

Akademia Bialska im. Jana Pawła II

SYSTEM ZARZĄDZANIA KRYZYSOWEGO W TEORII I PRAKTYCE BEZPIECZEŃSTWA



Marta Chodyka
Zbigniew Ciekanski
Sławomir Żurawski

Biała Podlaska 2025



System zarządzania kryzysowego w teorii i praktyce bezpieczeństwa

Marta Chodyka
Zbigniew Ciekankowski
Sławomir Żurawski

Biała Podlaska 2025

Wydawca

Akademia Bialska im. Jana Pawła II

Recenzja

prof. dr hab. inż. dr h.c. Jarosław Wołejczo

płk prof. dr hab. inż. Leszek Elak

© Copyright by Akademia Bialska im. Jana Pawła II



Książka jest udostępniana na licencji Creative Commons Uznanie autorstwa –
Użycie niekomercyjne – Bez utworów zależnych 4.0 Międzynarodowa

ISBN 978-83-68103-32-8

<https://doi.org/10.29316/9788368103328>

Nakład: 50 egzemplarzy



Wydawnictwo AB JP II

ul. Sidorska 95/97

21-500 Biała Podlaska

wydawnictwo.akademiabialska.pl

Projekt okładki, skład i druk

druk-24h.com.pl
DRUKARNIA CYFROWA

Hurtowa 21, 15-399 Białystok

tel. 535 500 898

e-mail: studio@druk-24h.com.pl

Spis treści

Wykaz skrótów	5
Wprowadzenie	11
Rozdział I. System bezpieczeństwa narodowego	15
1.1. Koncepcja i architektura systemu bezpieczeństwa narodowego	15
1.2. Podsystem kierowania w systemie bezpieczeństwa narodowego	22
1.3. Operacyjne podsystemy wykonawcze.	34
1.4. Podsystemy wykonawcze o charakterze wsparcia	45
1.5. Bezpieczeństwo wewnętrzne i zewnętrzne	56
Rozdział II. Istota i uwarunkowania zarządzania kryzysowego.	65
2.1. Koncepcja i zakres zarządzania kryzysowego.	65
2.2. Zarządzanie kryzysowe w systemie nauk o bezpieczeństwie	85
2.3. Geneza i ewolucja zarządzania kryzysowego w Polsce i na świecie.	102
2.4. Podstawy prawne i instytucjonalne zarządzania kryzysowego	126
2.5. Kluczowe zasady i funkcje zarządzania kryzysowego	142
Rozdział III. Fazy i procesy zarządzania kryzysowego	147
3.1. Identyfikacja i ocena zagrożeń	147
3.2. Planowanie i przygotowanie do sytuacji kryzysowych	158
3.3. Reagowanie i zarządzanie w czasie kryzysu	175
3.4. Odbudowa i odtwarzanie po kryzysie	185
3.5. Doskonalenie systemu i zarządzanie wiedzą po zdarzeniu	199
Rozdział IV. Instrumenty i narzędzia zarządzania kryzysowego	207
4.1. Systemy informatyczne i bazy danych w zarządzaniu kryzysowym	207
4.2. Centra zarządzania kryzysowego i systemy ostrzegania ludności	215
4.3. Wykorzystanie technologii GIS, dronów i analityki danych	230
4.4. Planowanie zasobów i logistyka w sytuacjach kryzysowych	246
4.5. Komunikacja i informacja w zarządzaniu kryzysowym	253

Rozdział V. Zarządzanie kryzysowe w wymiarze lokalnym, krajowym i międzynarodowym	263
5.1. Zarządzanie kryzysowe w jednostkach samorządu terytorialnego	263
5.2. Zarządzanie kryzysowe na poziomie wojewódzkim i krajowym.	275
5.3. Zarządzanie kryzysowe w Unii Europejskiej i NATO	291
5.4. Współpraca transgraniczna i regionalna w reagowaniu kryzysowym	304
5.5. Przykłady dobrych praktyk i doświadczenia z wybranych państw	313
Rozdział VI. Wyzwania, trendy i kierunki rozwoju zarządzania kryzysowego	329
6.1. Nowe typy zagrożeń: cyber, hybrydowe i środowiskowe.	329
6.2. Zarządzanie ryzykiem i odporność społeczna.	341
6.3. Innowacje technologiczne w zarządzaniu kryzysowym.	353
6.4. Edukacja, szkolenia i kultura bezpieczeństwa.	362
6.5. Kierunki doskonalenia systemu zarządzania kryzysowego w Polsce	377
Podsumowanie	387
Literatura	391
Spis rysunków	410
Spis tabel	412

Wykaz skrótów

AAR	After Action Review (analiza działań po kryzysie)
ABW	Agencja Bezpieczeństwa Wewnętrznego
AI	Artificial Intelligence (sztuczna inteligencja)
ALFA	pierwszy (najniższy) stopień alarmowy
AON	Akademia Obrony Narodowej
APT	Advanced Persistent Threat (zaawansowane trwałe zagrożenie cybernetyczne)
ARIA	system ARIA (baza danych awarii przemysłowych we Francji)
ASF	afrykański pomór świń
BALEX	ćwiczenie BALEX DELTA (międzynarodowe manewry reagowania na wyciek ropy na Morzu Bałtyckim)
BBB	Build Back Better (zasada „odbudowy lepszej niż przed katastrofą”)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Niemiecki Federalny Urząd Ochrony Ludności i Pomocy w Katastrofach)
BCP	Business Continuity Plan (plan ciągłości działania)
BGK	Bank Gospodarstwa Krajowego
BRAVO	drugi stopień alarmowy
CAP	Common Alerting Protocol (standard formatu komunikatów alarmowych)
CBOS	Centrum Badania Opinii Społecznej
CBRN	Chemical, Biological, Radiological, Nuclear (zagrożenia chemiczne, biologiczne, radiologiczne i nuklearne)
CECIS	Common Emergency Communication and Information System (wspólny system łączności i informacji ratunkowej UE)
CEPC	Civil Emergency Planning Committee (Komitet Planowania Cywilnego NATO)
CERC	Crisis and Emergency Risk Communication (model komunikacji kryzysowej)
CERT	Computer Emergency Response Team (zespół reagowania na incydenty komputerowe)

CMX	Crisis Management Exercise (doroczne ćwiczenie zarządzania kryzysowego NATO)
COBRA	Cabinet Office Briefing Room A (brytyjski rządowy zespół kryzysowy „COBRA”)
COVID-19	Coronavirus Disease 2019 (choroba wywoływana przez koronawirus SARS-CoV-2)
CRED	Centre for Research on the Epidemiology of Disasters (Centrum Badań nad Epidemiologią Katastrof)
CRP	stopnie alarmowe CRP (dotyczące cyberprzestrzeni Rzeczypospolitej Polskiej)
CSIRT	Computer Security Incident Response Team (zespół reagowania na incydenty bezpieczeństwa komputerowego)
CZK	Centrum Zarządzania Kryzysowego
DGSCGC	Direction Générale de la Sécurité Civile et de la Gestion des Crises (Francuska Dyrekcja Generalna ds. Bezpieczeństwa Cywilnego i Zarządzania Kryzysowego)
DHS	Department of Homeland Security (Departament Bezpieczeństwa Krajowego USA)
DMR	Digital Mobile Radio (cyfrowy standard łączności radiowej)
DPS	Dom Pomocy Społecznej
DRR	Disaster Risk Reduction (redukcja ryzyka katastrof)
EADRCC	Euro-Atlantic Disaster Response Coordination Centre (Euroatlantyckie Centrum Koordynacji Reagowania na Katastrofy, NATO)
ECHO	European Civil Protection and Humanitarian Aid Operations (Dyrekcja Generalna ds. Pomocy Humanitarnej i Ochrony Ludności, KE)
ECMWF	European Centre for Medium-Range Weather Forecasts (Europejskie Centrum Prognoz Średnioterminowych)
ECURIE	European Community Urgent Radiological Information Exchange (system wczesnego powiadamiania o awariach jądrowych w Europie)
EDB	Edukacja dla Bezpieczeństwa (przedmiot szkolny)
EDXL	Emergency Data Exchange Language (standard wymiany danych w sytuacjach awaryjnych)
EFAS	European Flood Awareness System (Europejski System Ostrzegania Przeciwpowodziowego)
EFFIS	European Forest Fire Information System (Europejski System Informacji o Pożarach Lasów)
EM-DAT	Emergency Events Database (globalna baza danych o katastrofach)
EMIS	Emergency Management Information System (informatyczny system zarządzania kryzysowego)
EMS	Emergency Management Service (Copernicus EMS – program satelitarnego monitoringu sytuacji kryzysowych)

EPCRA	Emergency Planning and Community Right-to-Know Act (amerykańska ustawa o planowaniu awaryjnym i prawie do informacji, 1986)
EPRS	European Parliamentary Research Service (Analizy Parlamentu Europejskiego)
ERCC	Emergency Response Coordination Centre (Centrum Koordynacji Reagowania Kryzysowego UE)
FSUE	Fundusz Solidarności Unii Europejskiej
GCZK	Gminne Centrum Zarządzania Kryzysowego
GIS	Geographic Information System (system informacji geograficznej)
GLOBSEC	GLOBSEC (międzynarodowy think-tank i forum bezpieczeństwa w Bratysławie)
GOPR	Górskie Ochotnicze Pogotowie Ratunkowe
GPS	Global Positioning System (Globalny System Pozycjonowania)
GSM	Global System for Mobile Communications (standard telefonii komórkowej)
GZZK	Gminny Zespół Zarządzania Kryzysowego
HELCOM	Helsinki Commission (Komisja Helsińska ds. ochrony środowiska morskiego Bałtyku)
HFA	Hyogo Framework for Action (Ramowy Plan Działań z Hyogo 2005-2015)
HHS	Department of Health and Human Services (Departament Zdrowia i Opieki Społecznej USA)
HUSAR	Heavy Urban Search And Rescue (ciężka grupa poszukiwawczo-ratownicza)
HZS	Hasičský záchranný sbor (Czeska Straż Pożarna)
IAEM	International Association of Emergency Managers (Międzynarodowe Stowarzyszenie Menedżerów Kryzysowych)
ICS	Incident Command System (system dowodzenia incydem)
ICT	Information and Communication Technologies (technologie informacyjno-komunikacyjne)
IDNDR	International Decade for Natural Disaster Reduction (Międzynarodowa Dekada Ograniczania Skutków Klęsk Żywiolowych 1990-1999)
IDS	Intrusion Detection System (system detekcji włamań)
IMGW	Instytut Meteorologii i Gospodarki Wodnej
INPO	Institute of Nuclear Power Operations (Instytut Bezpiecznej Eksploatacji Elektrowni Jądrowych, USA)
INSARAG	International Search and Rescue Advisory Group (Międzynarodowa Grupa Doradcza ds. Poszukiwania i Ratownictwa, ONZ)
IPCC	Intergovernmental Panel on Climate Change (Międzyrządowy Zespół ds. Zmian Klimatu)
IPCR	Integrated Political Crisis Response (zintegrowany mechanizm politycznego reagowania kryzysowego UE)

ISOK	Informatyczny System Osłony Kraju (system map zagrożeń)
ISP	Internet Service Provider (dostawca usług internetowych)
IT	Information Technology (technologia informatyczna)
JRC	Joint Research Centre (Wspólne Centrum Badawcze UE)
JST	jednostka samorządu terytorialnego
KATWARN	KATWARN (niemiecki system ostrzegania ludności – aplikacja mobilna)
KPRM	Kancelaria Prezesa Rady Ministrów
KPZK	Krajowy Plan Zarządzania Kryzysowego
KSRG	Krajowy System Ratowniczo-Gaśniczy
LET	Logistics Emergency Team (międzynarodowa inicjatywa zespołów logistycznych sektora prywatnego)
LPR	Lotnicze Pogotowie Ratunkowe
MAEA	Międzynarodowa Agencja Energii Atomowej (International Atomic Energy Agency, IAEA)
MAHB	Major Accident Hazards Bureau (Biuro ds. Zagrożeń Poważnymi Awariami, JRC)
MIC	Monitoring and Information Centre (Centrum Monitorowania i Informacji, poprzednik ERCC)
MODEX	Modular Exercise (ćwiczenia modułów ratunkowych w ramach UCPM)
MOLDEX	EU MOLDEX (międzynarodowe ćwiczenie modułów ratowniczych w Mołdawii)
MON	Ministerstwo Obrony Narodowej
MSB	Myndigheten för samhällsskydd och beredskap (Szwedzka Agencja ds. Ochrony Ludności)
MSF	Médecins Sans Frontières (Lekarze bez Granic)
MZ	Ministerstwo Zdrowia
NASK	Naukowa i Akademicka Sieć Komputerowa
NATO	Organizacja Traktatu Północnoatlantyckiego (NATO)
NGO	Non-Governmental Organization (organizacja pozarządowa)
NIK	Najwyższa Izba Kontroli
NIMS	National Incident Management System (Narodowy System Zarządzania Incydentami, USA)
NINA	Notfall-Informationen- und Nachrichten-App (niemiecka aplikacja alarmowa NINA)
NLP	Natural Language Processing (przetwarzanie języka naturalnego)
NRC	Nuclear Regulatory Commission (Komisja Dozoru Jądrowego USA)
OASIS	Organization for the Advancement of Structured Information Standards (organizacja standaryzacyjna IT)
OC	Obrona Cywilna

ONZ	Organizacja Narodów Zjednoczonych (United Nations, UN)
ORSEC	Plan ORSEC (francuski plan ratownictwa i ochrony ludności)
OSART	Operational Safety Review Team (misja inspekcyjna MAEA ds. bezpieczeństwa elektrowni)
OSP	Ochotnicza Straż Pożarna
PAA	Państwowa Agencja Atomistyki
PCK	Polski Czerwony Krzyż
PCPM	Polskie Centrum Pomocy Międzynarodowej
PCZK	Powiatowe Centrum Zarządzania Kryzysowego
PIG-PIB	Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
PKB	Produkt Krajowy Brutto
PRL	Polska Rzeczpospolita Ludowa
PRM	Państwowe Ratownictwo Medyczne
PSP	Państwowa Straż Pożarna
PTSD	Post-Traumatic Stress Disorder (zespół stresu pourazowego)
PZH	Państwowy Zakład Higieny (Narodowy Instytut Zdrowia Publicznego)
PZZK	Powiatowy Zespół Zarządzania Kryzysowego
RACI	Responsible, Accountable, Consulted, Informed (macierz odpowiedzialności RACI)
RASFF	Rapid Alert System for Food and Feed (unijny system szybkiego powiadamiania o niebezpiecznej żywności i paszach)
RCB	Rządowe Centrum Bezpieczeństwa
RM	Rada Ministrów
RP	Rzeczpospolita Polska
RSO	Regionalny System Ostrzegania
RZZK	Rządowy Zespół Zarządzania Kryzysowego
SAMU	Service d'Aide Médicale Urgente (francuski system pogotowia ratunkowego)
SAR	Search and Rescue (poszukiwanie i ratownictwo)
SAREX	Search and Rescue Exercise (ćwiczenia poszukiwawczo-ratownicze)
SARS	Severe Acute Respiratory Syndrome (zespół ostrej ciężkiej niewydolności oddechowej)
SBN	System Bezpieczeństwa Narodowego
SGSP	Szkoła Główna Służby Pożarniczej
SISMS	Samorządowy Informator SMS (system powiadamiania mieszkańców)
SMS	Short Message Service (usługa wiadomości SMS)
SNA	Social Network Analysis (analiza sieci społecznych)

SOR	Szpitalny Oddział Ratunkowy
SWD	System Wspomagania Dowodzenia
THW	Technisches Hilfswerk (Niemiecki Federalny Urząd ds. Pomocy Technicznej)
TMI	Three Mile Island (awaria elektrowni jądrowej Three Mile Island, 1979)
UAV	Unmanned Aerial Vehicle (bezzałogowy statek powietrzny, dron)
UCPM	Union Civil Protection Mechanism (Unijny Mechanizm Ochrony Ludności)
UE	Unia Europejska (European Union)
UK	United Kingdom (Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej)
UKF	ultrakrótkie fale (pasmo UKF w radiokomunikacji)
UNDRR	United Nations Office for Disaster Risk Reduction (Biuro ONZ ds. Redukcji Ryzyka Katastrof)
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs (Biuro ONZ ds. Koordynacji Pomocy Humanitarnej)
USA	Stany Zjednoczone Ameryki (United States of America)
USAR	UrbanSearchAndRescue(miejskagrupapozukiwawczo-ratownicza)
VMS	Variable Message Sign (elektroniczna tablica informacyjna na drodze)
WCZK	Wojewódzkie Centrum Zarządzania Kryzysowego
WEA	Wireless Emergency Alerts (amerykański system alarmowania ludności przez telefony komórkowe)
WFP	World Food Programme (Światowy Program Żywnościowy ONZ)
WHO	World Health Organization (Światowa Organizacja Zdrowia)
WMS	Web Map Service (usługa udostępniania map w Internecie)
WOPR	Wodne Ochotnicze Pogotowie Ratunkowe
WOT	Wojska Obrony Terytorialnej
WPZK	Wojewódzki Plan Zarządzania Kryzysowego
WZZK	Wojewódzki Zespół Zarządzania Kryzysowego
XML	Extensible Markup Language (uniwersalny język znaczników XML)
ZZK	Zespół Zarządzania Kryzysowego

Wprowadzenie

Współczesne państwa i społeczności lokalne funkcjonują w realiach narastającej złożoności i niepewności. Zmiany klimatyczne, gwałtowny rozwój technologii, rosnąca zależność od złożonych systemów infrastruktury krytycznej, a także napięcia geopolityczne sprawiają, że sytuacje o charakterze kryzysowym przestają być zjawiskiem wyjątkowym, stając się trwałym elementem krajobrazu bezpieczeństwa. Zarządzanie kryzysowe – jeszcze niedawno postrzegane głównie jako domena służb ratowniczych – staje się dziś jednym z kluczowych obszarów nauk o bezpieczeństwie oraz praktyki działania administracji publicznej i innych podmiotów odpowiedzialnych za ochronę ludności.

Czytelniku, oddajemy w Twoje ręce monografię poświęconą systemowi zarządzania kryzysowego w teorii i praktyce bezpieczeństwa. Jej zasadniczym celem jest całościowe ukazanie zarządzania kryzysowego jako integralnego elementu systemu bezpieczeństwa narodowego, a zarazem jako rozwijającej się subdyscypliny nauk o bezpieczeństwie, posiadającej własny aparat pojęciowy, ugruntowane podstawy teoretyczne i rosnące znaczenie aplikacyjne. Autorzy dążą do połączenia perspektywy teoretycznej (definicje, modele, paradygmaty) z doświadczeniami praktyki – rozwiązaniami instytucjonalnymi, instrumentami działania i studium polskiego systemu zarządzania kryzysowego na tle rozwiązań międzynarodowych. Monografia adresowana jest do kilku grup odbiorców. Po pierwsze – do środowiska naukowego nauk o bezpieczeństwie, dla którego może stanowić uporządkowaną syntezę dorobku teoretycznego zarządzania kryzysowego oraz punkt wyjścia do dalszych badań nad jego miejscem w systemie bezpieczeństwa państwa. Po drugie – do studentów kierunków związanych z bezpieczeństwem, administracją publiczną i zarządzaniem, którym opracowanie ma ułatwić zrozumienie logiki działań w sytuacjach kryzysowych oraz powiązań

między różnymi podsystemami bezpieczeństwa. Po trzecie wreszcie – do praktyków: pracowników administracji rządowej i samorządowej, funkcjonariuszy służb, inspekcji i straży, oficerów sił zbrojnych, a także operatorów infrastruktury krytycznej, dla których może być narzędziem refleksji nad funkcjonowaniem systemu, jego mocnymi stronami i obszarami wymagającymi doskonalenia.

