 10.17951/we.2023.9.2.11-28.