Struktura opracowania została podporządkowana logice przechodzenia od ujęcia systemowego bezpieczeństwa narodowego i osadzenia zarządzania kryzysowego w architekturze państwa, przez podstawy pojęciowe, prawne i instytucjonalne oraz opis procesów i narzędzi, aż po identyfikację wyzwań i kierunków rozwoju w perspektywie przyszłości. Rozdział I przedstawia system bezpieczeństwa narodowego Rzeczypospolitej Polskiej jako ramę odniesienia dla działań podejmowanych w sytuacjach nadzwyczajnych. Omówiono w nim istotę i strukturę systemu bezpieczeństwa narodowego RP oraz miejsce, jakie zajmuje w nim zarządzanie kryzysowe. Zarysowano powiązania zarządzania kryzysowego z bezpieczeństwem wewnętrznym i zewnętrznym, podkreślając, że współczesne zagrożenia często mają charakter przekrojowy i wymagają skoordynowanej reakcji wielu podmiotów. Istotną część rozdziału stanowi analiza roli administracji publicznej w organizacji i koordynacji działań kryzysowych – od poziomu lokalnego po centralny – a także omówienie zadań Sił Zbrojnych RP oraz służb, inspekcji i straży w systemie reagowania. Całość dopełnia problematyka koordynacji działań międzysektorowych i współpracy międzyinstytucjonalnej, warunkujących sprawność funkcjonowania państwa w obliczu zdarzeń przekraczających kompetencje pojedynczych instytucji. Rozdział II koncentruje się na istocie i uwarunkowaniach zarządzania kryzysowego. W pierwszej kolejności uporządkowano aparat pojęciowy i przedstawiono zarządzanie kryzysowe jako kategorię teoretyczną i praktyczną, wskazując jego miejsce w systemie nauk o bezpieczeństwie. Następnie zaprezentowano genezę i ewolucję zarządzania kryzysowego – zarówno w Polsce, jak i w ujęciu międzynarodowym – co pozwala uchwycić kierunki zmian w podejściu do ryzyka, prewencji i reagowania. Szczególną uwagę poświęcono podstawom prawnym i instytucjonalnym polskiego systemu, a także kluczowym zasadom i funkcjom zarządzania kryzysowego. W tej części omówiono m.in. znaczenie zasad organizacyjnych i kompetencyjnych (w tym subsydiarności, jednoosobowego

kierownictwa czy powszechności) oraz klasyczny model działań oparty na cyklu czterech faz: zapobieganie, przygotowanie, reagowanie i odbudowa – jako spójnej logice planowania oraz oceny efektywności systemu. Rozdział III poświęcono fazom i procesom zarządzania kryzysowego, ujmowanym jako ciąg wzajemnie powiązanych działań – od identyfikacji i oceny zagrożeń, przez planowanie i przygotowanie, po reagowanie, odbudowę oraz doskonalenie systemu. Przedstawiono metody rozpoznawania i szacowania ryzyka, zasady konstruowania planów zarządzania kryzysowego na różnych poziomach administracji oraz organizację działań operacyjnych w trakcie kryzysu. Podkreślono również wagę działań pokryzysowych: analiz wniosków, zarządzania wiedzą i mechanizmów ciągłego uczenia się systemu. Rozdział IV omawia instrumenty i narzędzia wykorzystywane w zarządzaniu kryzysowym. Zaprezentowano rolę systemów informatycznych i baz danych, funkcjonowanie centrów zarządzania kryzysowego oraz systemów ostrzegania i alarmowania ludności. Przedmiotem analizy jest również wykorzystanie nowoczesnych technologii – takich jak GIS, drony oraz analityka danych – w rozpoznaniu sytuacji, wspieraniu decyzji i koordynacji działań. Uzupełnieniem rozdziału są zagadnienia planowania zasobów i logistyki oraz komunikacji i informacji – zarówno w wymiarze wewnętrznym (w strukturach reagowania), jak i zewnętrznym (w relacjach z obywatelami i mediami). Rozdział V przenosi rozważania na poziom lokalny, krajowy i międzynarodowy, ukazując wieloszczeblowy charakter systemu. Przedstawiono specyfikę zarządzania kryzysowego w jednostkach samorządu terytorialnego, a następnie na poziomie wojewódzkim i krajowym, z uwzględnieniem podziału kompetencji i mechanizmów koordynacyjnych. W dalszej części omówiono wymiar ponadpaństwowy – Unię Europejską i NATO – w tym ramy współpracy, instrumenty wsparcia oraz mechanizmy reagowania kryzysowego. Rozdział uzupełniają zagadnienia współpracy transgranicznej i regionalnej oraz dobre praktyki zaczerpnięte z doświadczeń wybranych państw, które mogą stanowić punkt odniesienia dla rozwoju rozwiązań krajowych. Rozdział VI ma charakter prospektywny i syntetyzuje wyzwania, trendy oraz kierunki rozwoju zarządzania kryzysowego. Zidentyfikowano nowe typy zagrożeń – w szczególności cybernetyczne, hybrydowe i środowiskowe – oraz wskazano rosnące znaczenie podejścia opartego na zarządzaniu ryzykiem i budowaniu odporności społecznej. Omówiono wpływ

innowacji technologicznych na praktykę działania instytucji odpowiedzialnych za bezpieczeństwo, a także znaczenie edukacji, szkoleń i kształtowania kultury bezpieczeństwa. Rozdział zamykają propozycje kierunków doskonalenia polskiego systemu zarządzania kryzysowego, formułowane w oparciu o wcześniejsze rozważania teoretyczne oraz wnioski wynikające z praktyki funkcjonowania instytucji publicznych.

Monografia łączy podejście systemowe i interdyscyplinarne: korzysta z dorobku nauk o bezpieczeństwie, zarządzania, prawa, socjologii, nauk technicznych i studiów strategicznych. Zastosowana metoda badawcza obejmuje analizę literatury przedmiotu, dokumentów normatywnych i strategicznych, wybrane studia przypadku oraz syntezę doświadczeń funkcjonowania polskiego systemu zarządzania kryzysowego w ostatnich dekadach. Dzięki temu opracowanie stara się nie tylko opisać stan obecny, lecz także wskazać logiczne kierunki zmian – od wzmocnienia podstaw prawnych i organizacyjnych, przez rozwój narzędzi informacyjnych i kompetencji kadr, po budowanie odporności społecznej na kryzysy.

Mamy nadzieję, że lektura monografii pozwoli Ci – jako badaczowi, studentowi lub praktykowi – spojrzeć na zarządzanie kryzysowe jako na spójny, wielopoziomowy system, w którym spotykają się teoria i praktyka, struktury państwa i zaangażowanie społeczeństwa, rozwiązania krajowe i standardy międzynarodowe. Jeśli monografia stanie się inspiracją do dalszych badań, dyskusji oraz konkretnych działań na rzecz podnoszenia bezpieczeństwa i odporności Rzeczypospolitej Polskiej, cel, jaki przyświecał autorom, zostanie w pełni osiągnięty.

Miłej lektury
Autorzy

Rozdział I.

System bezpieczeństwa narodowego

1.1. Koncepcja i architektura systemu bezpieczeństwa narodowego

Punktem wyjścia do analizy systemu bezpieczeństwa narodowego jest samo rozumienie bezpieczeństwa jako kategorii wielowymiarowej i dynamicznej. W naukach o bezpieczeństwie podkreśla się, że bezpieczeństwo nie jest wyłącznie „stanem braku zagrożenia”, lecz obejmuje także zdolność podmiotu do utrzymania ciągłości istnienia, przetrwania oraz rozwoju, a więc ma charakter procesualny i zależy od warunków zewnętrznych oraz wewnętrznych¹. W konsekwencji współczesne ujęcia bezpieczeństwa narodowego odchodzą od wąskiego, militarnego paradygmatu, akcentując poszerzenie repertuaru zagrożeń o wymiary polityczne, ekonomiczne, społeczne, informacyjne czy środowiskowe, co wymusza podejście całościowe w planowaniu oraz organizowaniu działań państwa na rzecz bezpieczeństwa^{2,3}. Rozumienie bezpieczeństwa narodowego jako zadania przekrojowego prowadzi do przyjęcia perspektywy systemowej. W ujęciu ogólnym system oznacza celowo wyodrębniony zbiór elementów (podmiotów, zasobów,

¹ R. Rosicki, O pojęciu i istocie bezpieczeństwa, *Przegląd Politologiczny*, (3), 2010, s. 24-32. <https://doi.org/10.14746/pp.2010.15.3.2>

² D. Brązkiewicz, M. Chodyka, T. Grudniewski, J. Nowicka, (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część pierwsza*, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103199>

³ D. Brązkiewicz, M. Chodyka, T. Grudniewski, S. Żurawski, *Wielowymiarowość środowiska bezpieczeństwa. Część druga*, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103205>

narzędzi) oraz relacji i sprzężeń między nimi, które wspólnie umożliwiają realizację określonej funkcji. Zastosowanie tej optyki w badaniach nad bezpieczeństwem pozwala uchwycić nie tylko katalog instytucji, lecz także mechanizmy współdziałania i zależności między komponentami bezpieczeństwa państwa, w tym relacje z otoczeniem⁴. W praktyce oznacza to, że bezpieczeństwo narodowe nie jest sumą odrębnych „resortowych” działań, ale wynikiem skoordynowanego wykorzystania różnorodnych instrumentów państwa i społeczeństwa. W tym sensie przyjęta w niniejszym rozdziale koncepcja systemu bezpieczeństwa narodowego opiera się na rozumieniu go jako układu współzależnych elementów, których skuteczność zależy od jakości powiązań, procedur i zdolności koordynacyjnych. Architektura systemu oznacza natomiast sposób uporządkowania podsystemów, relacji między nimi oraz mechanizmów przepływu decyzji, informacji i zasobów. Ujęcie architektoniczne pozwala wskazać, gdzie powstaje spójność działania państwa, a gdzie pojawiają się potencjalne „wąskie gardła” integracji.

W polskiej debacie strategicznej system bezpieczeństwa narodowego (SBN) jest ujmowany jako kategoria obejmująca całość sił, środków i zasobów przeznaczonych do realizacji zadań w dziedzinie bezpieczeństwa, zorganizowanych w podsystemy, utrzymywanych i przygotowywanych stosownie do tych zadań. Takie rozumienie, przyjęte w dokumentach państwowych, akcentuje zarówno element „potencjałowy” (zasoby), jak i „organizacyjny” (struktura i procedury), a zarazem wskazuje na potrzebę integracji komponentów bezpieczeństwa w spójny mechanizm działania. Syntetyczną definicję SBN przedstawia Biała Księga Bezpieczeństwa Narodowego, wskazując, że system obejmuje podsystem kierowania oraz podsystemy wykonawcze, w tym operacyjne (obronny i ochronne) oraz wsparcia (społeczne i gospodarcze)⁵. Warto podkreślić, że definicja ta nie sprowadza bezpieczeństwa wyłącznie do domeny militarnej, lecz zakłada istnienie wielu komplementarnych obszarów działania państwa, których integracja tworzy dopiero „system” w sensie funkcjonalnym. Analogiczny sposób konceptualizacji utrwala Strategia Bezpieczeństwa Narodowego z 2014 r., która *explicite* stwierdza,

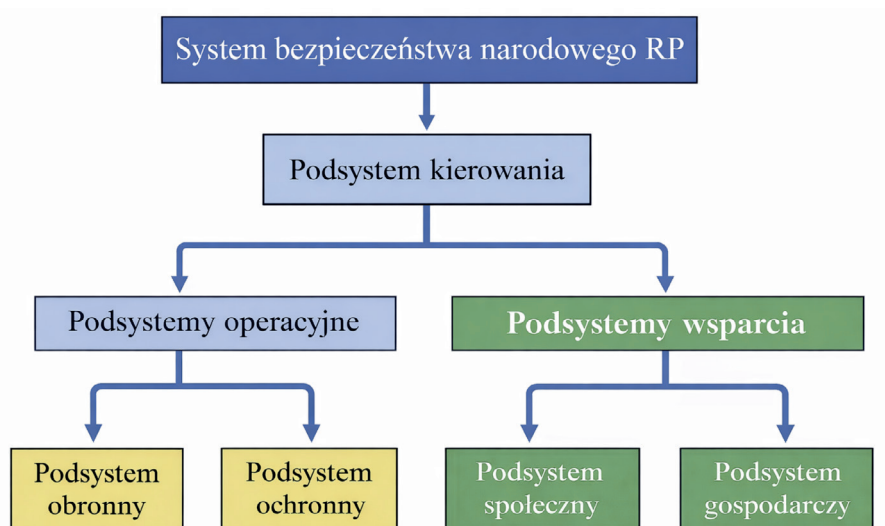
⁴ H. Spustek, A. Paluch, *Struktura systemu bezpieczeństwa narodowego Polski*, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

⁵ Biuro Bezpieczeństwa Narodowego, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, BBN, 2013.

że system obejmuje siły, środki i zasoby przeznaczone do realizacji zadań bezpieczeństwa, odpowiednio zorganizowane, utrzymywane i przygotowane, a zarazem składa się z podsystemu kierowania oraz podsystemów wykonawczych⁶. Jednocześnie należy zaznaczyć, że Strategia z 2020 r. formalnie zastąpiła dokument z 2014 r., co pokazuje, iż system (jako kategoria praktyczna) podlega cyklicznej reinterpretacji w zależności od uwarunkowań bezpieczeństwa⁷. W kontekście strukturalnym istotne jest odwołanie do rysunku 1, w którym układ SBN przedstawiono jako zależność między podsystemem kierowania a podsystemami wykonawczymi (operacyjnymi i wsparcia). Schemat porządkuje architekturę SBN w ujęciu strukturalnym, pokazując nadrzędność podsystemu kierowania oraz dwie zasadnicze warstwy wykonawcze: operacyjną i wsparcia. W takim ujęciu architektura systemu nie jest wyłącznie opisem elementów, lecz sposobem ich sprzęgnięcia tak, aby decyzje strategiczne mogły być skutecznie przekładane na działania wykonawcze. W tym miejscu kluczowe jest jednak nie samo nazwanie elementów, lecz przyjęcie założenia, że nadrzędną funkcją systemu jest zapewnienie spójności celów, decyzji i alokacji zasobów w różnych sektorach bezpieczeństwa.

⁶ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2014.

⁷ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.



Rysunek 1. Struktura systemu bezpieczeństwa narodowego RP – podsystem kierowania oraz podsystemy wykonawcze (operacyjne i wsparcia)

Źródło: opracowanie własne.

Normatywne podstawy SBN wynikają przede wszystkim z Konstytucji RP, która wyznacza wartości podlegające ochronie, a tym samym „ramuje” rozumienie bezpieczeństwa narodowego jako obowiązku państwa. Szczególne znaczenie ma art. 5 Konstytucji, który wiąże bezpieczeństwo z ochroną niepodległości i integralności terytorialnej, praw i wolności obywatelskich, dziedzictwa narodowego oraz środowiska, wprowadzając jednocześnie zasadę zrównoważonego rozwoju jako dyrektywę działania państwa⁸. Takie ujęcie konstytucyjne wzmacnia tezę, że bezpieczeństwo narodowe ma charakter kompleksowy, obejmując nie tylko obronę i porządek publiczny, lecz także fundamenty rozwoju społeczno-gospodarczego i odporności państwa. Wymiar ustrojowy ma także art. 7 Konstytucji, wprowadzający zasadę legalizmu (działanie organów władzy publicznej na podstawie i w granicach prawa). Z perspektywy SBN oznacza to, że system bezpieczeństwa nie może być rozumiany jedynie jako praktyka administracyjna, lecz musi być osadzony w kompetencjach, odpowiedzialnościach i procedurach przypisanych

⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

przez prawo, co stanowi warunek przewidywalności, rozliczalności i ciągłości działania państwa w sytuacjach stabilnych oraz nadzwyczajnych.

Na poziomie ustawowym istotnym elementem „szkieletu” SBN jest regulacja zarządzania kryzysowego. Ustawa o zarządzaniu kryzysowym w art. 2 definiuje zarządzanie kryzysowe jako działalność organów administracji publicznej będącą elementem kierowania bezpieczeństwem narodowym, obejmującą zapobieganie sytuacjom kryzysowym, przygotowanie, reagowanie, usuwanie skutków oraz odtwarzanie zasobów i infrastruktury krytycznej⁹. Definicja ustawowa ma znaczenie systemowe: lokuje zarządzanie kryzysowe nie jako wyodrębnioną politykę sektorową, lecz jako funkcjonalny składnik kierowania bezpieczeństwem narodowym, a tym samym jako narzędzie integrujące działania w wielu domenach. Współczesne podstawy prawne SBN obejmują także akty regulujące obronność oraz ochronę ludności, które rozwijają instytucjonalne i zasobowe filary odporności państwa. Do tej grupy należą m.in. rozwiązania ustawowe w obszarze obrony (w tym kodyfikacje i modernizacje przepisów dotyczących systemu obronnego państwa) oraz odrębna regulacja ochrony ludności i obrony cywilnej, która wzmacnia część cywilną systemu w odpowiedzi na współczesne ryzyka (w szczególności wynikające z konfliktów zbrojnych oraz zagrożeń pozamilitarnych)¹⁰. W ramach niniejszego ujęcia koncepcyjno-architektonicznego kluczowe jest jednak uchwycenie tendencji: ustawodawca wzmacnia systemowe podejście do bezpieczeństwa, rozbudowując instrumentarium cywilne równoległe do instrumentarium obronnego.

Oprócz norm prawnych fundamentalną rolę w kształtowaniu SBN odgrywają dokumenty doktrynalne i strategiczne, które porządkują cele państwa oraz wskazują architekturę i priorytety modernizacji systemu. Biała Księga Bezpieczeństwa Narodowego stanowi w tym zakresie dokument szczególny, ponieważ łączy funkcję diagnozy z funkcją konceptualizacji: przedstawia założenia transformacji systemu, akcentując integrację oraz budowanie synergii między podsystemem kierowania, podsystemami operacyjnymi i podsystemami wsparcia, a także wskazuje na potrzebę racjonalizacji

⁹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590).

¹⁰ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r., poz. 1907).

kompetencji i wydatków w bezpieczeństwie¹¹. W logice tego dokumentu SBN ma być przygotowany do działania w różnych stanach funkcjonowania państwa, co wzmacnia postulat ciągłości działania i gotowości instytucjonalnej jako elementów „systemowości” bezpieczeństwa.

Strategia Bezpieczeństwa Narodowego z 2014 r. rozwija tę perspektywę, ujmując bezpieczeństwo narodowe jako obszar wymagający optymalnego wykorzystania wszystkich zasobów państwa w sferze obronnej, ochronnej, społecznej i gospodarczej, a jako kluczowe wskazując ich właściwą integrację w systemie bezpieczeństwa narodowego¹². W narracji strategicznej integracja nie jest więc hasłem organizacyjnym, lecz warunkiem zdolności państwa do reagowania na złożone zagrożenia, których trajektoria często przekracza granice sektorów administracji. W Strategii z 2020 r. akcent przesuwają się wyraźnie w stronę „zarządzania bezpieczeństwem narodowym” jako mechanizmu integrującego, obejmującego m.in. scalanie dotychczas funkcjonujących systemów, w szczególności kierowania bezpieczeństwem narodowym, zarządzania kryzysowego oraz cyberbezpieczeństwem, a także budowanie zdolności adaptacyjnych państwa¹³. Jednocześnie dokument ten jednoznacznie wskazuje, że z dniem zatwierdzenia Strategii w 2020 r. utraciła moc Strategia z 2014 r., co nie tylko porządkuje hierarchię dokumentów, ale też unaocznia cykliczność „odnawiania” podstaw doktrynalnych SBN wraz ze zmianą uwarunkowań strategicznych.

Definicja SBN ma konsekwencje metodologiczne: wyznacza granice tego, co w analizie bezpieczeństwa należy uznać za element systemu, a co za element otoczenia. Jeżeli przyjmuje się, że system jest celowo określonym zbiorem obiektów i sprzężeń, to każda część bezpieczeństwa narodowego jest istotna o tyle, o ile da się ją opisać jako zasób, kompetencję, procedurę lub narzędzie pozostające w relacji z innymi elementami systemu i współdziałające w realizacji funkcji bezpieczeństwa¹⁴. Z tej perspektywy SBN jest

¹¹ Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.

¹² Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2014.

¹³ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

¹⁴ H. Spustek, A. Paluch, Struktura systemu bezpieczeństwa narodowego Polski, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

nie tyle „zbiorem służb”, ile mechanizmem uzgadniania celów, mobilizowania zasobów i koordynowania reakcji państwa.

W literaturze podkreśla się, że wielopłaszczyznowość misji i zadań państwa w obszarze bezpieczeństwa wymaga istnienia uporządkowanego, kolektywnego zbioru elementów zdolnego do skoordynowanego działania, przy czym podstawowym warunkiem takiej koordynacji są kompetencje organów administracji publicznej wynikające z prawa¹⁵. W konsekwencji „system bezpieczeństwa narodowego” należy rozumieć jako konstrukcję jednocześnie funkcjonalną (ukierunkowaną na realizację misji bezpieczeństwa), organizacyjną (wyrażoną w relacjach między elementami) i normatywną (opartą na przydziale odpowiedzialności i uprawnień). Takie ujęcie legitymizuje potrzebę rozróżnienia w dalszych rozdziałach między poziomem kierowania (koordynacja, decyzje strategiczne, procedury) a poziomem wykonawczym (instrumenty operacyjne i wsparciowe), bez redukcji SBN do jednej domeny.

Warto także odnotować konsekwencję systemową wynikającą z ustawy o zarządzaniu kryzysowym: skoro zarządzanie kryzysowe jest elementem kierowania bezpieczeństwem narodowym¹⁶, to musi być analizowane jako narzędzie integrujące sektorowe zdolności reagowania, pozostające w relacji zarówno do komponentów cywilnych, jak i do komponentów obronnych. Zbieżne podejście prezentują opracowania dotyczące kierowania bezpieczeństwem narodowym, które wskazują, że kierowanie obejmuje także działania administracji publicznej wobec katastrof czy awarii technicznych oraz koordynację sił i środków reagowania kryzysowego¹⁷. Na poziomie definicyjnym oznacza to, iż SBN zawiera w sobie mechanizmy działania w stanach rutynowych i nadzwyczajnych oraz obejmuje komponenty zdolne do przechodzenia między tymi stanami, co jest jednym z wyznaczników dojrzałej „systemowości” bezpieczeństwa. Z perspektywy konstrukcji monografii rozdział koncepcyjno-architektoniczny powinien zatem zostać domknięty trzema tezami. Po pierwsze, SBN jest kategorią nadrzędną wobec systemów

¹⁵ W. Kitler, System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne, *Wiedza Obronna*, 268(3), 2019, s. 5-33.

¹⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590).

¹⁷ W. Molek, K. Stec, R. Marciniak, Zarządzanie kryzysowe w systemie kierowania bezpieczeństwem narodowym, *Bezpieczeństwo Narodowe*, (17), 2011, s. 46-60.

sektorowych: łączy je poprzez podsystem kierowania oraz zestaw podsystemów wykonawczych. Po drugie, podstawy SBN są podwójne: konstytucyjno-ustawowe (legitymizacja, kompetencje, procedury) oraz doktrynalno-strategiczne (cele, priorytety, kierunki transformacji), co razem wyznacza „architekturę” bezpieczeństwa państwa. Po trzecie, współczesne rozumienie SBN zakłada integrację narzędzi militarnych i cywilnych oraz zdolność adaptacji do zagrożeń hybrydowych i wielodomenowych, co wprost wynika z kierunków wskazanych w Strategii z 2020 r.

1.2. Podsystem kierowania w systemie bezpieczeństwa narodowego

Podsystem kierowania jest nadrzędnym komponentem systemu bezpieczeństwa narodowego, ponieważ skupia uprawnienia do ustanawiania celów, podejmowania decyzji, koordynowania działań oraz egzekwowania odpowiedzialności w całym układzie bezpieczeństwa państwa¹⁸. Jego istotą nie jest „wykonywanie” zadań bezpieczeństwa, lecz tworzenie warunków organizacyjno-prawnych i informacyjnych, w których podsystemy wykonawcze mogą działać spójnie, adekwatnie do zagrożeń oraz zgodnie z konstytucyjnymi zasadami ustrojowymi i ograniczeniami władzy publicznej^{19,20}. W praktyce podsystem kierowania obejmuje konstytucyjne organy państwa, zwłaszcza Prezydenta i Radę Ministrów, wraz z parlamentarnymi mechanizmami kontroli oraz zapleczem doradczym i sztabowym, w tym Radą Bezpieczeństwa Narodowego i Biurem Bezpieczeństwa Narodowego, a po stronie rządowej również wyspecjalizowane mechanizmy koordynacyjne oraz centra zarządzania kryzysowego, które zapewniają przepływ informacji i gotowość do działania w trybach kryzysowych^{21,22}. Wymiar współczesny

¹⁸ H. Spustek, A. Paluch, Struktura systemu bezpieczeństwa narodowego Polski, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

¹⁹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

²⁰ Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.

²¹ Biuro Bezpieczeństwa Narodowego, Biuro Bezpieczeństwa Narodowego 2015-2025, Warszawa, BBN, 2025.

²² Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

podsystemu kierowania obejmuje narastającą konieczność integracji międzysektorowej, w tym włączenia cyberbezpieczeństwa i przeciwdziałania zagrożeniom hybrydowym do głównego nurtu zarządzania bezpieczeństwem, przy jednoczesnym utrzymaniu przejrzystości kompetencyjnej, rozliczalności i interoperacyjności struktur^{23,24}.

Podsystem kierowania, w ujęciu przyjmowanym w literaturze systemowej dotyczącej bezpieczeństwa, stanowi część systemu bezpieczeństwa narodowego przeznaczoną do kierowania jego funkcjonowaniem; obejmuje organy władzy publicznej i kierowników jednostek realizujących zadania bezpieczeństwa, wraz z organami doradczymi, aparatem administracyjno-sztabowym, procedurami oraz infrastrukturą kierowania i łączności²⁵. W perspektywie funkcjonalnej kierowanie bezpieczeństwem narodowym polega na podejmowaniu decyzji przez uprawnione organy w taki sposób, aby utrzymywać pożądany poziom bezpieczeństwa w różnych dziedzinach, przy zachowaniu zdolności do działania zarówno w warunkach pokoju, jak i kryzysu, stanów nadzwyczajnych oraz wojny.

Podsystem kierowania pełni rolę nadrzędną wobec podsystemów wykonawczych. Wyznacza cele strategiczne, uruchamia i koordynuje zasoby, zapewnia priorytetyzację działań, a także ustanawia kryteria oceny skuteczności oraz mechanizmy korekty w oparciu o informację zwrotną. Ten nadrzędny charakter nie oznacza zastępowania podsystemów wykonawczych, lecz nadawanie im wspólnego kierunku i zapewnianie, aby działania w domenie obronnej, ochronnej i wsparcia były wzajemnie komplementarne oraz zgodne z prawem i polityką państwa. Funkcje podsystemu kierowania można analitycznie opisać jako wiązkę powiązanych procesów. Po pierwsze, funkcja normatywno-strategiczna obejmuje diagnozę zagrożeń, definiowanie interesów i celów, przyjmowanie strategii oraz inicjowanie zmian prawnych i organizacyjnych, które tworzą ramy dla działań państwa²⁶. Po drugie, funkcja decyzyjno-koordynacyjna realizuje się poprzez uruchamianie procedur,

²³ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia hybrydowe (synteza wyników kontroli), Warszawa, NIK, 2023.

²⁴ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

²⁵ H. Spustek, A. Paluch, Struktura systemu bezpieczeństwa narodowego Polski, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

²⁶ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

uzgadnianie działań w układzie międzyresortowym i wieloszczeblowym, a w razie potrzeby przechodzenie na tryby nadzwyczajne, w których ciężar decyzyjny i zasady podległości są zmodyfikowane w sposób przewidziany prawem^{27,28,29}. Po trzecie, funkcja informacyjno-analityczna obejmuje zapewnianie ciągłego monitorowania zagrożeń, gromadzenia danych, przetwarzania informacji i wsparcia decydentów analizą, w tym poprzez centra zarządzania kryzysowego i systemy łączności. Po czwarte, funkcja kontrolna i rozliczalnościowa polega na osadzeniu kierowania w mechanizmach odpowiedzialności konstytucyjnej i politycznej, w tym w relacjach między władzą wykonawczą a ustawodawczą oraz w zewnętrznej kontroli instytucjonalnej³⁰.

Konstytucyjna architektura kierowania bezpieczeństwem w Polsce opiera się na modelu, w którym kluczowe kompetencje w zakresie bezpieczeństwa i obronności są rozdzielone między główne organy państwa, a ich współdziałanie ma charakter ustrojowego „współrzędzenia” w sprawach bezpieczeństwa. Fundamentem roli głowy państwa jest norma konstytucyjna stanowiąca, że Prezydent Rzeczypospolitej Polskiej czuwa nad przestrzeganiem Konstytucji, stoi na straży suwerenności i bezpieczeństwa państwa oraz jest gwarantem ciągłości władzy państwowej³¹. W obszarze ściśle obronnym Prezydent jest najwyższym zwierzchnikiem Siły Zbrojne Rzeczypospolitej Polskiej, sprawuje zwierzchnictwo w czasie pokoju pośrednio, a w czasie wojny ma kompetencje do mianowania Naczelnego Dowódcy, przy czym szczegółowe zasady powiązania dowodzenia z konstytucyjnymi organami państwa określają ustawy³². Relację Prezydenta z rządem w sferze bezpieczeństwa wzmacnia instrument Rady Gabinetowej jako forum obrad

²⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

²⁸ Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. poz. 1301).

²⁹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

³⁰ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia hybrydowe (synteza wyników kontroli), Warszawa, NIK, 2023.

³¹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 126, ust. 1-2).

³² Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 134, ust. 1-2, ust. 4 oraz ust. 6).

rządu pod przewodnictwem Prezydenta w sprawach szczególnej wagi, przy jednoczesnym zachowaniu zasady, że Rada Gabinetowa nie przejmuje kompetencji Rady Ministrów³³. Centralną rolę w bieżącym kierowaniu aparatem państwa ponosi Rada Ministrów, która prowadzi politykę wewnętrzną i zagraniczną, kieruje administracją rządową i zapewnia bezpieczeństwo wewnętrzne oraz zewnętrzne państwa, a także koordynuje i kontroluje pracę organów administracji rządowej³⁴. Z perspektywy mechaniki podsystemu kierowania istotne jest, że Konstytucja przypisuje Prezesowi Rady Ministrów kompetencje koordynacyjne i nadzorcze wobec członków rządu oraz funkcję zwierzchnika służbowego administracji rządowej, co w praktyce przesądza o roli premiera jako głównego węzła koordynacji międzyresortowej w sprawach bezpieczeństwa³⁵. Jednocześnie system konstytucyjny zachowuje mechanizmy kontroli i odpowiedzialności, w tym przez zasadę kontrasygnaty aktów urzędowych Prezydenta, która wiąże skuteczność większości aktów z podpisem premiera, a tym samym z odpowiedzialnością rządu przed parlamentem³⁶. Z perspektywy władzy ustawodawczej fundamentalne znaczenie ma udział Sejm Rzeczypospolitej Polskiej w kontroli decyzji nadzwyczajnych władzy wykonawczej, w szczególności weryfikacja rozporządzeń o wprowadzeniu stanu wojennego i stanu wyjątkowego, przedstawianych Sejmowi w krótkim terminie, z możliwością uchylenia przez parlament, co stanowi istotny bezpiecznik przeciwko arbitralności władzy wykonawczej³⁷. Dodatkowo konstytucyjne ograniczenia dotyczące zmian prawa wyborczego i zasad ustrojowych w czasie stanów nadzwyczajnych wzmacniają stabilność instytucjonalną, co w podsystemie kierowania jest warunkiem zachowania ciągłości rządu w sytuacjach krytycznych³⁸. Udział Senatu Rzeczypospolitej Polskiej w systemie kierowania ujawnia się

³³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 141, ust. 1-2).

³⁴ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 146, ust. 1, ust. 3 oraz ust. 4 pkt 3, 7 i 8).

³⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 148, pkt 2, 5 i 7).

³⁶ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 144, ust. 2; z zastrzeżeniem wyjątków z art. 144 ust. 3).

³⁷ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 231, w zw. z art. 229 oraz art. 230 ust. 1-2).

³⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228, ust. 6-7).

nie tyle poprzez kompetencje operacyjne, ile poprzez jego miejsce w architekturze ustawodawczej oraz wskazania strategiczne zawarte w dokumentach państwowych dotyczących przygotowań organów parlamentu do zarządzania bezpieczeństwem³⁹.

Instytucjonalnym zapleczem Prezydenta w obszarze bezpieczeństwa jest Rada Bezpieczeństwa Narodowego jako organ doradczy w zakresie bezpieczeństwa wewnętrznego i zewnętrznego, ustanowiony konstytucyjnie⁴⁰. W praktyce funkcjonowanie Rady jest wspierane przez Biuro Bezpieczeństwa Narodowego, które zapewnia obsługę merytoryczną i organizacyjną Rady, a jego status prawny wynika z regulacji ustawowej przewidującej, że Prezydent wykonuje zadania w zakresie bezpieczeństwa i obronności przy pomocy BBN oraz że organizację i zakres działania BBN określa, na podstawie upoważnienia ustawowego, sam Prezydent⁴¹. Ten model, oparty na ustawowym umocowaniu i aktach wewnętrznych Prezydenta, wzmacnia elastyczność organizacyjną zaplecza prezydenckiego, ale jednocześnie oznacza, że szczegółowe rozwiązania instytucjonalne mogą podlegać zmianom w ramach prerogatyw organizacyjnych głowy państwa, co wymaga szczególnej dbałości o ciągłość procedur i pamięć instytucjonalną⁴².

Po stronie rządowej istotnym elementem zaplecza kierowniczego jest Rządowe Centrum Bezpieczeństwa oraz system zarządzania kryzysowego jako element kierowania bezpieczeństwem narodowym, co wynika wprost z ustawowej definicji zarządzania kryzysowego jako działalności organów administracji publicznej ukierunkowanej na zapobieganie sytuacjom kryzysowym, przygotowanie, reagowanie, usuwanie skutków oraz odtwarzanie zasobów i infrastruktury krytycznej⁴³. Ustawodawca wiąże z tym reżimem zarówno obowiązki planistyczne, jak i organizacyjne, co włącza zarządzanie kryzysowe w rdzeń podsystemu kierowania, zwłaszcza poprzez wymóg

³⁹ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁴⁰ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 135).

⁴¹ Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655).

⁴² Biuro Bezpieczeństwa Narodowego, Biuro Bezpieczeństwa Narodowego 2015-2025, Warszawa, BBN, 2025.

⁴³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

istnienia planów na szczeblu krajowym i terytorialnym oraz przez instytucjonalizację zespołów i centrów wspierających decydentów.

W wymiarze organizacyjnym podsystem kierowania łączy dwa kluczowe porządki: porządek ustrojowy (wynikający z Konstytucji i ustaw kompetencyjnych) oraz porządek funkcjonalny (wynikający z potrzeb koordynacji zagrożeń wielodomenowych, wieloszczeblowych i często transgranicznych). Literatura systemowa podkreśla, że na najwyższym poziomie kierowania usytuowane są Prezydent i Rada Ministrów wraz z organami doradczymi i aparatem sztabowym oraz z organami dowodzenia sił zbrojnych; te elementy tworzą instytucjonalny „szczyt” kierowania w czasie pokoju, kryzysu i wojny⁴⁴. W tym sensie podsystem kierowania obejmuje zarówno kierowanie polityczno-strategiczne, jak i kierowanie operacyjne w znaczeniu uruchamiania mechanizmów wykonawczych przez właściwe węzły systemu⁴⁵.

Mechanizmy koordynacji międzyresortowej w obszarze bezpieczeństwa opierają się na formalnych ciałach pomocniczych oraz na procedurach uzgadniania stanowisk. Przykładowo, na poziomie rządowym funkcjonuje komitet właściwy do spraw bezpieczeństwa, obrony i cyberprzestrzeni jako organ pomocniczy Rady Ministrów i premiera, wyposażony w zadania koordynacji wykonywania zadań bezpieczeństwa, analiz, opiniowania projektów dokumentów i aktów prawnych oraz przygotowywania rekomendacji strategicznych, przy czym jego rozstrzygnięcia mają charakter uzgodnień, a w razie braku konsensu decyduje stanowisko przewodniczącego, z zachowaniem możliwości zgłaszania zdań odrębnych⁴⁶. Z punktu widzenia podsystemu kierowania istotne jest również formalne powiązanie tego mechanizmu z rządowym procesem decyzyjnym, w tym z trybem prac Rady Ministrów, co pozwala traktować go jako narzędzie „przedsionka” uzgodnień dla decyzji gabinetowych w obszarze bezpieczeństwa. W obszarze kryzysowym ustawodawca przewiduje wyraźne mechanizmy koordynacji, w tym istnienie rządowego zespołu zarządzania kryzysowego jako organu

⁴⁴ H. Spustek, A. Paluch, *Struktura systemu bezpieczeństwa narodowego Polski*. Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

⁴⁵ W. Molek, K. Stec, R. Marciniak, *Zarządzanie kryzysowe w systemie kierowania bezpieczeństwem narodowym*. *Bezpieczeństwo Narodowe*, 17, 2011, s. 45-60.

⁴⁶ Zarządzenie nr 53 Prezesa Rady Ministrów z dnia 16 maja 2024 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego (M.P. 2024 poz. 372).

opiniodawczo-doradczego właściwego w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. W tym reżimie Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium państwa, a w przypadkach niecierpiących zwłoki kompetencję tę wykonuje minister właściwy do spraw wewnętrznych, z obowiązkiem rozliczenia działań na najbliższym posiedzeniu rządu, co wprowadza mechanizm zarówno sprawności decyzyjnej, jak i ex post kolegialnej kontroli gabinetowej⁴⁷. Dodatkowo prawo przewiduje możliwość wydawania poleceń obowiązujących w sytuacji kryzysowej, co stanowi narzędzie władcze wzmacniające zdolność przejęcia kontroli nad rozproszonymi zasobami administracji i infrastruktury, przy jednoczesnym określeniu granic tych poleceń. Koordynacja w podsystemie kierowania ma również wymiar terytorialny, ponieważ skuteczność reagowania i odporność państwa zależą od spójności działań na poziomie centralnym, regionalnym i lokalnym. Ustawa o zarządzaniu kryzysowym przypisuje kompetencje organom właściwym na kolejnych szczeblach: wojewodzie na poziomie województwa, staroście w powiecie oraz wójtowi, burmistrzowi lub prezydentowi miasta w gminie, określając zarazem, że zadania tych organów obejmują kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń oraz organizację planowania cywilnego właściwą dla poziomu kompetencji. Istotnym elementem jest instytucjonalizacja zespołów i centrów zarządzania kryzysowego na poziomie wojewódzkim i gminnym, co zapewnia całodobowy obieg informacji, dokumentowanie działań, nadzór nad systemami ostrzegania i alarmowania oraz współdziałanie z innymi centrami w administracji publicznej. Ten wieloszczeblowy charakter podsystemu kierowania współgra z ujęciem literaturowym, które identyfikuje cztery zasadnicze poziomy zarządzania: centralny, wojewódzki, powiatowy i gminny, a ich spójność uznaje za warunek sterowalności systemu bezpieczeństwa jako całości.

Analiza podsystemu kierowania wymaga rozróżnienia trybów decyzyjnych w „stanie normalnym” oraz w warunkach nadzwyczajnych, przy czym granice między nimi nie są wyłącznie faktem politycznym, lecz są konstrukcją prawną sprzężoną z katalogiem stanów nadzwyczajnych oraz

⁴⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

z odrębnymi reżimami planistyczno-operacyjnymi. Konstytucja ustanawia katalog stanów nadzwyczajnych, dopuszczając ich wprowadzenie, gdy zwykłe środki konstytucyjne są niewystarczające⁴⁸, a jednocześnie określa podstawę prawną i formę ich wprowadzenia⁴⁹, ogólne ramy ograniczeń i zasad działania organów władzy publicznej w tych stanach⁵⁰ oraz konstytucyjne granice dopuszczalnych ograniczeń praw i wolności w poszczególnych stanach nadzwyczajnych⁵¹, a także mechanizmy kontroli parlamentarnej⁵². W przypadku stanu wojennego Prezydent może go wprowadzić na wniosek Rady Ministrów w razie zewnętrznego zagrożenia lub napaści⁵³, natomiast w przypadku stanu wyjątkowego analogiczny mechanizm opiera się na wniosku rządu w sytuacji zagrożenia ustroju, bezpieczeństwa obywateli lub porządku publicznego⁵⁴. Rozporządzenia Prezydenta w tych sprawach są przedstawiane Sejmowi, który może je uchylić, co strukturalnie wpisuje władzę ustawodawczą w kluczowy węzeł kontroli podsystemu kierowania w trybach nadzwyczajnych⁵⁵. W przypadku stanu klęski żywiołowej konstytucyjnie umocowana jest kompetencja Rady Ministrów do wprowadzenia tego stanu na czas oznaczony, z możliwością przedłużenia za zgodą parlamentu, co potwierdza model, w którym zarządzanie katastrofami i awariami noszącymi znamiona klęski jest w istocie elementem kierowania wykonywanego przez rząd w ramach administracji publicznej⁵⁶.

Ustawy „okołostanowe” rozwijają konstytucyjny szkielet w kierunku proceduralnej wykonalności. W reżimie stanu wyjątkowego ustawodawca

⁴⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228, ust. 1).

⁴⁹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228, ust. 2).

⁵⁰ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228, ust. 3 i ust. 5).

⁵¹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 233 ust. 1-3).

⁵² Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 231, art. 230 ust. 2, art. 232).

⁵³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 231, art. 229).

⁵⁴ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 230, ust. 1).

⁵⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 231).

⁵⁶ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 232).

precyzuje, że to Rada Ministrów podejmuje uchwałę o skierowaniu wniosku do Prezydenta, a następnie Prezydent rozpatruje wniosek i wydaje rozporządzenie, które przedstawia Sejmowi w 48 godzin, przy czym ustawodawca rozdziela też zadania koordynacyjne między premiera i wojewodę w zależności od zasięgu terytorialnego stanu wyjątkowego⁵⁷. W reżimie stanu klęski żywiołowej ustawodawca ustanawia jednoznaczną zasadę „jednolitego kierownictwa” działań oraz hierarchicznego podporządkowania w układzie wójt-starosta-wojewoda-minister (w zależności od zasięgu terytorialnego), wzmacniając sterowalność działań w warunkach koniecznego współdziałania wielu organów i służb⁵⁸. Model decyzyjny w czasie wojny i stanu wojennego jest szczególnie istotny dla oceny podsystemu kierowania, ponieważ ujawnia konstytucyjny mechanizm współdziałania Prezydenta i Rady Ministrów w kierowaniu obroną państwa. Ustawa o stanie wojennym wskazuje, że w czasie tego stanu obroną państwa kieruje Prezydent we współdziałaniu z Radą Ministrów, a w ramach kompetencji Prezydenta mieszczą się decyzje dotyczące przejścia organów na stanowiska kierowania, stanów gotowości bojowej, zadań sił zbrojnych oraz ewentualnego mianowania Naczelnego Dowódcy, natomiast rząd uruchamia system kierowania obroną państwa i może, w określonych warunkach, modyfikować zasady działania administracji w strefie bezpośrednich działań wojennych⁵⁹. Na poziomie konstytucyjnym dopełnieniem jest kompetencja Prezydenta do mianowania Naczelnego Dowódcy na czas wojny, co tworzy łącznik między kierowaniem politycznym a dowodzeniem wojskowym⁶⁰.

Instrumentarium planowania i przygotowania w podsystemie kierowania ma charakter wielowarstwowy. W warstwie strategicznej kluczowym dokumentem jest Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, która nakreśla także postulaty dotyczące integracji zarządzania bezpieczeństwem narodowym, w tym scalania dotychczasowych systemów kierowania bezpieczeństwem, zarządzania kryzysowego i cyberbezpieczeństwa,

⁵⁷ Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. poz. 985).

⁵⁸ Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. poz. 558).

⁵⁹ Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. poz. 1301).

⁶⁰ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

oraz tworzenia ponadresortowych mechanizmów koordynacji strategicznej powiązanych z modernizacją roli struktur kryzysowych⁶¹. W tym samym dokumencie przewidziano przygotowanie aktu prawnego dotyczącego zarządzania bezpieczeństwem narodowym; w tym zakresie, na poziomie deklaracji strategicznej, kierunek jest jednoznaczny, natomiast szczegółowy status realizacji tej zapowiedzi jako obowiązującej regulacji jest w niniejszym opracowaniu nieokreślony, ponieważ nie wynika bezpośrednio z przywołanych tu źródeł normatywnych. Warstwa planowania kryzysowego jest w Polsce silnie zinstytucjonalizowana. Ustawa o zarządzaniu kryzysowym oblige do tworzenia krajowego oraz wojewódzkich, powiatowych i gminnych planów, które obejmują m.in. charakterystykę zagrożeń i ocenę ryzyka, rozpisanie zadań i odpowiedzialności w postaci siatki bezpieczeństwa, zestawienie sił i środków oraz procedury reagowania i współdziałania⁶². Jednocześnie ustawa wiąże planowanie z cyklem aktualizacji oraz z wymaganiami dotyczącymi systemów ostrzegania, alarmowania, łączności i informowania ludności, co wzmacnia element „ciągłego sterowania” w podsystemie kierowania, zamiast traktowania planów jako statycznej dokumentacji. Uzupełnieniem jest obowiązek sporządzania raportu o zagrożeniach bezpieczeństwa narodowego, koordynowanego na poziomie centralnym i przyjmowanego przez Radę Ministrów, co tworzy formalne ogniwo łączące diagnozę ryzyka z decyzją strategiczną o priorytetach i przedsięwzięciach.

Rosnące znaczenie ciągłości działania i odporności instytucjonalnej powoduje, że podsystem kierowania musi obejmować także mechanizmy zapewniania ciągłości świadczenia kluczowych usług publicznych i ciągłości funkcjonowania administracji w warunkach zakłóceń. W polskich regulacjach kryzysowych wyraźnie obecny jest wątek ciągłości działania poprzez powiązanie zarządzania kryzysowego z odtwarzaniem zasobów i infrastruktury krytycznej oraz przez wymagania dotyczące funkcjonowania centrów zarządzania kryzysowego i stałych dyżurów. Dodatkowym narzędziem w obszarze infrastruktury krytycznej są dokumenty programowe koordynowane na poziomie rządowym, w tym Narodowy Program Ochrony Infrastruktury

⁶¹ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁶² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

Krytycznej, który porządkuje standardy i wymagania dotyczące odporności oraz odtwarzania kluczowych systemów państwa⁶³. Warto zauważyć, że w praktyce rośnie też znaczenie instrumentów audytowych i metodycznych odnoszących się do planów ciągłości świadczenia usług publicznych, adresowanych do sektora publicznego, co wspiera rozliczalność i uczenie się instytucji na poziomie procesów⁶⁴.

Współczesne środowisko bezpieczeństwa kształtuje podsystem kierowania w warunkach „zacierania się granic” między pokojem, kryzysem i wojną oraz narastania zagrożeń hybrydowych, informacyjnych i cybernetycznych, które wymagają koordynacji zarówno resortowej, jak i międzysektorowej. Strategia z 2020 r. wprost postuluje integrację systemu zarządzania bezpieczeństwem narodowym poprzez scalenie dotychczas funkcjonujących systemów, w tym zarządzania kryzysowego i cyberbezpieczeństwa, a także budowę narzędzi umożliwiających płynne przechodzenie od stanu pokoju do kryzysu i wojny⁶⁵. W ujęciu analitycznym oznacza to dążenie do redukcji silosowości decyzyjnej i wzmocnienia wspólnej świadomości sytuacyjnej, co w literaturze bywa wskazywane jako podstawowy warunek sprawnego zawiadywania bezpieczeństwem w układzie wielodomenowym⁶⁶.

Wyzwanie hybrydowe ujawnia się organom kierowania nie tylko jako kwestia rozpoznania i reagowania, lecz jako problem projektowania instytucjonalnej odporności. Kontrole i analizy wskazują na ryzyko braku kompleksowych mechanizmów budowania odporności państwa na skutki działań hybrydowych w ramach systemów zarządzania kryzysowego i obrony cywilnej, co wprost dotyka „sterowalności” systemu w warunkach presji rozproszonej, często poniżej progu klasycznych stanów nadzwyczajnych⁶⁷. W tym kontekście nośny staje się postulat rozwijania jednolitych procedur współdziałania, standardów łączności i interoperacyjności struktur, ponieważ

⁶³ Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity, Warszawa, RCB, 2023.

⁶⁴ OECD, Wsparcie realizacji audytu planów ciągłości świadczenia usług publicznych w Polsce (wytyczne/metodyka audytu), 2024.

⁶⁵ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁶⁶ W. Kitler, System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne, *Wiadza Obronna*, 268(3), 2019, s. 5-33.

⁶⁷ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia hybrydowe (synteza wyników kontroli), Warszawa, NIK, 2023.

bez takich standardów podsystem kierowania może zachowywać formalne kompetencje, ale tracić zdolność do efektywnego kierowania w sensie operacyjnym^{68,69}. Wyzwanie cyberbezpieczeństwa ma charakter przekrojowy, ponieważ dotyka równocześnie infrastruktury krytycznej, operacji wojskowych, porządku publicznego, gospodarki i sfery informacyjnej. Ustawowe ramy cyberbezpieczeństwa wyodrębniają system podmiotów właściwych w tej domenie, jednak z perspektywy podsystemu kierowania kluczowa jest zdolność włączenia procedur cyber w główny obieg decyzyjno-koordynacyjny państwa, a nie utrzymywania cyberbezpieczeństwa wyłącznie jako wyspecjalizowanej „wyspy” organizacyjnej⁷⁰. W praktyce temu celowi służą zarówno postulaty strategiczne dotyczące scalania systemów, jak i rozwijanie rządowych mechanizmów koordynacji, które obejmują bezpieczeństwo cyberprzestrzeni jako jeden z obszarów wprost przypisanych do zadań komitetu rządowego⁷¹.

Wreszcie, problemem stale obecnym w dyskursie o kierowaniu bezpieczeństwem jest relacja między odpowiedzialnością a sprawnością. Z jednej strony podsystem kierowania wymaga szybkiej decyzyjności, zwłaszcza w warunkach kryzysu, z drugiej strony musi zachować mechanizmy kontroli i rozliczalności. Konstytucyjne wymogi przedstawiania rozporządzeń o wprowadzeniu stanu wojennego i wyjątkowego parlamentowi oraz możliwość ich uchylecia, podobnie jak wymóg kontrasygnaty wielu aktów Prezydenta, są tu klasycznymi przykładami „hamulców” zapewniających rozliczalność władzy wykonawczej⁷². W obszarze kryzysowym równoważenie sprawności i odpowiedzialności widać w konstrukcji, w której decyzje podejmowane w trybie pilnym przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na posiedzeniu rządu, co wzmacnia kolegialny charakter odpowiedzialności politycznej. Z perspektywy doskonalenia podsystemu kierowania oznacza to, że modernizacja powinna koncentrować

⁶⁸ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁶⁹ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia hybrydowe (synteza wyników kontroli), Warszawa, NIK, 2023.

⁷⁰ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

⁷¹ Zarządzenie nr 53 Prezesa Rady Ministrów z dnia 16 maja 2024 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego (M.P. 2024 poz. 372).

⁷² Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. poz. 985).

się na poprawie interoperacyjności, łączności, wspólnych procedur i jakości analiz, a nie na obchodzeniu mechanizmów kontroli, które stanowią część konstytucyjnej legitymizacji kierowania bezpieczeństwem.

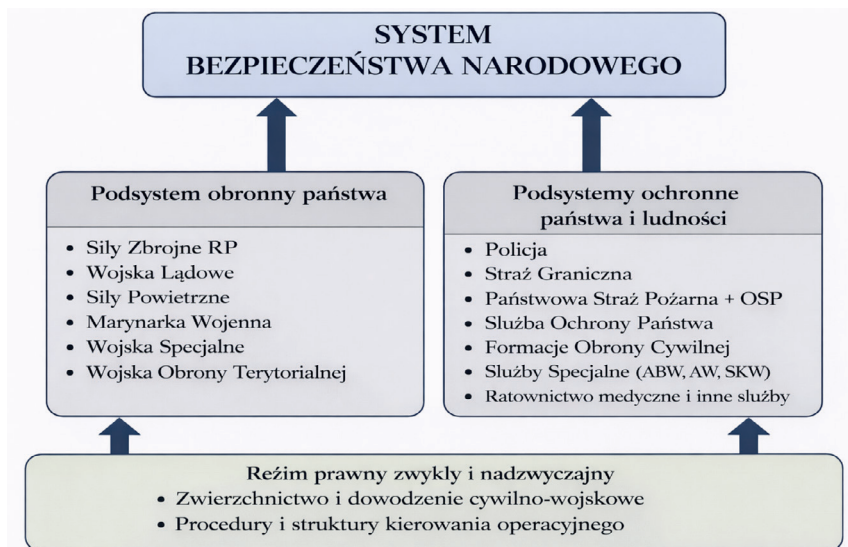
1.3. Operacyjne podsystemy wykonawcze

Operacyjne podsystemy wykonawcze stanowią „rdzeń sprawczy” systemu bezpieczeństwa narodowego: są zbiorem instytucji i zdolności, które realizują zadania obronne i ochronne w praktyce, w czasie pokoju, kryzysu oraz wojny. W ujęciu przyjętym w polskich dokumentach strategicznych i opracowaniach systemowych obejmują one przede wszystkim podsystem obronny państwa oraz podsystemy ochronne państwa i ludności, pozostające w dyspozycji organów kierowania bezpieczeństwem narodowym. Logika operacyjnych podsystemów wykonawczych opiera się na rozdziale między poziomem strategiczno-politycznym (kierowanie) a poziomem realizacyjnym (wykonywanie). W praktyce oznacza to, że instytucje operacyjne są uruchamiane i ukierunkowywane decyzjami organów kierowania, ale wykonują działania w ściśle określonych reżimach prawnych (zwykłych i nadzwyczajnych) oraz w ramach wyspecjalizowanych procedur, struktur dowodzenia i łączności. Współczesne środowisko bezpieczeństwa wzmacnia znaczenie interoperacyjności i koordynacji cywilno-wojskowej. Zagrożenia hybrydowe i cybernetyczne przesuwają część aktywności „operacyjnej” poza klasyczny obszar użycia siły zbrojnej i porządku publicznego, a jednocześnie wymagają spójności planowania cywilnego i obronnego, ochrony infrastruktury krytycznej oraz zdolności do ciągłości działania państwa. Te kierunki zostały wyraźnie zaakcentowane w Strategii Bezpieczeństwa Narodowego RP 2020, która kładzie nacisk na budowę odporności, integrację przygotowań i rozwój systemowych narzędzi reagowania również na zagrożenia o charakterze hybrydowym⁷³.

W klasyfikacji przyjętej w polskich dokumentach państwowych operacyjne podsystemy wykonawcze są wyodrębnianą kategorią w ramach systemu bezpieczeństwa narodowego. Struktura operacyjnych podsystemów

⁷³ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

wykonawczych systemu bezpieczeństwa narodowego RP (podsystem obronny oraz podsystemy ochronne) w reżimie prawnym zwykłym i nadzwyczajnym zobrażowana została na rysunku 2.



Rysunek 2. Operacyjne podsystemy wykonawcze systemu bezpieczeństwa narodowego RP – komponent obronny i ochronny

Źródło: opracowanie własne.

Ich wspólną cechą jest bezpośrednia zdolność do przeciwdziałania zagrożeniom: albo w logice militarnej (obrona państwa), albo w logice ochronnej (bezpieczeństwo cywilne i pozamilitarne, w tym porządek publiczny, ochrona ludności, bezpieczeństwo wewnętrzne). W Białej Księdze Bezpieczeństwa Narodowego RP podsystemy wykonawcze zdefiniowano jako siły i środki przewidziane do realizacji ustawowo określonych zadań w dziedzinie bezpieczeństwa, pozostające w dyspozycji organów kierowania bezpieczeństwem; wyróżnia się wśród nich podsystemy operacyjne oraz podsystemy wsparcia, przy czym operacyjne tworzą podsystem obronny państwa oraz podsystemy ochronne państwa i ludności⁷⁴. Taki podział, choć modelowy, ma doniosłe konsekwencje organizacyjne. Po pierwsze, pozwala odróżnić sferę „oddziaływania na zagrożenie” (operacje obronne i ochronne) od sfery

⁷⁴ Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.

„utrzymania odporności i zasobów” (wsparcie społeczne i gospodarcze). Po drugie, porządkuje relacje kompetencyjne: operacyjne podsystemy wykonawcze działają w ramach odrębnych łańcuchów dowodzenia i nadzoru (wojskowych oraz cywilnych), ale muszą być zdolne do wspólnych działań w sytuacjach złożonych, gdy występuje jednocześnie komponent militarny, porządkowy, ratowniczy i informacyjny. W literaturze systemowej wskazuje się, że takie ujęcie sprzyja analizie sprzężeń i punktów styku między obszarami działań, zwłaszcza gdy zagrożenia mają charakter przekrojowy⁷⁵.

Należy podkreślić, że „operacyjność” podsystemów wykonawczych ujawnia się przede wszystkim w ich podporządkowaniu celom wyznaczanym na poziomie kierowania oraz w ich gotowości do uruchomienia sił i środków w trybie natychmiastowym, w warunkach presji czasu i deficytu informacji. W tym sensie operacyjne podsystemy wykonawcze są elementami systemu „działającego”, a nie wyłącznie „planistycznego”: łączą zdolności, procedury i zasoby, które muszą funkcjonować w sposób ciągły oraz podlegać stałemu doskonaleniu poprzez szkolenie, ćwiczenia i weryfikację procedur. Podsystem obronny jest tą częścią operacyjnych podsystemów wykonawczych, która odpowiada za przeciwdziałanie zagrożeniom polityczno-militarnym oraz realizację obrony państwa, w tym odstraszenie, obronę terytorium i wsparcie sojuszników. W ujęciu systemowym Biała Księga wskazuje go jako pierwszy komponent podsystemów operacyjnych, co odpowiada tradycyjnemu rozumieniu obronności jako zdolności państwa do zachowania suwerenności i integralności terytorialnej w warunkach zagrożenia militarnego.

W wymiarze normatywnym współczesnym punktem ciężkości regulacji podsystemu obronnego jest Ustawa o obronie Ojczyzny⁷⁶, która porządkuje strukturę sił zbrojnych, zasady pełnienia służby, organizację rezerw oraz część mechanizmów funkcjonowania państwa w obszarze obronności. Ustawa ta wskazuje katalog rodzajów Sił Zbrojnych, obejmujący m.in. Wojska Lądowe, Siły Powietrzne, Marynarkę Wojenną, Wojska Specjalne i Wojska Obrony Terytorialnej, co ma znaczenie z punktu widzenia planowania użycia sił oraz alokacji zdolności w scenariuszach kryzysowych i wojennych.

⁷⁵ H. Spustek, A. Paluch, *Struktura systemu bezpieczeństwa narodowego Polski*, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.

⁷⁶ Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655).

Istotą operacyjności podsystemu obronnego jest jego zdolność do działania w trzech reżimach czasu: pokoju, kryzysu i wojny. W czasie pokoju dominują zadania stałej gotowości, szkolenia, monitorowania zagrożeń, współpracy sojuszniczej oraz budowy zdolności odstraszania. W czasie kryzysu granicznego lub polityczno-militarnego rośnie waga działań podprogowych i działań osłonowych, w tym wzmacniania obecności, podnoszenia gotowości, wsparcia ochrony granic czy zabezpieczenia infrastruktury krytycznej. W czasie wojny podsystem obronny przechodzi do realizacji operacji obronnych i prowadzenia działań połączonych, przy jednoczesnej konieczności utrzymania powiązań z systemem kierowania oraz z cywilnymi systemami ochrony ludności. Kierunkowość tych przygotowań znajduje odzwierciedlenie w Strategii Bezpieczeństwa Narodowego 2020, która podkreśla potrzebę budowy systemu odporności państwa, zdolnego do płynnego przechodzenia od pokoju do kryzysu i wojny⁷⁷. Z perspektywy monografii o systemie bezpieczeństwa narodowego szczególnie ważny jest „most” między obroną a reagowaniem kryzysowym. Ustawa o zarządzaniu kryzysowym przewiduje możliwość użycia pododdziałów lub oddziałów Sił Zbrojnych do wykonywania zadań z zakresu zarządzania kryzysowego, gdy użycie innych sił i środków jest niemożliwe lub niewystarczające, a minister właściwy do spraw obrony może przekazać je do dyspozycji wojewody na wniosek wojewody. Jednocześnie ustawa wskazuje katalog typowych zadań, obejmujący m.in. monitoring zagrożeń, ewakuację ludności i mienia, prace zabezpieczające i ratownicze, usuwanie skażeń chemicznych i biologicznych, odtwarzanie infrastruktury technicznej czy działania sanitarno-epidemiczne⁷⁸.

Włączenie wojska do reagowania kryzysowego ma podwójny wymiar. Po pierwsze, jest sposobem zwiększenia masy i specjalistyczności zasobów, zwłaszcza w obszarach, gdzie siły cywilne nie dysponują analogicznymi kompetencjami lub sprzętem. Po drugie, jest mechanizmem budowania interoperacyjności cywilno-wojskowej, która w warunkach zagrożeń hybrydowych staje się warunkiem skuteczności państwa jako całości. Zasadą ograniczającą jest jednak wymóg, aby użycie oddziałów Sił Zbrojnych w sytuacji

⁷⁷ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁷⁸ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

kryzysowej nie zagrażało ich zdolności do realizacji konstytucyjnych zadań oraz zobowiązań wynikających z umów międzynarodowych.

Integralną częścią współczesnej operacyjności podsystemu obronnego jest także komponent cybernetyczny. Ustawa o obronie Ojczyzny ustanawia rozwiązania dotyczące dowodzenia jednostkami Wojsk Obrony Cyberprzestrzeni, co potwierdza instytucjonalizację cyberprzestrzeni jako obszaru działań obronnych i konieczność powiązania jej z klasycznym systemem dowodzenia⁷⁹. W tym miejscu ujawnia się kluczowa cecha systemowa: cyberzagrożenia są jednocześnie kwestią obronną i ochronną, ponieważ uderzają w państwo zarówno jako przeciwnik zewnętrzny, jak i jako zakłócenie usług krytycznych, co wymusza współdziałanie wojska z cywilnym systemem cyberbezpieczeństwa oraz z operatorami infrastruktury krytycznej⁸⁰. Wreszcie, warunkiem operacyjności podsystemu obronnego jest zdolność do rozwinięcia sił, uzupełniania strat oraz utrzymania wysiłku długotrwałego, co prowadzi do problematyki mobilizacji i rezerw. Ustawa o obronie Ojczyzny wprowadza rozróżnienie aktywnej i pasywnej rezerwy oraz opisuje mechanizmy pełnienia służby w rezerwie, wskazując ją jako narzędzie zapewniania uzupełnieniowych potrzeb Sił Zbrojnych. W kontekście współczesnej debaty o odporności państwa oznacza to, że rezerwy nie są wyłącznie zasobem „na czas wojny”, lecz elementem stałego modelu gotowości, powiązanim z planowaniem, szkoleniem i logistyką, a w praktyce także z gotowością do wsparcia sytuacji kryzysowych.

Podsystem ochronny obejmuje te komponenty operacyjnych podsystemów wykonawczych, które odpowiadają za bezpieczeństwo wewnętrzne i cywilne: ochronę porządku konstytucyjnego, porządku publicznego, bezpieczeństwa powszechnego oraz ochronę ludności i infrastruktury na terytorium państwa. Jego istotną cechą jest różnorodność instytucjonalna: funkcjonują w nim formacje porządkowe i graniczne, służby specjalne, elementy wymiaru sprawiedliwości oraz systemy ratownicze. W ujęciu strategicznym potrzeba szerokiego rozumienia bezpieczeństwa wewnętrznego jest w polskiej literaturze akcentowana jako konsekwencja zmienności

⁷⁹ Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655).

⁸⁰ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

zagrożeń i przenikania wymiaru wewnętrznego i zewnętrznego⁸¹. Pierwszą grupę instytucji ochronnych tworzą organy porządku publicznego, z Policją jako podstawową formacją przeznaczoną do ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego. Ustawa o Policji określa zasadnicze ramy działań policyjnych, wskazując cele związane m.in. z ochroną bezpieczeństwa i porządku publicznego, a więc z utrzymaniem warunków funkcjonowania społeczeństwa i państwa w codzienności oraz w sytuacjach nadzwyczajnych⁸². Operacyjny charakter Policji przejawia się w gotowości do prowadzenia działań interwencyjnych i zabezpieczających, w tym zabezpieczenia miejsca zdarzeń masowych, ochrony mienia, wsparcia ewakuacji, a także w zdolności do działania w warunkach podwyższonego ryzyka, co w praktyce wiąże się z koniecznością współdziałania z innymi służbami (ratowniczymi i specjalnymi) oraz z władzami administracyjnymi. Drugą grupę stanowią służby specjalne, których rola w podsystemie ochronnym polega na rozpoznawaniu, zapobieganiu i zwalczaniu zagrożeń godzących w bezpieczeństwo państwa, w tym w porządek konstytucyjny, oraz na dostarczaniu informacji i zdolności kontrwywiadowczych i wywiadowczych. Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wskazuje zadania ABW obejmujące m.in. rozpoznawanie i zwalczanie zagrożeń dla bezpieczeństwa wewnętrznego oraz obronności, a także ustanawia relację podległości szefów agencji wobec Prezesa Rady Ministrów i kontrolę parlamentarną⁸³.

W analogicznej logice funkcjonują wojskowe służby specjalne, których podstawy prawne wynikają z ustawy o SKW i SWW⁸⁴. Z perspektywy operacyjnych podsystemów wykonawczych służby specjalne pełnią rolę „systemu nerwowego” państwa: zmniejszają niepewność decyzyjną, wzmacniają rozpoznanie i przeciwdziałanie, a w przypadku zagrożeń hybrydowych i cybernetycznych stanowią część mechanizmu wczesnego ostrzegania

⁸¹ W. Kitler, Bezpieczeństwo wewnętrzne w świetle współczesnych wyzwań teorii i praktyki problemu, *Wiedza Obronna*, 282(1), 2023, s. 117-148. <https://doi.org/10.34752/2023-f282>

⁸² Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2024 r. poz. 145 ze zm.).

⁸³ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2025 r. poz. 902 ze zm.).

⁸⁴ Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2024 r. poz. 1198 ze zm.).

i neutralizacji wrogich oddziaływań⁸⁵. Trzecią grupę stanowi obszar wymiaru sprawiedliwości i egzekwowania prawa, którego funkcja w logice operacyjnej polega na zapewnieniu wykonalności norm w kryzysie oraz utrzymaniu zdolności państwa do reakcji na przestępczość, w tym przestępczość zorganizowaną lub inspirowaną zewnątrz. Choć wymiar sprawiedliwości jest często postrzegany jako „system następczy” względem działań służb porządkowych, w warunkach kryzysu i wojny jego znaczenie rośnie, ponieważ stabilność społeczeństwa zależy również od sprawnego ścigania, izolacji najbardziej niebezpiecznych sprawców oraz ochrony praw obywateli przy jednoczesnym utrzymaniu porządku. Te zależności są w literaturze o bezpieczeństwie narodowym ujmowane jako część szerokiej funkcji ochronnej państwa, obejmującej komponenty instytucjonalne i normatywne⁸⁶. Czwartą grupę tworzą systemy ratownicze i ochrony ludności, które w operacyjnym wymiarze realizują działania „pierwszej reakcji” i „odtworzenia podstawowych funkcji”. W obszarze ochrony przeciwpożarowej kluczową częścią aparatu operacyjnego jest Krajowy System Ratowniczo-Gaśniczy, którego zadania są osadzone ustawowo w przepisach o ochronie przeciwpożarowej. Z kolei w obszarze ratownictwa medycznego ustawa o Państwowym Ratownictwie Medycznym wskazuje, że system PRM tworzy się w celu zapewnienia pomocy każdej osobie znajdującej się w stanie nagłego zagrożenia zdrowotnego, a regulacja obejmuje organizację, funkcjonowanie i finansowanie systemu⁸⁷. Operacyjność tych systemów polega na zdolności do jednoczesnego działania wielu podmiotów (ratownictwo techniczne, medyczne, ewakuacja, zabezpieczenie porządku), przy czym o jakości ich działania przesądza interoperacyjność dyspozytorska, łącznościowa i dowódcza, a także zdolność do koordynacji z administracją publiczną (np. w zakresie ewakuacji, organizacji miejsc czasowego pobytu, wsparcia logistycznego). Piątym, rosnącym komponentem ochronnym jest bezpieczeństwo cybernetyczne w wymiarze operacyjnym. Ustawa o krajowym systemie cyberbez-

⁸⁵ S. Żurawski, M. Chodyka, Systemy wczesnego ostrzegania przed cyberzagrożeniami jako narzędzie bezpieczeństwa państwa, *Przegląd Naukowo-Metodyczny. Edukacja dla bezpieczeństwa*, XVIII, 2(67), 2025, s. 81-92.

⁸⁶ R. Rosicki, O pojęciu i istocie bezpieczeństwa, *Przegląd Politologiczny*, (3), 2010, s. 23-32. <https://doi.org/10.14746/pp.2010.15.3.2>

⁸⁷ Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2024 r. poz. 652 ze zm.).

pieczeństwa ustanawia zadania i obowiązki podmiotów w systemie oraz reguluje zadania zespołów reagowania (CSIRT), co tworzy formalny fundament operacyjnego reagowania na incydenty cybernetyczne na poziomie krajowym⁸⁸. Ponieważ ataki cybernetyczne mogą wpływać na świadczenie usług kluczowych, cyberbezpieczeństwo styka się bezpośrednio z ochroną infrastruktury krytycznej i ciągłością działania, a więc z tymi segmentami podsystemu ochronnego, które są powiązane z operatorami infrastruktury i administracją.

W polskim porządku prawnym nastąpiło wzmocnienie obszaru ochrony ludności i obrony cywilnej poprzez uchwalenie ustawy o ochronie ludności i obronie cywilnej, która określa zadania, organy i podmioty realizujące te zadania oraz mechanizmy zasobowe⁸⁹. Z punktu widzenia operacyjnych podsystemów wykonawczych jest to istotne, ponieważ wzmacnia formalne ramy organizowania zasobów ochronnych na poziomie terytorialnym i centralnym oraz wzmacnia powiązanie ochrony ludności z systemami reagowania, w tym z planowaniem, ćwiczeniami i ewidencją zasobów.

Opis operacyjnych podsystemów wykonawczych nie może abstrahować od relacji z podsystemem kierowania, ponieważ to właśnie w miejscu styku „decyzji” i „wykonania” ujawniają się kluczowe napięcia systemowe: problem szybkości uruchamiania zasobów, rozdział odpowiedzialności, kompatybilność planowania, a także zdolność do działania w warunkach eskalacji. W warunkach normalnych relacja ta ma charakter administracyjno-funkcjonalny: organy kierowania określają priorytety i finansowanie, tworzą dokumenty strategiczne i planistyczne, natomiast instytucje operacyjne odpowiadają za gotowość i bieżące działanie. W warunkach kryzysowych relacja ulega „zagęszczeniu”: rośnie rola procedur uruchamiania zasobów, a decyzje strategiczne muszą zostać przełożone na dyspozycje dla struktur wykonawczych w sposób jednoznaczny i szybszy niż w trybie rutynowym. Z punktu widzenia cywilno-wojskowej koordynacji szczególnie istotne są rozwiązania ustawowe dotyczące użycia wojska do wsparcia działań kryzysowych, ponieważ wymagają one uruchomienia odpowiednich kanałów

⁸⁸ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

⁸⁹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

wnioskowania, przekazania sił i zapewnienia współdziałania na miejscu działań, przy zachowaniu autonomii dowodzenia wojskowego w ramach regulaminów sił zbrojnych.

Szczególnym polem współdziałania są zagrożenia hybrydowe i cybernetyczne, które rozmywiają tradycyjny podział na „obronne” i „ochronne” instrumenty państwa. Strategia Bezpieczeństwa Narodowego 2020 wskazuje wprost potrzebę budowy odporności na zagrożenia, w tym hybrydowe, oraz integracji systemu bezpieczeństwa narodowego w taki sposób, by obejmował on płynne przechodzenie od pokoju do kryzysu i wojny. Z perspektywy operacyjnych podsystemów wykonawczych oznacza to konieczność równoczesnego działania komponentu obronnego i ochronnego: wojsko może budować zdolności odstraszania i obrony, ale jednocześnie potrzebne są działania policyjne, kontrwywiadowcze, ratownicze i informacyjne, żeby przeciwdziałać destabilizacji „poniżej progu wojny”.

Koordinacja współdziałania zależy także od zdolności do ochrony i odtwarzania infrastruktury krytycznej, ponieważ to infrastruktura jest wspólnym „punktem ciężkości” zarówno dla obrony, jak i ochrony. Ustawa o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną jako systemy i powiązane z nimi obiekty, instalacje, urządzenia i usługi kluczowe dla bezpieczeństwa państwa i obywateli oraz dla sprawnego funkcjonowania administracji i gospodarki, a jednocześnie ustanawia obowiązki informacyjne i planistyczne związane z jej ochroną. W tym kontekście Narodowy Program Ochrony Infrastruktury Krytycznej, publikowany na poziomie rządowym, wskazuje cykl ochrony obejmujący zapobieganie zakłóceniom, przygotowanie na kryzysy, reagowanie i odtwarzanie. Ponieważ wiele elementów infrastruktury krytycznej znajduje się w rękach operatorów publicznych i prywatnych, współdziałanie operacyjnych podsystemów wykonawczych musi obejmować również komponent międzysektorowy, obejmujący wymianę informacji, uzgodnienia techniczne, procedury priorytetyzacji usług i zasady współpracy w cyberincydentach. Relacja z podsystemem kierowania ujawnia także problem rozliczalności w działaniach operacyjnych: operacyjne podsystemy wykonawcze działają na podstawie upoważnień ustawowych, ale podlegają kontroli politycznej i prawnej. Przykładem są służby specjalne, których szefowie podlegają bezpośrednio Prezesowi Rady Ministrów, a działalność podlega kontroli Sejmu, co ma znaczenie w zakresie legalności

i proporcjonalności działań operacyjnych. Podobnie Policja realizuje zadania w zakresie porządku publicznego, ale jej działania w sytuacjach nadzwyczajnych muszą pozostawać w reżimie legalizmu i podlegać kontroli sądowej oraz prokuratorskiej, co w praktyce determinuje sposoby użycia środków przymusu i zakres ingerencji w prawa jednostki⁹⁰.

Wyzwania dotyczące operacyjnych podsystemów wykonawczych mają charakter zarówno strukturalny, jak i funkcjonalny. Po stronie strukturalnej najtrudniejsze są te problemy, które wynikają z wielości instytucji i reżimów kompetencyjnych: podsystem obronny posługuje się odmienną logiką dowodzenia niż podsystem ochronny, a systemy ratownicze, policyjne i specjalne mają własne procedury i hierarchie. W warunkach zagrożeń złożonych największym ryzykiem jest spadek szybkości i spójności reakcji wynikający z braku interoperacyjności systemów łączności, z rozbieżności procedur oraz z niejednoznaczności priorytetów. Strategia Bezpieczeństwa Narodowego 2020 postuluje wprost rozwój systemu łączności na potrzeby zarządzania systemem bezpieczeństwa narodowego oraz spójność planowania cywilnego i obronnego, co można interpretować jako odpowiedź na diagnozowane deficyty integracyjne⁹¹. Po stronie funkcjonalnej kluczowe są wyzwania związane z zasobami, szkoleniem i gotowością. Operacyjność podsystemu obronnego zależy od zdolności do rozwinięcia sił, uzupełniania strat i utrzymania działań długotrwałych, co wzmacnia znaczenie dobrze zarządzanych rezerw i systemu szkolenia. Normatywnie ustawa o obronie Ojczyzny tworzy podstawy aktywnej i pasywnej rezerwy oraz opisuje mechanizmy powołań i służby, jednak efektywność tych rozwiązań zależy od praktyki implementacyjnej, zdolności szkoleniowej i logistyki państwa, co w samym tekście ustawy pozostaje opisywane generalnie, a nie w formie gwarancji operacyjnych⁹². Równolegle podsystem ochronny musi utrzymywać zdolności do reagowania na zdarzenia masowe, epidemie, katastrofy i zagrożenia hybrydowe, co wymaga nie tylko kadr, lecz także sprawnych procedur dowodzenia incydemem i koordynacji wielopodmiotowej.

⁹⁰ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 1990 r. Nr 30, poz. 179).

⁹¹ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

⁹² Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2024 r. poz. 248 ze zm.).

Ważnym obszarem ryzyka pozostaje ochrona ludności oraz zdolność do działania w warunkach degradacji infrastruktury. Najwyższa Izba Kontroli wielokrotnie wskazywała na problemy dotyczące systemu ochrony ludności, a także jakości planowania i przygotowania, obejmujące m.in. niedoskonałości raportowania sytuacyjnego, deficyty analiz i prognoz oraz nieefektywne rozwiązania w zakresie powiadamiania podmiotów ujętych w siatce bezpieczeństwa i planach zarządzania kryzysowego⁹³. Z perspektywy operacyjnych podsystemów wykonawczych ma to znaczenie bezpośrednie, ponieważ słabości planowania i łączności przekładają się na opóźnienia w uruchamianiu zasobów ochronnych i na spadek skuteczności działań w terenie.

Wyzwania hybrydowe i cybernetyczne ujawniają ponadto konieczność ścisłej współpracy z sektorem prywatnym i z operatorami usług kluczowych. Ochrona infrastruktury krytycznej, zgodnie z definicją ustawową i programami rządowymi, obejmuje nie tylko działanie państwa, lecz także obowiązki informacyjne i planistyczne po stronie właścicieli i posiadaczy elementów infrastruktury, co w praktyce wymaga dojrzałych mechanizmów wymiany danych, wspólnych ćwiczeń i jasnych modeli odpowiedzialności. W cyberbezpieczeństwie podobna logika jest osadzona w ustawie o krajowym systemie cyberbezpieczeństwa, która reguluje zadania CSIRT i współdziałanie w reagowaniu na incydenty, ale pozostawia otwarte pytanie o tempo wdrażania zdolności i o poziom integracji z planowaniem obronnym⁹⁴. Konsekwencją tych diagnoz jest rosnące znaczenie spójnych instrumentów programowych i instytucjonalnych. Przyjęcie ustawy o ochronie ludności i obronie cywilnej oraz zatwierdzenie Programu Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 można interpretować jako próbę wzmocnienia „cywilnego ramienia” operacyjnych zdolności ochronnych, w tym poprzez porządkowanie zadań, zasobów i ćwiczeń^{95,96}.

⁹³ Najwyższa Izba Kontroli, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej (Informacja o wynikach kontroli), nr ewidencyjny: P/17/039 (KPB.430.009.2017; Nr ewid. 147/2018/P/17/039/KPB), Warszawa, 2019.

⁹⁴ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

⁹⁵ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

⁹⁶ Uchwała nr 72 Rady Ministrów z dnia 27 maja 2025 r. w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 (M.P. z 2025 r. poz. 541).

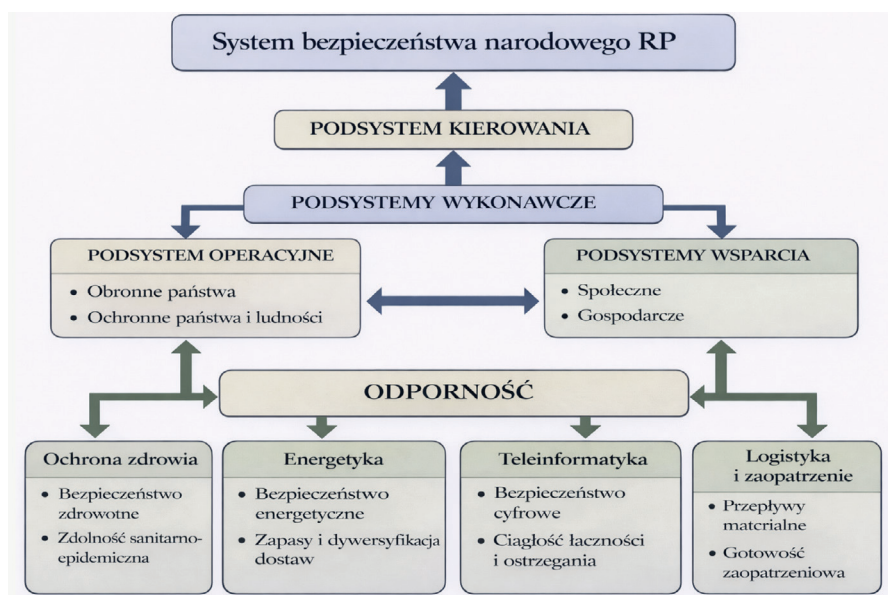
Z punktu widzenia monografii o systemie bezpieczeństwa narodowego zasadniczą kwestią pozostaje jednak to, czy reformy te doprowadzą do realnego zwiększenia interoperacyjności i gotowości na styku podsystemu obronnego i ochronnego, a w szczególności w obszarze działania państwa w „szarej strefie” zagrożeń hybrydowych, gdzie granice między obroną i ochroną są funkcjonalnie płynne, choć prawnie nadal rozdzielone.

1.4. Podsystemy wykonawcze o charakterze wsparcia

Podsystemy wykonawcze o charakterze wsparcia stanowią tę część systemu bezpieczeństwa narodowego, która podtrzymuje zdolność państwa i społeczeństwa do funkcjonowania oraz odtwarzania kluczowych zasobów w warunkach presji kryzysowej i zagrożeń o charakterze współczesnym, w tym hybrydowym i cybernetycznym. Ich istota polega na zapewnianiu „ciągłości” w trzech nakładających się wymiarach: ciągłości usług warunkujących standard życia i stabilność społeczno-gospodarczą, ciągłości działania administracji publicznej oraz ciągłości wsparcia dla podsystemów operacyjnych, które realizują zadania ochronne i obronne. W polskich dokumentach strategicznych i programowych podkreśla się, że budowanie odporności państwa wymaga rozwijania zdolności do ochrony i odtwarzania zasobów, w szczególności w obszarach energii, łączności, transportu, ochrony zdrowia oraz zasobów żywności i wody. Przyjęte ramy prawne (zarządzanie kryzysowe, ochrona infrastruktury krytycznej, rezerwy strategiczne, cyberbezpieczeństwo, bezpieczeństwo energetyczne) tworzą instrumentarium, które pozwala łączyć logikę sektorową z wymogiem koordynacji międzysektorowej. W praktyce problemem krytycznym nie jest samo istnienie „sfer wsparcia”, lecz ich spójne włączenie w mechanizmy planowania, finansowania i odpowiedzialności, tak, aby wsparcie nie było wyłącznie zasobem „do uruchomienia”, ale trwałą zdolnością systemową.

W przyjętej w monografii logice systemowej podsystemy wsparcia sytuują się wśród podsystemów wykonawczych obok podsystemów operacyjnych. Ich odrębność nie wynika z „mniejszej wagi”, ale z odmiennej funkcji: zamiast bezpośredniego neutralizowania zagrożeń realizują one funkcje utrzymywania zdolności państwa do trwania, sprawnego rządzenia

i odtwarzania potencjału społecznego oraz gospodarczego. W klasycznym ujęciu system bezpieczeństwa narodowego składa się z podsystemu kierowania oraz podsystemów wykonawczych, w tym operacyjnych i wsparcia. Wsparcie ma w szczególności wymiar społeczny i gospodarczy, a jego „powszechność przygotowań” jest warunkiem synergii całego systemu⁹⁷. Na poziomie definicyjnym podsystemy wsparcia opisuje się jako podmioty społeczne i gospodarcze przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukcji ryzyk i przeciwdziałania zagrożeniom o charakterze społecznym i gospodarczym, a w ujęciu systemowym – jako element wykonawczy pozostający w dyspozycji organów kierowania bezpieczeństwem. Schemat struktury systemu bezpieczeństwa narodowego RP, obejmujący podsystem kierowania oraz podsystemy wykonawcze (operacyjne i wsparcia), z uwzględnieniem funkcji wsparcia jako warstwy odporności państwa, przedstawiony został na rysunku 3.



Rysunek 3. Miejsce podsystemów wsparcia w strukturze systemu bezpieczeństwa narodowego RP

Źródło: opracowanie własne.

⁹⁷ Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.

Warto zauważyć, że to „klasyczne” rozróżnienie (społeczne i gospodarcze) wymaga dziś interpretacji funkcjonalnej, ponieważ współczesne wsparcie obejmuje również obszary, które są jednocześnie sektorami gospodarki, zasobami społecznymi i domenami infrastrukturalnymi, takie jak ochrona zdrowia, teleinformatyka, energetyka czy logistyka łańcuchów dostaw. Logika ta jest spójna z szerokim rozumieniem bezpieczeństwa jako możliwości zaspokajania potrzeb egzystencjalnych, przetrwania i rozwoju, które obejmuje coraz silniej wymiary pozamilitarne.

Konsekwencją takiego ujęcia jest traktowanie podsystemów wsparcia jako „warstwy odporności” systemu państwa. W Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 odporność rozumiana jest praktycznie jako zdolność państwa do utrzymania ciągłości rządzenia i funkcjonowania, zapewnienia skutecznych dostaw energii, utrzymania odpornych sieci telekomunikacyjnych i systemów teleinformatycznych, systemów informowania i ostrzegania oraz wydolnego transportu, a także do gromadzenia i utrzymywania zdolności odtwarzania niezbędnych zasobów. Z perspektywy podsystemu wsparcia oznacza to przesunięcie akcentu z „doraźnego zabezpieczenia” na trwałe zdolności ciągłości i odbudowy.

Zakres wsparcia najlepiej uchwycić przez pryzmat funkcji, a nie listy instytucji. W praktyce podsystemy wsparcia obejmują utrzymywanie i rozwijanie zasobów społecznych, produkcyjnych, infrastrukturalnych i informacyjnych, które umożliwiają realizację interesów bezpieczeństwa w czasie pokoju, kryzysu i wojny. W dokumentach państwowych wyraźnie widać, że współczesne wsparcie jest powiązane z krytycznymi usługami publicznymi i rynkowymi: przepływem pieniądza, dostępnością energii, zdolnością systemu ochrony zdrowia, odpornością teleinformatyczną oraz zdolnością do utrzymania standardu życia i spójności społecznej. W komponencie społecznym kluczowe znaczenie mają mechanizmy, które stabilizują społeczeństwo i redukują podatność na presję kryzysową: bezpieczeństwo socjalne i zdrowotne, spójność społeczna, kapitał ludzki i zaufanie do instytucji. Strategia 2020 ujmuje je w kategoriach celów rozwojowych i demograficznych oraz bezpieczeństwa zdrowotnego obywateli, wskazując potrzebę poprawy koordynacji, ciągłości i kompleksowości opieki, a także zdolności przeciwdziałania zagrożeniom epidemiologicznym. W tym sensie bezpieczeństwo zdrowotne jest zarazem wsparciem społecznym i warunkiem funkcjonowania

państwa jako organizacji zdolnej do działania w warunkach masowych zakłóceń.

Komponent gospodarczy wsparcia obejmuje zarówno zdolności produkcyjne i usługowe, jak i stabilność finansów publicznych oraz mechanizmy „sterowania” gospodarką w sytuacjach zakłóceń. Strategia 2020 wskazuje wprost na wzmocnienie bezpieczeństwa ekonomicznego, w tym finansowego, poprzez zwiększanie odporności na kryzysy finansowe i stabilność systemu finansów publicznych; podnosi również kwestię utrzymania sprawnego systemu przepływu pieniądza w przypadku zakłócenia funkcjonowania systemu bankowego. Z perspektywy wsparcia bezpieczeństwo ekonomiczne ma charakter infrastrukturalny: nie jest wyłącznie „polityką gospodarczą”, lecz zdolnością do utrzymania krytycznych funkcji gospodarczych w warunkach presji (wahań, sankcji, zakłóceń logistycznych, szoków popytowo-podażowych).

W komponencie energetycznym, będącym rdzeniem wsparcia gospodarczego i infrastrukturalnego, istotą jest ciągłość dostaw energii i paliw oraz możliwość reagowania na sytuacje niedoboru⁹⁸. Ustawowa definicja bezpieczeństwa energetycznego w polskim prawie podkreśla zdolność gospodarki do pokrycia bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska⁹⁹. Strategia 2020 rozwija ten kierunek poprzez akcent na modernizację mocy wytwórczych i sieci przesyłu/dystrybucji w celu zapewnienia ciągłości dostaw oraz na dywersyfikację źródeł dostaw surowców energetycznych¹⁰⁰. W warunkach zagrożeń hybrydowych energetyka jest jednocześnie zasobem wsparcia i potencjalnym celem oddziaływania przeciwnika, co wymusza ściśle sprzężenie wsparcia z ochroną infrastruktury krytycznej.

⁹⁸ T. Grudniewski, M. Czernastek, I. Lasek-Surowiec, M. Frelak, Bezpieczeństwo energetyczne w regionach przygranicznych Polski, w: *Ochrona granicy Rzeczypospolitej Polskiej w dobie współczesnych zagrożeń bezpieczeństwa*, S. Żurawski, M. Oskierko, T. Grudniewski (red.), Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025, s. 283-294. https://doi.org/10.29316/9788368103236_17

⁹⁹ Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2024 r. poz. 266 ze zm., art. 3 pkt 16).

¹⁰⁰ Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, BBN, 2020.

Komponent informacyjno-łącznościowy jest jednym z najbardziej „dwufunkcyjnych” elementów wsparcia: zapewnia komunikację dla rządu i współdziałania instytucji, a równocześnie jest polem oddziaływania (cyberataki, dezinformacja). W Ustawie o krajowym systemie cyberbezpieczeństwa cyberbezpieczeństwo zdefiniowano jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność danych lub usług, a celem systemu jest m.in. niezakłócone świadczenie usług kluczowych i usług cyfrowych oraz zapewnienie obsługi incydentów¹⁰¹. Z perspektywy wsparcia oznacza to, że łączność i teleinformatyka nie są wyłącznie „narzędziem”, lecz jednym z podstawowych zasobów odpornościowych państwa. Jednocześnie kanały komunikacji publicznej są instrumentem ochrony ludności: Rządowe Centrum Bezpieczeństwa opisuje Alert RCB jako system SMS-owego powiadamiania wykorzystywany w sytuacjach nadzwyczajnych przy prawdopodobieństwie bezpośredniego zagrożenia życia lub zdrowia na znaczącym obszarze, bazujący na informacjach m.in. od służb i instytucji publicznych¹⁰².

Logistyka i zaopatrzenie – choć często „niewidoczne” w ujęciach instytucjonalnych – są funkcją przekrojową wsparcia. Są one zarazem komponentem gospodarczym (rynek, produkcja, magazynowanie), elementem ochrony ludności (dystrybucja wody, żywności, leków) oraz warunkiem utrzymania operacyjności podsystemów obronnego i ochronnego.

Planowanie podsystemów wsparcia jest w praktyce planowaniem zdolności państwa do utrzymania funkcji krytycznych i do szybkiej odbudowy. Jego rdzeń stanowią mechanizmy planowania cywilnego, planowania ochrony infrastruktury krytycznej i planowania rezerw. W prawie o zarządzaniu kryzysowym podkreśla się, że zarządzanie kryzysowe obejmuje działania od zapobiegania i przygotowania po reagowanie i odtwarzanie infrastruktury, co z definicji wpisuje wsparcie w logikę „ciągłości funkcjonowania”. Szczególnie istotne jest tu umiejscowienie planowania cywilnego w zadaniach państwa: w katalogu zadań centralnych organów wsparcia wskazuje się m.in. opracowywanie i aktualizowanie krajowego planu reagowania

¹⁰¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

¹⁰² Rządowe Centrum Bezpieczeństwa, Alert RCB – najważniejsze pytania i odpowiedzi, <https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi>, [dostęp: 10.07.2025].

kryzysowego, analizę i ocenę zagrożeń, planowanie wsparcia administracji publicznej dla realizacji zadań Sił Zbrojnych oraz zapewnienie obiegu informacji między strukturami krajowymi i zagranicznymi¹⁰³.

W wymiarze systemowym oznacza to, że wsparcie jest projektowane „dwukierunkowo”: z jednej strony na rzecz ochrony ludności i utrzymania usług, z drugiej na rzecz zdolności obronnych (spójność planowania cywilnego i obronnego jest wskazywana jako cel strategiczny).

Najbardziej materialnym instrumentem wsparcia są rezerwy strategiczne. Ustawa o rezerwach strategicznych określa je jako zasób tworzony na wypadek zagrożeń bezpieczeństwa i obronności państwa, bezpieczeństwa, porządku i zdrowia publicznego oraz klęsk żywiołowych lub sytuacji kryzysowych, w celach wsparcia realizacji zadań przez organy i podmioty odpowiedzialne¹⁰⁴. Mechanizm planistyczny ma postać Rządowego Programu Rezerw Strategicznych, który określa asortymenty i ilości rezerw, a projekt Programu opracowywany jest przez Prezesa Rady Ministrów we współpracy z agencją rezerw oraz właściwymi ministrami. Z punktu widzenia zarządzania systemowego szczególnie ważne są dwie konsekwencje: po pierwsze, decyzja o udostępnieniu rezerw ma charakter decyzji centralnej (w praktyce „uruchomienia zasobu strategicznego”), po drugie, logika rezerw łączy bezpieczeństwo wewnętrzne i zewnętrzne, bo rezerwy mogą być udostępniane przy zarówno zagrożeniach militarnych, jak i niemilitarnych. W tym układzie instytucjonalnym funkcję wykonawczą w zakresie utrzymywania i obsługi rezerw pełni Rządowa Agencja Rezerw Strategicznych, której genezę i przekształcenie z Agencji Rezerw Materiałowych wiąże się wejściem w życie ustawy o rezerwach strategicznych¹⁰⁵. W kategoriach wsparcia oznacza to formalizację „logistyki strategicznej państwa” jako zdolności instytucjonalnej: magazynowanie, wymiana (rotacja) zasobów, mechanizmy zakupowe w sytuacjach szczególnych i dystrybucja do odbiorców publicznych w przypadkach zagrożeń. Wymiar planowania wsparcia w ochronie

¹⁰³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590).

¹⁰⁴ Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz.U. z 2024 r. poz. 1598, art. 2 pkt 1).

¹⁰⁵ Rządowa Agencja Rezerw Strategicznych, Historia, (informacja o przekształceniu ARM w RARS na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych, obowiązującej od 23 lutego 2021 r.), <https://www.gov.pl/web/rars/historia2>, [dostęp: 10.07.2025].

zdrowia pokazuje, jak silnie przenikają się obszary społeczne, gospodarcze i infrastrukturalne. Strategia 2020 wskazuje potrzebę rozwijania zdolności systemu ochrony zdrowia i administracji publicznej do zwalczania zagrożeń epidemicznych oraz włączenia odpowiednich środków ochrony i sprzętu medycznego do programu rezerw strategicznych, wraz ze wspieraniem krajowych zdolności produkcyjnych branży medycznej¹⁰⁶. W logice wsparcia jest to przykład przejścia od „pomocy” do „zdolności reprodukcyjnej” państwa, gdzie bezpieczeństwo zależy nie tylko od zapasów, ale i od zdolności produkcji oraz dystrybucji w warunkach kryzysu.

Podsystemy wsparcia, rozpatrywane jako fundament odporności państwa, w istotnym zakresie opierają się na ochronie oraz zapewnieniu ciągłości działania infrastruktury krytycznej. Ustawa o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną jako systemy oraz powiązane funkcjonalnie obiekty, instalacje, urządzenia i usługi kluczowe dla bezpieczeństwa państwa i obywateli oraz sprawnego funkcjonowania administracji publicznej, instytucji i przedsiębiorców; jednocześnie wskazuje, że obejmuje ona m.in. systemy energii i paliw, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne oraz ratownicze¹⁰⁷. Ustawowe wyliczenie ma charakter systemowy, ponieważ porządkuje obszary wsparcia poprzez wskazanie kluczowych usług i funkcji państwa, a nie wyłącznie sektorowych polityk publicznych. W tym ujęciu Narodowy Program Ochrony Infrastruktury Krytycznej 2023 stanowi ramę programową rozwijającą podejście do ochrony infrastruktury krytycznej jako procesu zorientowanego na ochronę ciągłości świadczenia usług oraz ich odtwarzanie po zakłóceniu. Dokument akcentuje, że przerwanie funkcjonowania współdzielonej infrastruktury państwa i przedsiębiorców może generować skutki wykraczające poza pojedynczą organizację, co uzasadnia podejście partnerskie oraz redukcję ryzyk wynikających ze współzależności¹⁰⁸. Program doprecyzowuje również układ odpowiedzialności,

¹⁰⁶ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

¹⁰⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590).

¹⁰⁸ Rządowe Centrum Bezpieczeństwa, Alert RCB – najważniejsze pytania i odpowiedzi, <https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi>, [dostęp: 10.07.2025].

wskazując rolę RCB, operatorów infrastruktury krytycznej, ministrów właściwych dla poszczególnych systemów oraz innych organów administracji, a także podkreślając znaczenie współpracy, wymiany informacji i uwarunkowań finansowania ochrony infrastruktury krytycznej.

Z perspektywy odporności państwa istotne jest także ujęcie strategiczne, w ramach którego Strategia z 2020 r. formułuje zadanie wdrożenia modelu ochrony infrastruktury krytycznej polegającego na zapewnieniu ciągłości działania i świadczonych usług. Oznacza to przesunięcie akcentu z ochrony zasobów materialnych ku ochronie funkcji i zdolności do nieprzerwanego świadczenia usług o znaczeniu krytycznym¹⁰⁹. Konsekwencją takiego podejścia jest wymóg planowania ochrony infrastruktury krytycznej z uwzględnieniem ciągłości funkcjonowania, a także potrzeba systematycznego prowadzenia ćwiczeń oraz testowania procedur odtwarzania jako elementu operacyjnej gotowości podsystemów wsparcia. Na poziomie instytucjonalnym kategoria „ciągłości działania” coraz częściej przyjmuje postać wymagania formalnego, a nie jedynie dobrowolnej praktyki zarządczej. W analizach dotyczących wdrażania ustawy o ochronie ludności i obronie cywilnej wskazuje się na potrzebę promowania ciągłości działania w wymiarze lokalnym oraz rozwijania kultury zapobiegania ryzyku, w tym w relacji do wymogów ochrony infrastruktury krytycznej. Jednocześnie należy odnotować, że pełne doprecyzowanie kompetencji oraz standardów wykonawczych w tym obszarze będzie weryfikowalne dopiero po analizie kompletnego zestawu aktów wykonawczych oraz ocenie praktyki ich implementacji w administracji publicznej i u operatorów usług kluczowych.

Relacja między podsystemem kierowania a podsystemami wsparcia ma charakter „sterowania zasobami” oraz „sterowania ciągłością działania” państwa. W ujęciu systemowym podsystem wsparcia pozostaje zasadniczo wykonawczy, lecz jednocześnie współkształtuje realną sprawczość kierowania: bez dostępu do infrastruktury, zasobów materialnych i finansowych oraz społecznej legitymizacji decyzje strategiczne tracą wykonalność. Z tego powodu w Białej Księdze Bezpieczeństwa Narodowego RP akcentowano, że synergia systemu bezpieczeństwa powinna wynikać z integracji kierowania,

¹⁰⁹ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

profesjonalizacji podsystemów operacyjnych oraz powszechności przygotowań w podsystemach wsparcia¹¹⁰. W konsekwencji wsparcie można traktować jako „warunek brzegowy” skuteczności operacyjnej: dostarcza finansowania, energii, zdolności transportowych, łączności, materiałów i zasobów, zabezpiecza potencjał medyczny, a także umożliwia odtwarzanie utraconych zdolności i usług. W stanie normalnego funkcjonowania państwa (pokoju) oddziaływanie podsystemu wsparcia ma przede wszystkim wymiar strukturalny i długofalowy. Obejmuje ono inwestycje w odporność infrastruktury, rozwój zdolności produkcyjnych i logistycznych w obszarze zasobów strategicznych, budowanie stabilności fiskalnej, modernizację systemu ochrony zdrowia, utrzymywanie rezerw oraz rozwijanie systemów teleinformatycznych i kanałów ostrzegania. Wprost wpisuje się to w rozumienie odporności państwa przyjęte w Strategii Bezpieczeństwa Narodowego RP 2020, gdzie wskazuje się m.in. potrzebę zapewnienia ciągłości rządzenia, bezpieczeństwa dostaw energii, odporności sieci telekomunikacyjnych, sprawnego systemu informowania i ostrzegania ludności oraz wydolnego transportu. Oznacza to, że „pokój” należy ujmować jako okres budowy zdolności, które w warunkach kryzysowych powinny uruchamiać się możliwie automatycznie, w oparciu o uprzednio przygotowane zasoby, procedury i infrastrukturę, a nie poprzez improwizację.

W stanie kryzysu podsystem wsparcia zyskuje charakter mechanizmu kompensacji niedoborów oraz skracania czasu od zakłócenia do przywrócenia kluczowych usług. Uruchamianie rezerw strategicznych, redystrybucja zasobów, priorytetyzacja dostaw energii, działania stabilizujące w sferze finansów publicznych, a także zapewnienie łączności i wymiany informacji nie stanowią „dodatku” do działań ochronnych, lecz warunek utrzymania zdolności państwa do odzyskania kontroli nad sytuacją. Logikę tę wspierają rozwiązania prawne: regulacje dotyczące rezerw strategicznych przewidują udostępnianie rezerw decyzją Prezesa Rady Ministrów w razie wystąpienia zagrożeń, natomiast ustawa o zarządzaniu kryzysowym osadza planowanie

¹¹⁰ Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.

cywilne oraz obieg informacji jako zadania systemowe^{111,112}. W tym kontekście szczególnego znaczenia nabierają instrumenty komunikacji publicznej, w tym ostrzeganie ludności (np. Alert RCB), które pełni zarazem funkcję wsparcia społecznego i operacyjnego, ponieważ wpływa na zachowania ludności oraz ogranicza skalę strat i chaosu decyzyjnego¹¹³.

W stanie wojny rola wsparcia ulega dalszemu usystemowieniu: przechodzi od logiki podtrzymania podstawowych usług publicznych do logiki utrzymania zdolności obronnych państwa jako całości. Strategia Bezpieczeństwa Narodowego RP 2020 akcentuje konieczność budowania zdolności produkcji zasobów strategicznych w warunkach pokoju, kryzysu i wojny, a także potrzebę takiego kształtowania systemu rezerw strategicznych, aby odpowiadał zmianom środowiska bezpieczeństwa¹¹⁴. W wymiarze instytucjonalnym wzmacniane są również mechanizmy zapewnienia ciągłości działania administracji w warunkach wojennych; przykładowo regulacje z zakresu ochrony ludności i obrony cywilnej przewidują obowiązki w zakresie zapewnienia funkcjonowania urzędów w czasie wojny na poziomie samorządu terytorialnego¹¹⁵. W rezultacie wsparcie przesuwają się w stronę problematyki odporności państwa jako organizacji: utrzymanie usług, łańcuchów dostaw i zdolności produkcyjnych staje się współrównoważne z utrzymaniem sprawczości kierowania oraz zdolności operacyjnych.

Współczesne wyzwania dla podsystemów wsparcia wynikają z faktu, że „wsparcie” bywa dziś pierwszą linią oddziaływania przeciwnika albo źródłem kaskadowych skutków kryzysu. Dokumenty strategiczne podkreślają zagrożenia hybrydowe oraz potrzebę budowania odporności obejmującej zarówno komponent niemilitarny, jak i militarny, w tym zdolności odtwarzania zasobów oraz zapewnienia ciągłości działania kluczowych systemów¹¹⁶.

¹¹¹ Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz.U. z 2024 r. poz. 1598, art. 2 pkt 1).

¹¹² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590).

¹¹³ Rządowe Centrum Bezpieczeństwa, Informacje o systemie ostrzegania ludności (Alert RCB), <https://www.gov.pl/web/rcb>, [dostęp: 10.07.2025].

¹¹⁴ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

¹¹⁵ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, (Dz.U. z 2024 r. poz. 1907).

¹¹⁶ Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.

W wymiarze praktycznym oznacza to, że testem dla wsparcia staje się odporność na zdarzenia wielodomenowe, w których równocześnie dochodzi do zakłóceń energetycznych, teleinformatycznych, logistycznych oraz informacyjnych. Pierwszym z głównych wyzwań pozostaje odporność łańcuchów dostaw oraz zdolność do redystrybucji zasobów w warunkach ograniczeń transportowych, niedoborów rynkowych lub presji popytowej. Odpowiedzią instytucjonalną są rezerwy strategiczne oraz narzędzia ich planowania i udostępniania, jednak skuteczność tych rozwiązań zależy od jakości prognoz, właściwej rotacji asortymentu oraz sprawności systemu dystrybucji¹¹⁷. Z perspektywy systemowej problem „rezerw” nie sprowadza się do magazynowania, lecz dotyczy budowy zdolności logistycznej państwa, w tym współpracy z podmiotami prywatnymi w zakresie mocy produkcyjnych i usług, co znajduje odzwierciedlenie w rozwiązaniach ustawowych. Drugim wyzwaniem jest energetyka. Transformacja technologiczna oraz rosnąca złożoność systemu elektroenergetycznego zwiększają wymagania wobec niezawodności sieci i zdolności bilansowania dostaw, a jednocześnie podnoszą wrażliwość na presję zewnętrzną i sabotaż infrastrukturalny. Bezpieczeństwo energetyczne staje się tu jednocześnie celem polityki gospodarczej oraz warunkiem działania podsystemów operacyjnych, co uzasadnia normatywne i strategiczne ujęcie ciągłości dostaw oraz modernizacji infrastruktury wytwórczej i sieciowej¹¹⁸. Trzecim wyzwaniem jest cyberbezpieczeństwo i bezpieczeństwo informacyjne. Ustawa o krajowym systemie cyberbezpieczeństwa ustanawia ramy systemu, w tym funkcjonowanie zespołów CSIRT na poziomie krajowym oraz kategorie incydentów, co uzasadnia traktowanie cyberbezpieczeństwa jako warunku niezakłóconego świadczenia usług kluczowych¹¹⁹. Równolegle rozwijane są instrumenty reagowania na dezinformację, m.in. inicjatywy prowadzone przez Rządowe Centrum Bezpieczeństwa, lokowane w krajowym systemie przeciwdziałania dezinformacji i propagandzie. Istotne jest także to, że sfera informacyjna została włączona do porządku prawnego poprzez zadania organów ochrony ludności: wskazano obowiązek przeciwdziałania dezinformacji obniżającej odporność społeczną w zakresie

¹¹⁷ Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz.U. z 2024 r. poz. 1598 ze zm.).

¹¹⁸ Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2024 r. poz. 266 ze zm.).

¹¹⁹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

właściwości rzeczowej organów. W efekcie wsparcie informacyjne przestaje mieć charakter wyłącznie „miękki” i staje się komponentem odporności państwa wymagającym planowania, koordynacji oraz rozliczalności.

Czwartym wyzwaniem pozostaje finansowanie wsparcia oraz rozkład odpowiedzialności w układzie publiczno-prywatnym. Ochrona infrastruktury krytycznej ma bowiem naturę współzależności między państwem a operatorami, a dokumenty programowe w obszarze ochrony infrastruktury akcentują potrzebę wielostronnej, partnerskiej współpracy na rzecz nieprzerwanego dostępu do usług. Z punktu widzenia zarządzania systemowego wymaga to równoważenia regulacji, zachęt inwestycyjnych i standardów ciągłości działania, a także ochrony informacji wrażliwej, przy jednoczesnym utrzymaniu sprawnych mechanizmów koordynacji sektorowej i międzysektorowej. Ujęcie systemowe podkreśla w tym miejscu znaczenie sprzężeń i sterowania: przepływ zasobów oraz informacji współdecyduje o zdolności całego układu bezpieczeństwa do działania, a więc o realnej „sterowalności” państwa w warunkach zakłóceń.

1.5. Bezpieczeństwo wewnętrzne i zewnętrzne

Bezpieczeństwo państwa stanowi kategorię nadrzędną, obejmującą całokształt warunków i działań umożliwiających ochronę podstawowych wartości konstytucyjnych, utrzymanie sprawności instytucji publicznych oraz realizację interesów narodowych w zmiennym otoczeniu. W ujęciu analitycznym jest to zjawisko wielowymiarowe i dynamiczne, ponieważ pozostaje rezultatem relacji pomiędzy identyfikowanymi zagrożeniami a zdolnościami państwa do ich zapobiegania, neutralizacji oraz ograniczania skutków¹²⁰.

Jednym z klasycznych i nadal użytecznych sposobów porządkowania tej problematyki jest rozróżnienie bezpieczeństwa wewnętrznego i zewnętrznego. Podział ten pozwala uporządkować źródła ryzyk, określić dominujące instrumenty reagowania oraz wskazać główne podmioty odpowiedzialne

¹²⁰ Z. Ciekankowski, J. Nowicka, H. Wyřębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Siedlce, Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, 2016.

za realizację zadań bezpieczeństwa. Jednocześnie współczesne środowisko bezpieczeństwa powoduje, że rozróżnienia tego nie należy interpretować w sposób dychotomiczny (jako dwa „rozłączne” porządki działania), lecz raczej jako układ współzależnych wymiarów, w którym zagrożenia mogą mieć równocześnie wektor zewnętrzny i skutki wewnętrzne, a granica między nimi bywa funkcjonalnie płynna¹²¹.

W ujęciu ogólnym bezpieczeństwo zewnętrzne koncentruje się na ochronie suwerenności, integralności terytorialnej oraz zdolności państwa do realizacji interesów w środowisku międzynarodowym. Z kolei bezpieczeństwo wewnętrzne odnosi się do utrzymania porządku konstytucyjnego, ochrony ludności i mienia, zapewnienia bezpieczeństwa powszechnego oraz ciągłości funkcjonowania kluczowych instytucji i usług publicznych. Należy jednak podkreślić, że w warunkach zagrożeń transgranicznych (np. cybernetycznych, informacyjnych, ekonomicznych czy hybrydowych) oba wymiary coraz częściej wymagają komplementarnych narzędzi oraz koordynacji działań między instytucjami odpowiedzialnymi za domenę obronną, ochroną i wsparcia. Ogólny schemat podziału bezpieczeństwa państwa na wymiar wewnętrzny i zewnętrzny przedstawiono na rysunku 4.



Rysunek 4. Bezpieczeństwo państwa w ujęciu dualnym

Źródło: opracowanie własne.

¹²¹ Z. Ciekanowski, Człowiek wobec współczesnych zagrożeń bezpieczeństwa państwa, *Studia Bezpieczeństwa Narodowego*, 11(1), 2017, s. 31-52. <https://doi.org/10.37055/sbn/129880>

W polskiej literaturze przedmiotu spotyka się ujęcie, w którym bezpieczeństwo zewnętrzne rozumiane jest jako stan i proces równowagi między zagrożeniami wywołanymi czynnikami zewnętrznymi (np. użycie siły, terroryzm międzynarodowy, proliferacja, przestępczość międzynarodowa) a potencjałem obronnym państwa, natomiast bezpieczeństwo wewnętrzne jako stan i proces równowagi między czynnikami wewnętrznymi (np. klęski żywiołowe, przestępczość, napięcia społeczne) a zdolnościami państwa do ochrony wartości i interesów wewnętrznych¹²². Tak zarysowane definicje mają dwie konsekwencje istotne z perspektywy systemu bezpieczeństwa narodowego. Po pierwsze, wskazują na „procesualność” bezpieczeństwa: nie jest ono wyłącznie stanem, lecz relacją dynamiczną między zagrożeniami a zdolnościami państwa. Po drugie, sugerują, że w każdym z wymiarów kluczowym zasobem pozostaje zdolność organizowania i integrowania potencjałów (obronnych, ochronnych, społecznych i gospodarczych) w odpowiedzi na ewolucję ryzyk. Wprost potwierdza to państwowa perspektywa strategiczna: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 explicite opisuje aspekt podmiotowy bezpieczeństwa jako obejmujący „wymiar wewnętrzny” oraz „środowisko międzynarodowe” (stosunki i współpracę w różnych formatach), a więc traktuje oba wymiary jako elementy jednej, spójnej logiki bezpieczeństwa państwa.

W ujęciu klasycznym (państwowocentrycznym) bezpieczeństwo zewnętrzne wiązano nadrzędnie z zagrożeniem militarnym, odstraszaniem i obroną terytorium, natomiast bezpieczeństwo wewnętrzne – z porządkiem publicznym, stabilnością ustroju oraz ochroną ludności. Taki podział odpowiadał logice dominacji konfliktów międzypaństwowych oraz względnie wyraźnego rozdziału między polityką obronną i polityką porządku publicznego. Rozszerzenie agendy bezpieczeństwa (po zimnej wojnie) doprowadziło jednak do wzmocnienia ujęć wielosektorowych, w których zagrożenia i podatności rozpatruje się nie tylko w sektorze militarnym, lecz także politycznym, ekonomicznym, społecznym i środowiskowym. Jest to typowe m.in. dla dorobku szkoły kopenhaskiej¹²³.

¹²² E. Nowak, Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych, Warszawa, Akademia Obrony Narodowej, 2007.

¹²³ B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner Publishers, 1998. <https://doi.org/10.1515/9781685853808>

Z perspektywy niniejszego podrozdziału kluczowe jest to, że wielosektorowość „rozmywa” tradycyjną linię podziału wewnętrzne-zewnętrzne: zagrożenia ekonomiczne (np. szoki energetyczne), informacyjne (operacje wpływu), cybernetyczne czy zdrowotne nie mają jednoznacznej lokalizacji terytorialnej i nie dają się redukować do jednego resortu. Dopełnieniem tej zmiany jest rosnące znaczenie ujęć ludziocentrycznych (human security), które akcentują bezpieczeństwo jednostek i wspólnot jako kluczowe kryterium oceny polityk publicznych. Raport UNDP z 1994 r. wprowadził pojęcie „human security”, przesuwając ciężar interpretacyjny z ochrony terytorium na ochronę człowieka i jego podstawowych warunków życia¹²⁴. Ujęcie to sprzyja interpretacji bezpieczeństwa wewnętrznego jako obszaru odporności społecznej i państwowej (np. zdrowie publiczne, bezpieczeństwo środowiskowe), ale jednocześnie uwidacznia jego powiązania z otoczeniem zewnętrznym (globalne łańcuchy dostaw, migracje, ryzyka transgraniczne). W konsekwencji rośnie znaczenie podejścia, w którym bezpieczeństwo wewnętrzne i zewnętrzne są rozumiane jako współzależne komponenty jednej polityki bezpieczeństwa: bezpieczeństwo zewnętrzne chroni podstawy istnienia państwa (suwerenność, integralność), a bezpieczeństwo wewnętrzne – podstawy sprawności państwa i spójności społecznej, bez których odstraszanie i obrona tracą oparcie materialne i legitymizacyjne.

Bezpieczeństwo zewnętrzne odnosi się do zdolności państwa do ochrony suwerenności, integralności terytorialnej oraz interesów w środowisku międzynarodowym. W praktyce jego „logika” opiera się na trzech filarach: odstraszaniu i obronie, aktywności sojuszniczej oraz dyplomacji (w tym budowie koalicji i utrzymaniu korzystnego porządku międzynarodowego). W strategii państwowej ten wymiar jest ujmowany nie tylko jako reakcja na zagrożenia militarne, lecz także jako kształtowanie środowiska bezpieczeństwa poprzez współpracę w organizacjach i formatach wielostronnych. Z perspektywy Rzeczypospolitej Polskiej kluczową determinantą bezpieczeństwa zewnętrznego pozostaje zakotwiczenie w strukturach sojuszniczych. Sojusz Północnoatlantycki (NATO) opiera zbiorową obronę na art. 5 Traktatu Północnoatlantyckiego, zgodnie z którym zbrojny atak na jednego członka jest traktowany jako atak na wszystkich, uruchamiając zobowiązanie do

¹²⁴ UNDP, Human Development Report 1994, 1994.

udzielenia pomocy (z zakresem działań pozostawionym decyzji państw sojuszu). W ujęciu systemowym oznacza to, że bezpieczeństwo zewnętrzne nie jest wyłącznie funkcją narodowego potencjału militarnego, lecz także funkcją wiarygodności sojuszu, interoperacyjności i zdolności do współdziałania. Równolegle, członkostwo w Unii Europejskiej wzmacnia zewnętrzny wymiar bezpieczeństwa przez instrumenty polityczne, prawne i gospodarcze, a ponadto przez klauzule wzajemnej pomocy. Art. 42 ust. 7 Traktatu o Unii Europejskiej (tzw. klauzula wzajemnej obrony) stanowi zobowiązanie państw członkowskich do udzielenia pomocy i wsparcia w przypadku zbrojnej napaści na terytorium jednego z nich, przy jednoczesnym zastrzeżeniu spójności z zobowiązaniami wynikającymi z NATO dla państw należących do sojuszu¹²⁵. Ten element jest istotny również w analizie relacji wewnętrzne-zewnętrzne, ponieważ pokazuje „wielowarstwowość” gwarancji bezpieczeństwa: państwo korzysta równolegle z mechanizmów wojskowych i polityczno-instytucjonalnych. Jednocześnie strategie i dokumenty programowe Polski podkreślają, że bezpieczeństwo zewnętrzne obejmuje nie tylko obronę terytorium, ale także aktywność w misjach i operacjach międzynarodowych oraz współpracę na forach organizacji międzynarodowych (w tym z Organizacją Narodów Zjednoczonych). Taką logikę można odnaleźć w Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, która akcentuje znaczenie członkostwa w NATO i UE jako ram wzmacniających bezpieczeństwo w zmieniającym się środowisku międzynarodowym.

Bezpieczeństwo wewnętrzne obejmuje te obszary aktywności państwa, które służą utrzymaniu porządku konstytucyjnego, bezpieczeństwa powszechnego oraz zdolności do ochrony życia i zdrowia ludności, mienia i środowiska, a także stabilności instytucji publicznych. Jego specyfika polega na tym, że operuje przede wszystkim w przestrzeni krajowej, ale coraz częściej reaguje na czynniki pochodzące z zewnątrz (cyberataki, presja migracyjna, przestępczość transgraniczna, operacje wpływu). W dokumentach polskich bezpieczeństwo wewnętrzne jest ujmowane szeroko – jako domena obejmująca m.in. porządek publiczny, ratownictwo, bezpieczeństwo zdrowotne, migracyjne, ekonomiczne czy informacyjne – co wprost wynika z przyjęcia całościowego podejścia do bezpieczeństwa oraz wyodrębniania

¹²⁵ NATO, The North Atlantic Treaty, 1949.

licznych sektorów bezpieczeństwa narodowego, w tym sektorów „transsektorowych” (np. cyberbezpieczeństwo, antyterroryzm). Z perspektywy systemowej oznacza to konieczność spójnego łączenia instrumentów ochronnych (porządkowych i ratowniczych) oraz zasobów wsparcia (infrastrukturalnych, gospodarczych i społecznych), ponieważ bez nich bezpieczeństwo wewnętrzne nie jest trwałe. Znaczenie wewnętrznego wymiaru bezpieczeństwa wyraźnie podkreśla również perspektywa unijna. Strategia EU Security Union Strategy wskazuje, że środowisko zagrożeń w UE ewoluuje w stronę coraz bardziej złożonych, transgranicznych i międzysektorowych ryzyk, co wzmacnia potrzebę ściślejszej współpracy państw członkowskich w zakresie bezpieczeństwa¹²⁶. Ten sposób diagnozowania problemu jest ważny dla rozróżnienia wewnętrzne-zewnętrzne: wiele zagrożeń „wewnętrznych” ma bowiem genezę zewnętrzną lub jest katalizowanych przez zależności międzynarodowe (np. ekonomiczne i technologiczne). Dodatkowo, art. 222 Traktatu o funkcjonowaniu Unii Europejskiej (tzw. klauzula solidarności) przewiduje wspólne działania UE i państw członkowskich w przypadku ataku terrorystycznego lub klęski żywiołowej/katastrofy spowodowanej przez człowieka, przy mobilizacji instrumentów pozostających w dyspozycji Unii, w tym środków wojskowych udostępnionych przez państwa członkowskie. Z perspektywy bezpieczeństwa wewnętrznego jest to kluczowe: wskazuje na możliwość „zewnętrznego wsparcia” dla reagowania na kryzysy typowo krajowe, a jednocześnie potwierdza, że granica między bezpieczeństwem wewnętrznym a zewnętrznym może być funkcjonalnie przekraczana w ramach uzgodnionych mechanizmów prawnych.

Najsilniejszym czynnikiem erozji tradycyjnego podziału bezpieczeństwa na wewnętrzne i zewnętrzne jest wzrost znaczenia zagrożeń hybrydowych, cybernetycznych i informacyjnych. Ich istotą jest łączenie różnorodnych środków (od presji ekonomicznej po działania w cyberprzestrzeni i manipulację informacją) w sposób skoordynowany, często „poniżej progu” otwartej agresji zbrojnej, tak, aby przeciążać instytucje państwa i osłabiać spójność społeczną. Dokumenty unijne ujmują hybrydowość jako oddziaływanie wykorzystujące podatności, służące wywoływaniu szkód bez formalnej eskalacji do działań wojennych, z zastosowaniem metod

¹²⁶ Komisja Europejska, EU Security Union Strategy (COM/2020/605 final), 2020.

konwencjonalnych i niekonwencjonalnych w wielu domenach¹²⁷. W tym kontekście wyraźnie widać zbieżność myślenia UE i NATO. EU Strategic Compass for Security and Defence akcentuje potrzebę wzmocnienia odporności i zdolności przeciwdziałania zagrożeniom hybrydowym, cyberatakami oraz zewnętrznej manipulacji i ingerencji informacyjnej, wskazując m.in. na wykorzystywanie migracji nieregularnej jako narzędzia presji, lawfare oraz przymus ukierunkowany na bezpieczeństwo ekonomiczne i energetyczne. Z kolei NATO Strategic Concept 2022 podkreśla komplementarność trzech zadań podstawowych (odstraszanie i obrona; zapobieganie kryzysom i zarządzanie kryzysowe; bezpieczeństwo kooperacyjne) oraz akcentuje rozwijanie odporności zbiorowej i przewagi technologicznej jako warunku realizacji tych zadań¹²⁸.

Implikacja dla rozróżnienia wewnętrzne-zewnętrzne jest zasadnicza: zagrożenia hybrydowe mają jednocześnie wektor zewnętrzny (źródło, sprawca, interes geopolityczny) i skutek wewnętrzny (dezorganizacja usług publicznych, polaryzacja społeczna, presja na instytucje, utrata zaufania). Taki mechanizm sprawia, że bezpieczeństwo zewnętrzne nie może ograniczać się do klasycznych instrumentów militarnych, a bezpieczeństwo wewnętrzne nie może być traktowane jako domena wyłącznie administracyjno-porządkowa. Wymaga to wspólnej świadomości sytuacyjnej, kompatybilnych procedur współdziałania oraz zdolności do ochrony i odtwarzania funkcji krytycznych państwa. W polskiej perspektywie strategicznej znajduje to odzwierciedlenie w akcentowaniu integracji zarządzania bezpieczeństwem narodowym oraz w traktowaniu bezpieczeństwa państwa i obywateli jako filaru obejmującego m.in. zarządzanie oraz odporność (przy jednoczesnym utrzymaniu odrębnego filaru odnoszącego się do miejsca Polski w systemie bezpieczeństwa międzynarodowego). Innymi słowy: państwo opisuje własne bezpieczeństwo jako układ, w którym wymiar wewnętrzny i zewnętrzny są równoległymi punktami odniesienia dla jednej strategii.

Z punktu widzenia konstrukcji systemu bezpieczeństwa narodowego rozróżnienie bezpieczeństwa wewnętrznego i zewnętrznego pozostaje użyteczne, ale w sensie metodologicznym powinno być traktowane jako

¹²⁷ European External Action Service, Countering Hybrid Threats, 2022.

¹²⁸ NATO, Strategic Concept (Madryt, 29.06.2022), 2022.

rozdzielenie funkcji, a nie jako rozdzielenie „światów instytucjonalnych”. Po stronie bezpieczeństwa zewnętrznego dominują instrumenty odstraszania i obrony oraz mechanizmy współpracy sojuszniczej (w tym zobowiązania i planowanie w ramach NATO, a także mechanizmy wsparcia w UE). Po stronie bezpieczeństwa wewnętrznego dominują instrumenty ochrony ludności, porządku publicznego i ciągłości funkcjonowania państwa, ale ich efektywność jest coraz częściej zależna od zdolności do przeciwdziałania czynnikom o charakterze transgranicznym (cyber, wpływ informacyjny, przestępczość międzynarodowa, presja gospodarcza). W warunkach zagrożeń wielodomenowych „węzłem” łączącym oba wymiary staje się odporność: zdolność państwa i społeczeństwa do utrzymania funkcji krytycznych, szybkiego odtwarzania zdolności i redukcji podatności. Jest to podejście widoczne równoległe w dokumentach NATO i UE, które traktują odporność jako warunek skutecznego odstraszania i zarządzania kryzysowego. Dla analizy systemowej oznacza to, że ocena „sprawności” bezpieczeństwa wewnętrznego i zewnętrznego nie powinna koncentrować się wyłącznie na katalogu instytucji, lecz na jakości sprzężeń: przepływie informacji, zdolności do wspólnego planowania i ćwiczeń, kompatybilności procedur oraz zdolności do uruchamiania zasobów w sytuacjach niejednoznacznych (w szczególności poniżej progu formalnych stanów nadzwyczajnych lub progu otwartej agresji). W tej perspektywie rozdzielenie wewnętrzne-zewnętrzne zachowuje znaczenie porządkujące, ale strategicznie kluczowa staje się integracja i zdolność adaptacyjna państwa – tak, aby bezpieczeństwo zewnętrzne i wewnętrzne wzajemnie się wzmacniały, a nie konkurowały o zasoby i priorytety.

Rozdział II.

Istota i uwarunkowania zarządzania kryzysowego

2.1. Koncepcja i zakres zarządzania kryzysowego

Zarządzanie kryzysowe stanowi kluczowy element systemu bezpieczeństwa publicznego i narodowego, umożliwiający państwu oraz innym podmiotom skuteczne przygotowanie się na różnego rodzaju zagrożenia, minimalizowanie ich skutków, a w razie wystąpienia kryzysu – efektywne reagowanie i szybkie przywracanie normalnego funkcjonowania społeczeństwa i gospodarki. We współczesnym świecie zagrożenia o charakterze kryzysowym stają się coraz bardziej powszechne, według danych ONZ, w latach 2000-2019 odnotowano na świecie 7 348 poważnych katastrof naturalnych (np. powodzi, cyklonów, trzęsień ziemi), podczas gdy w latach 1980-1999 było ich 4 212, co obrazuje istotny wzrost częstotliwości występowania sytuacji kryzysowych¹²⁹. Tendencja ta – w dużej mierze wynikająca ze wzrostu liczby ekstremalnych zjawisk pogodowych i innych zagrożeń – podkreśla znaczenie efektywnego zarządzania kryzysowego na wszystkich szczeblach.

Pojęcia kryzys i sytuacja kryzysowa często bywają używane zamiennie, jednak w literaturze przedmiotu wskazuje się na istotne rozróżnienia między nimi. Kryzys – w ogólnym ujęciu – to nagłe lub narastające zdarzenie, zagrażające życiu, zdrowiu, mieniu bądź środowisku, przeciwstawienie się któremu wymaga zaangażowania sił i środków przekraczających zwykłe, lokalne możliwości. Kryzys ma zatem charakter wyjątkowy i przełomowy

¹²⁹ United Nations Office for Disaster Risk Reduction (UNDRR) – The Human Cost of Disasters: An overview of the last 20 years (2000-2019), Geneva, United Nations, 2020.

– charakteryzuje się elementem zaskoczenia, presją czasu oraz ryzykiem utraty kontroli nad rozwijającą się sytuacją. Istotą kryzysu jest zachwianie dotychczasowej równowagi systemu, groźba przerwania normalnego cyklu funkcjonowania, wymagająca podjęcia zdecydowanych działań zaradczych¹³⁰. Przykładowo, Władysław Kopaliński definiował kryzys jako moment przełomu i decydujący zwrot w przebiegu danego procesu¹³¹. Inne ujęcie opisuje kryzys jako kulminacyjną fazę narastającej sytuacji zagrożenia, powstającą na skutek niespodziewanych okoliczności i wiążącą się z odczuciem utraty kontroli. Z kolei Hermann klasycznie wskazywał trzy elementy kryzysu (w kontekście politycznym): nagłość, wysoki stopień zagrożenia cenionych wartości oraz ograniczony czas na decyzje – cechy te dobrze oddają naturę kryzysów również we współczesnym ujęciu zarządzania bezpieczeństwem¹³².

Sytuacja kryzysowa natomiast to szersze pojęcie, obejmujące całość okoliczności i zdarzeń prowadzących do wystąpienia kryzysu oraz towarzyszących mu uwarunkowań. Uważa się, że każda sytuacja kryzysowa może (choć nie musi) wygenerować kryzys, natomiast każdy kryzys jest zawsze zawarty w pewnej sytuacji kryzysowej. Innymi słowy, kryzys jest kulminacyjnym etapem sytuacji kryzysowej – najbardziej dramatyczną jej fazą – lecz sytuacja kryzysowa może istnieć i rozwijać się także przed osiągnięciem tego punktu krytycznego (i potencjalnie może zostać opanowana, zanim przerozdzi się w pełnoobjawowy kryzys). Jak ujmuje to Wiesław Otwinowski, „kryzys jest kulminacyjną fazą sytuacji kryzysowej. Każdy kryzys jest sytuacją kryzysową, lecz nie każda sytuacja kryzysowa jest fazą kryzysu”¹³³. Sytuację kryzysową możemy rozumieć jako zbiór okoliczności wewnętrznych i zewnętrznych, zakłócających normalne funkcjonowanie danego systemu (np. państwa, społeczności, organizacji) i wywołujących proces zmian, które mogą prowadzić do jakościowo nowego stanu tego systemu. Zazwyczaj sytuacja kryzysowa jest następstwem wystąpienia poważnego zagrożenia

¹³⁰ W. Otwinowski, Kryzys i sytuacja kryzysowa, *Przegląd Naukowo-Metodyczny Edukacja dla Bezpieczeństwa*, 2, s. 83-89.

¹³¹ W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa, 1968, s. 417.

¹³² C. Hermann, Some Consequences of Crisis Which Limit the Viability of Organizations, *Administrative Science Quarterly*, 8(1), 1963, s. 61-82. <https://doi.org/10.2307/2390887>

¹³³ W. Otwinowski, Kryzys i sytuacja kryzysowa, *Przegląd Naukowo-Metodyczny Edukacja dla Bezpieczeństwa*, 2, 2010, s. 83-89, s. 89.

– może to być katastrofa naturalna, awaria techniczna, atak terrorystyczny, poważne zamieszki społeczne, epidemia czy inne zdarzenie o dużej skali negatywnych skutków. Legalna definicja przyjęta w polskim porządku prawnym ujmuje sytuację kryzysową jako sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia znacznych rozmiarów lub środowiska, powodującą znaczne ograniczenia w działaniach właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków¹³⁴. Innymi słowy, sytuacja kryzysowa to taka sytuacja nadzwyczajna, w której rutynowe procedury i zasoby okazują się niewystarczające, przez co konieczne jest podjęcie specjalnych środków w trybie nadzwyczajnym.

Na potrzeby dalszych rozważań warto także rozgraniczyć pojęcia katastrofa, zdarzenie niepożądane oraz ryzyko, które często pojawiają się w kontekście kryzysów i zarządzania kryzysowego. Katastrofa (w kontekście klęski żywiołowej lub innego zdarzenia masowego) oznacza zwykle gwałtowne, niszczące zdarzenie, powodujące poważne straty w życiu lub zdrowiu ludzi, mieniu bądź środowisku na dużą skalę. Katastrofy charakteryzują się tym, że przekraczają zdolności danej społeczności lub systemu do samodzielnego poradzenia sobie – wymagają wsparcia z zewnątrz oraz uruchomienia nadzwyczajnych procedur ratunkowych¹³⁵. Przykładem katastrofy może być silne trzęsienie ziemi, rozległa powódź czy atak terrorystyczny o skutkach ogólnokrajowych. Zdarzenie niepożądane to termin używany na określenie wszelkich negatywnych incydentów, które zakłócają normalne działanie systemu, ale nie muszą osiągać skali sytuacji kryzysowej – mogą to być np. awarie infrastruktury, wypadki czy inne incydenty o ograniczonym zasięgu. Zdarzenia takie są typowym przedmiotem działań służb ratowniczych i porządkowych w trybie codziennym (np. pożar budynku, lokalna przerwa w dostawie prądu), dopiero gdy eskalują lub występują w kumulacji, mogą przerodzić się w sytuację kryzysową. Natomiast ryzyko to pojęcie z zakresu analizy zagrożeń oznaczające prawdopodobieństwo wystąpienia danego negatywnego zdarzenia oraz potencjalną skalę jego konsekwencji. Zarządzanie kryzysowe pozostaje w ścisłym związku z zarządzaniem ryzykiem

¹³⁴ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm., art. 3 ust.1).

¹³⁵ UNDRR (United Nations Office for Disaster Risk Reduction), *The Human Cost of Disasters: An overview of the last 20 years (2000-2019)*, Geneva, United Nations, 2020 (Raport – statystyki globalne dot. katastrof).

– identyfikacja i ocena ryzyka stanowi podstawę działań zapobiegawczych i przygotowawczych, mających na celu niedopuszczenie do rozwinięcia się sytuacji kryzysowych. Kryzys można zatem ująć jako punkt kulminacyjny (przesilenie) procesu narastania zagrożeń, wymagający pilnej reakcji pod presją czasu i często przy ograniczonej informacji, zaś sytuacja kryzysowa to szerszy stan zagrożenia i zakłócenia normalnego porządku, obejmujący okres przed, w trakcie i bezpośrednio po kryzysie. Katastrofa jest szczególnym przypadkiem sytuacji kryzysowej o kataklizmicznych skutkach, zdarzenie niepożądane – potencjalnym zarzewiem kryzysu o mniejszej skali, a ryzyko – miernikiem prawdopodobieństwa i potencjału wystąpienia tych zjawisk. Zrozumienie tych definicji i zależności między nimi jest punktem wyjścia do dalszych rozważań nad zarządzaniem kryzysowym.

W ujęciu teoretycznym pojęcie zarządzania kryzysowego pojawiło się w literaturze stosunkowo późno – badacze organizacji zaczęli go używać dopiero pod koniec lat 60. XX w., wraz ze wzrostem zainteresowania wpływem otoczenia na funkcjonowanie przedsiębiorstw w warunkach kryzysu¹³⁶. Od tego czasu wypracowano szereg definicji zarządzania kryzysowego, różniących się akcentami i zakresem. Ogólnie rzecz biorąc, termin ten odnosi się do zespołu działań kierowniczych związanych z reagowaniem na kryzysy lub zapobieganiem im. W literaturze przedmiotu spotkać można różne nazewnictwo – m.in. zarządzanie kryzysem, zarządzanie w kryzysie, zarządzanie sytuacją kryzysową, zarządzanie antykryzysowe – choć znaczeniowo dotyczą one zbliżonych zagadnień. W niniejszej pracy autorzy posługują się terminem zarządzanie kryzysowe w najszerszym znaczeniu, obejmującym zarówno fazy przed wystąpieniem kryzysu (prewencja, przygotowanie), jak i działania w trakcie kryzysu oraz po jego ustąpieniu (reakcja, odtwarzanie).

W tabeli 1 zestawiono definicje zarządzania kryzysowego sformułowane przez autorów polskich i zagranicznych oraz w ustawie, co pozwala ukazać wielowymiarowość tego pojęcia.

¹³⁶ A. Bieńkowska, Z. Kral, A. Zabłocka-Kluczka, *Istota i ewolucja zarządzania kryzysowego*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, 1092, 2005, s. 25-32.

Tabela 1. Ujęcia definicyjne zarządzania kryzysowego w literaturze i prawie

Źródło	Definicja zarządzania kryzysowego (wybrane ujęcie)
W. Crandall, M. L. Menefee (1996)	Proces radzenia sobie z trudnościami, które mogą zagrozić istnieniu organizacji lub jej kondycji finansowej (tj. działania podejmowane w obliczu sytuacji stanowiących zagrożenie dla przetrwania organizacji) ¹³⁷ .
U. Krystek (1987)	Działalność niezbędna do pokonania sytuacji zagrażającej egzystencji organizacji, szczególna forma zarządzania, proces kierowania rozpoczynający się z chwilą dostrzeżenia i rozpoznania kryzysu w organizacji ¹³⁸ .
M. Armstrong (1997)	Proces rozwiązywania nagłych (kryzysowych) sytuacji w sposób zorganizowany – poprzez planowanie, organizowanie, kierowanie i kontrolowanie szeregu współzależnych operacji ¹³⁹ .
S. Fink (2000)	Sztuka ograniczania ryzyka i niepewności w taki sposób, aby pozwolić organizacji osiągnąć większą kontrolę nad jej własnym losem ¹⁴⁰ .
Ustawa o zarządzaniu kryzysowym (2007)	Działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, polegająca na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejścia nad nimi kontroli poprzez planowane działania, reagowaniu w przypadku ich wystąpienia oraz usuwaniu ich skutków i odtwarzaniu zasobów i infrastruktury krytycznej ¹⁴¹ .

Źródło: opracowanie własne.

Jak wynika z powyższych definicji, zarządzanie kryzysowe bywa ujmowane niekiedy wąsko – np. jako proces reagowania na kryzys w organizacji w celu zapewnienia jej przetrwania – a niekiedy szerzej, jako całościowa sztuka i proces ograniczania ryzyka i negatywnych skutków zdarzeń nadzwyczajnych. W definicjach anglosaskich często podkreśla się aspekt procesowy (ciąg działań) oraz decyzyjny w obliczu zagrożenia, np. Crandall i Menefee traktują zarządzanie kryzysowe jako proces radzenia sobie z poważnymi

¹³⁷ W. Crandall, M. L. Menefee, Crisis Management in the Midst of Labor Strife: Preparing for the Worst, S.A.M. Advanced Management Journal, 61(1), 1996.

¹³⁸ U. Krystek, Unternehmenskrisen. Beschreibung, Vermeidung und Bewältigung überlebenskritischer Prozesse in Unternehmen, Gabler GmbH, Wiesbaden, 1987.

¹³⁹ M. Armstrong, Jak być lepszym menedżerem, Dom Wydawniczy ABC, Warszawa, 1997.

¹⁴⁰ S. Fink, Crisis Management. Planning for the Inevitable, An Authors Guild Backinprint.com Edition, Lincoln, iUniverse.com, Inc., 2000.

¹⁴¹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r., Nr 89, poz. 590 z późn. zm., art. 3 ust. 1).

trudnościami zagrażającymi organizacji. Polskie ujęcia, zwłaszcza w kontekście sektora publicznego, akcentują udział organów władzy publicznej i działania związane z bezpieczeństwem publicznym. Można zatem stwierdzić, że zarządzanie kryzysowe jest dziedziną interdyscyplinarną, leżącą na pograniczu nauk o bezpieczeństwie, nauk o zarządzaniu oraz nauk prawnych i administracyjnych, i obejmuje wszelkie działania podejmowane w celu zapobieżenia kryzysom, przygotowania na wypadek ich wystąpienia, efektywnej reakcji w trakcie kryzysu oraz odbudowy po kryzysie.

Poniżej omówiono trzy główne ujęcia zarządzania kryzysowego spotykane w literaturze: jako proces cykliczny, jako funkcja administracji publicznej, oraz jako element wielopodmiotowego governance związanego z bezpieczeństwem publicznym.

Jednym z dominujących paradygmatów jest postrzeganie zarządzania kryzysowego jako cyklicznego procesu obejmującego kolejne fazy działań przed, w trakcie i po wystąpieniu kryzysu. Klasyczny model – wywodzący się z praktyki zarządzania sytuacjami nadzwyczajnymi (emergency management) – dzieli cały cykl na cztery podstawowe fazy: zapobieganie (mitigation/prevention), przygotowanie (preparedness), reagowanie (response) oraz odbudowę (recovery). Fazy te tworzą zamknięty krąg ciągłego doskonalenia: po przejściu fazy odbudowy następuje wyciąganie wniosków i usprawnianie działań zapobiegawczych przed kolejnymi potencjalnymi zagrożeniami¹⁴². Model ten przedstawiony na rysunku 5 jest często prezentowany graficznie jako cykl zarządzania kryzysowego, co podkreśla ciągły i iteracyjny charakter całego procesu.

¹⁴² Z. Ciekanowski, S. Krysiński, Zarządzanie kryzysowe w Polsce w sytuacjach zagrożeń niemilitarnych jako sposób umacniania państwa, Wydawnictwo Państwowej Wyższej Szkoły Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza, 2014.



Rysunek 5. Cykl zarządzania kryzysowego – cztery podstawowe fazy działań: zapobieganie, przygotowanie, reagowanie, odbudowa

Źródło: opracowanie własne.

Tabela 2 przedstawia syntetyczne zestawienie czterech głównych faz cyklu zarządzania kryzysowego wraz z przykładami typowych działań podejmowanych w każdej z nich (na podstawie literatury i dobrych praktyk). Należy podkreślić, że poszczególne fazy nie są od siebie całkowicie odseparowane – często nakładają się na siebie (np. pewne działania odbudowy rozpoczynają się jeszcze w trakcie reagowania), a także nie mają sztywno określonych granic czasowych. Mimo to podział ten jest użyteczny analitycznie i organizacyjnie, gdyż pozwala uporządkować zadania oraz kompetencje w całym procesie radzenia sobie z kryzysami.

Tabela 2. Fazy zarządzania kryzysowego i przykładowe typy działań

Faza	Charakterystyka i przykładowe działania
Zapobieganie	Działania redukujące ryzyko wystąpienia kryzysu lub ograniczające jego skutki przed faktem. Obejmują m.in.: identyfikację zagrożeń i ocenę ryzyka (analizy zagrożeń dla danego obszaru, np. powodziowego, przemysłowego), planowanie prewencyjne (uwzględnianie zagrożeń w planach zagospodarowania przestrzennego, aby uniknąć budowania np. na terenach zalewowych), wdrażanie środków ochronnych (inwestycje techniczne, takie jak wały przeciwpowodziowe, zbiorniki retencyjne, systemy przeciwpowodziowe), monitoring i wczesne ostrzeżenie (systemy detekcji zagrożeń – czujniki, radary pogodowe, obserwacje hydrologiczne itp.), działania edukacyjne (kampanie informacyjne zwiększające świadomość zagrożeń w społeczeństwie).
Przygotowanie	Działania budujące gotowość na wypadek kryzysu. Kluczowe jest opracowanie i aktualizacja planów zarządzania kryzysowego na różnych szczeblach (gminnych, powiatowych, wojewódzkich) oraz procedur reagowania na określone scenariusze. Ponadto faza ta obejmuje organizację systemu: tworzenie i utrzymanie struktur oraz zasobów (centra kryzysowe, magazyny sprzętu i rezerw, alternatywne środki łączności), ustanowienie systemów ostrzegania i alarmowania ludności, przygotowanie systemu łączności i wymiany informacji między służbami, zapewnienie szkolenia i ćwiczeń dla personelu zaangażowanego w reagowanie (ćwiczenia ratownicze, gry decyzyjne, treningi sztabowe) w celu testowania planów i podnoszenia kompetencji. Ważnym elementem jest również gromadzenie rezerw finansowych i materiałowych na sytuacje kryzysowe (zgodnie z wymogami prawnymi, np. obowiązkowa rezerwa budżetowa w JST).
Reagowanie	Działania bezpośrednio podczas trwania sytuacji kryzysowej, mające na celu opanowanie zagrożenia i ratowanie życia oraz mienia. Obejmują aktywację centrów i zespołów kryzysowych oraz postawienie służb w stan gotowości 24/7. Następuje alarmowanie i informowanie ludności (uruchomienie syren, wysyłanie komunikatów SMS, nadawanie alertów przez media) oraz zarządzanie ewakuacją z obszarów zagrożonych, jeśli wymaga tego sytuacja. Równolegle prowadzone są akcje ratownicze: straż pożarna, policja, pogotowie, wojsko i inne służby realizują swoje zadania – gaszenie pożarów, uwalnianie uwięzionych osób, udzielanie pierwszej pomocy medycznej poszkodowanym, poszukiwanie zaginionych, zabezpieczanie uszkodzonej infrastruktury itd. Ważnym elementem jest ochrona porządku publicznego i mienia (zapobieganie panice, patrolowanie ewakuowanych obszarów, by uniknąć grabieży). Całość działań jest koordynowana przez odpowiednie struktury (np. sztab kryzysowy), które na bieżąco dokumentują sytuację, podejmują decyzje i przekazują polecenia wykonawcze. Trwa również bieżąca komunikacja kryzysowa – informowanie mediów i społeczeństwa o rozwijającej się sytuacji, instrukcjach bezpieczeństwa, zaleceniach i działaniach pomocowych. Istotą fazy reagowania jest szybkie opanowanie sytuacji – powstrzymanie dalszych szkód i zapobieżenie kolejnym ofiarom – oraz stworzenie warunków do przejścia w etap odbudowy.

Faza	Charakterystyka i przykładowe działania
Odbudowa	<p>Działania podejmowane po ustąpieniu bezpośredniego zagrożenia, skoncentrowane na usunięciu skutków kryzysu i przywróceniu normalnych warunków życia. W pierwszej kolejności realizowana jest krótkoterminowa odbudowa: przywrócenie podstawowych usług (energia, woda, komunikacja, transport) nawet prowizorycznymi środkami, zapewnienie poszkodowanym schronienia i opieki (organizacja tymczasowych miejsc zakwaterowania, dostarczanie żywności i leków), ocena szkód i strat (szacunki zniszczeń w infrastrukturze, strat materialnych, liczby poszkodowanych) jako podstawa do planowania pomocy. Następnie przystępuje się do długoterminowej odbudowy: naprawy lub odbudowy infrastruktury (drog, mostów, sieci energetycznych, wodociągów, budynków użyteczności publicznej, domów mieszkalnych) – często z wykorzystaniem nowoczesnych technologii i standardów zwiększających odporność na przyszłe zagrożenia, udzielania pomocy finansowej poszkodowanym (wypłata odszkodowań ubezpieczeniowych, zasiłków, funduszy pomocowych) oraz wsparcia społecznego (pomoc psychologiczna, programy socjalne dla utrzymania społeczności lokalnej). Równolegle prowadzone są działania na rzecz odtwarzania sił ratowniczych i zasobów zużytych podczas reagowania – uzupełnienie sprzętu, odnowienie rezerw, przywrócenie pełnej gotowości służb. Kończącym elementem fazy odbudowy jest ewaluacja działań i wyciągnięcie wniosków: sporządzenie raportów po akcji, analiza skuteczności podjętych decyzji, identyfikacja słabych punktów oraz aktualizacja planów kryzysowych i procedur na przyszłość. Ten proces uczenia się sprawia, że doświadczenia z kryzysu przekładają się na lepsze przygotowanie systemu na ewentualne kolejne zagrożenia.</p>

Źródło: opracowanie własne.

W każdym z etapów cyklu podejmowane są odmienne typy działań – od prewencji, przez gotowość, reakcję, po odbudowę – jednak wszystkie one składają się na kompleksowe zarządzanie kryzysowe. W literaturze podkreśla się, że pominięcie którejkolwiek z faz osłabia efektywność całego systemu¹⁴³. Na przykład zaniedbanie fazy zapobiegania zwiększa prawdopodobieństwo wystąpienia katastrofy, brak przygotowania skutkuje chaosem w reagowaniu, a niewłaściwa odbudowa (bez refleksji i ulepszeń) sprawia, że społeczność pozostaje równie podatna na kolejne kryzysy. Dlatego pełen cykl zarządzania kryzysowego powinien być traktowany jako ciągłe, iteracyjne działanie – po zakończeniu odbudowy następuje powrót do działań zapobiegawczych i przygotowawczych w oparciu o zdobyte doświadczenia, co zamyka i ponownie napędza koło zarządzania kryzysowego.

Faza zapobiegania polega na eliminowaniu lub redukowaniu prawdopodobieństwa wystąpienia sytuacji kryzysowej oraz ograniczaniu potencjalnych skutków zagrożeń, które mogą się pojawić. Obejmuje ona działania prewencyjne, takie jak identyfikacja zagrożeń, analiza i ocena ryzyka, wdrażanie środków ochronnych (np. budowa wałów przeciwpowodziowych, zabezpieczenia techniczne), a także edukację i uświadamianie społeczeństwa w zakresie właściwych zachowań i przygotowania na wypadek zagrożeń. Zapobieganie jest fundamentem całego cyklu – im skuteczniej zidentyfikujemy i zneutralizujemy potencjalne zagrożenia, tym rzadziej będziemy musieli reagować na realne kryzysy. Faza przygotowania obejmuje wszelkie działania planistyczne, organizacyjne i szkoleniowe podejmowane *ex ante*, aby zwiększyć gotowość na wypadek wystąpienia kryzysu. W ramach przygotowań opracowuje się plany zarządzania kryzysowego (na poziomie krajowym, regionalnym, lokalnym, a także w instytucjach czy przedsiębiorstwach), określające zadania, role i procedury na wypadek różnorodnych scenariuszy zagrożeń. Ważnym elementem jest tworzenie i utrzymywanie odpowiednich zasobów: rezerw materialnych (żywność, leki, sprzęt), systemów łączności i alarmowania, miejsc schronienia, a także szkolenie służb ratunkowych i administracji oraz ćwiczenia symulacyjne. Działania te mają na celu zapewnienie, że w chwili kryzysu zaangażowane podmioty będą

¹⁴³ M. J. Fagel, *Crisis management and emergency planning: preparing for today's challenges*, Boca Raton, CRC Press, 2014. <https://doi.org/10.1201/b16072>

wiedziały co robić i będą dysponowały środkami jak to zrobić. Faza reagowania to wszelkie działania podejmowane bezpośrednio po wystąpieniu kryzysu, mające na celu opanowanie sytuacji, ratowanie życia i zdrowia ludzi, ochronę mienia oraz ograniczenie dalszych szkód. W fazie tej uruchamia się centra zarządzania kryzysowego i sztaby operacyjne, wprowadza się procedury alarmowe, prowadzi akcje ratownicze, ewakuację zagrożonej ludności, udziela pomocy poszkodowanym. Charakterystyczna dla tej fazy jest praca pod presją czasu i w warunkach niepewności – często na podstawie niepełnych informacji, które napływają chaotycznie. Jak zauważa M. Clarke, jednym z największych wyzwań w trakcie rozwijającego się kryzysu jest przetworzenie ogromnej ilości informacji, tak aby kluczowi decydenci mieli właściwe dane na czas – przeciążenie informacyjne może prowadzić do utraty orientacji w sytuacji¹⁴⁴. Dlatego tak ważne w fazie reagowania jest skuteczne zarządzanie informacją i komunikacją (zarówno wewnątrz sztabów kryzysowych, jak i z ludnością oraz mediami), a także efektywna koordynacja wielu zaangażowanych służb i instytucji (straży pożarnej, policji, pogotowia, wojska, administracji, itd.). Faza odbudowy (odtworzenia) następuje po opanowaniu bezpośredniego zagrożenia i obejmuje działania zmierzające do przywrócenia normalnego funkcjonowania dotkniętej kryzysem społeczności, infrastruktury i instytucji. Działania te dzieli się na odbudowę krótkoterminową – polegającą na szybkim odtworzeniu podstawowych warunków życia (np. wznowienie dostaw wody, energii, komunikacji, zabezpieczenie dachu nad głową dla poszkodowanych) – oraz odbudowę długoterminową, która może trwać miesiące i lata, koncentrując się na rekonstrukcji zniszczonej infrastruktury, odbudowie gospodarczej regionu, kompensacji strat, wsparciu społecznemu i psychicznemu ofiar, itd. Ważnym aspektem tej fazy jest także wyciąganie wniosków – analiza przebiegu kryzysu i działań podjętych w jego trakcie, identyfikacja słabych punktów systemu oraz najlepszych praktyk. Wnioski te powinny następnie zostać wykorzystane do ulepszenia planów i środków w fazie zapobiegania i przygotowania, co zamyka cykl i podnosi odporność (resilience) na przyszłe zagrożenia.

¹⁴⁴ M. Clarke, Charakterystyka zachowania się w kryzysie, maszynopis wykładu wygłoszonego w Brukseli w 1995.

Opisany powyżej cykl – znany też jako disaster management cycle – stanowi podstawowy kanon zarządzania kryzysowego zarówno w administracji publicznej, jak i w wielu organizacjach prywatnych. W literaturze przedmiotu podkreśla się, że wszystkie fazy są równie istotne dla skutecznego zarządzania kryzysem, choć w praktyce często najczęściej uwagi poświęca się fazie reagowania (bezpośrednia walka z kryzysem). Tymczasem zaniedbania na etapie prewencji czy przygotowań mogą skutkować znacznie poważniejszymi konsekwencjami kryzysu, zaś brak należytej odbudowy – utrzymaniem się negatywnych skutków kryzysu na długie lata. Dlatego współczesne podejścia kładą nacisk na holistyczne traktowanie tego cyklu oraz na włączanie w proces zarządzania kryzysowego różnych podmiotów.

Drugie istotne ujęcie traktuje zarządzanie kryzysowe jako funkcję zarządzania publicznego i integralną część polityki bezpieczeństwa państwa. W tym kontekście zarządzanie kryzysowe jest postrzegane jako zadanie organów władzy publicznej na wszystkich szczeblach – od rządu centralnego, poprzez władze wojewódzkie i samorząd lokalny, aż po organy gminne – mające na celu ochronę obywateli i infrastruktury przed skutkami sytuacji kryzysowych. Jak stwierdza M. Cabaj, zarządzanie kryzysowe w administracji stanowi integralną część zarządzania bezpieczeństwem narodowym oraz odgrywa zasadniczą rolę w rozwiązywaniu – pod presją czasu – sytuacji kryzysowych groźnych dla bezpieczeństwa¹⁴⁵.

W modelu administracji publicznej zarządzanie kryzysowe obejmuje cały zestaw działań planistycznych, organizacyjnych i decyzyjnych realizowanych przez wyspecjalizowane struktury państwowe. Należą do nich m.in.: centrum zarządzania kryzysowego na poziomie krajowym (w Polsce – Rządowe Centrum Bezpieczeństwa), wojewódzkie, powiatowe i gminne zespoły zarządzania kryzysowego, a także różnego rodzaju służby, inspekcje i straże (Państwowa Straż Pożarna, Policja, Państwowe Ratownictwo Medyczne, inspekcje sanitarne, weterynaryjne itd.), które wchodzi w skład systemu reagowania kryzysowego. Ponadto w ramach administracji publicznej opracowywane są formalne plany zarządzania kryzysowego (na szczeblu krajowym i niższych), które są regularnie aktualizowane i koordynowane

¹⁴⁵ M. Cabaj, Zarządzanie kryzysowe – integralna część bezpieczeństwa narodowego, *Studia z zakresu prawa, administracji i zarządzania UKW*, 6, 2014, s. 101-113.

między resortami i jednostkami samorządu¹⁴⁶. Zarządzanie kryzysowe jako funkcja administracji ma charakter koordynacyjno-decyzyjny. Oznacza to, że organy władzy (np. wojewoda, burmistrz) w sytuacji kryzysowej przejmują rolę koordynatorów działań wszystkich zaangażowanych podmiotów – wydają decyzje, uruchamiają odpowiednie procedury (np. alarmowanie ludności, ewakuacja, uruchomienie rezerw strategicznych), wprowadzają specjalne regulacje (czasem stan nadzwyczajny, jak stan klęski żywiołowej), a także współpracują z organizacjami pozarządowymi i sektorem prywatnym w niesieniu pomocy. Ustawa o zarządzaniu kryzysowym podkreśla, że zarządzanie kryzysowe jest elementem kierowania bezpieczeństwem narodowym i przypisuje odpowiedzialność za nie konkretnym organom administracji (m.in. premierowi, ministrom, wojewodom, wójtom) wraz z określeniem ich zadań. Definicja ustawowa wyraźnie uwypukla cykliczność działań administracji: od zapobiegania, przez przygotowanie, reagowanie, po odtwarzanie – co omawialiśmy wyżej. Należy zaznaczyć, że w sektorze publicznym zarządzanie kryzysowe jest silnie powiązane z prawodawstwem i regulacjami. Każde państwo posiada własne ramy prawne określające organizację systemu zarządzania kryzysowego – w Polsce jest to wspomniana ustawa z 2007 r. (wraz z późniejszymi nowelizacjami) oraz akty wykonawcze, a także ustawy sektorowe (np. o stanie klęski żywiołowej¹⁴⁷, o stanie wyjątkowym¹⁴⁸, o ochronie przeciwpożarowej¹⁴⁹, o obronie Ojczyzny¹⁵⁰ itp.), które razem tworzą swoisty mechanizm prawny reagowania kryzysowego. Administracja publiczna pełni tu rolę gwaranta, że w obliczu kryzysu istnieje gotowa struktura decyzyjna i prawna do podjęcia działań nadzwyczajnych.

W literaturze przedmiotu zarządzanie kryzysowe w administracji bywa traktowane jako element szerszego systemu zarządzania bezpieczeństwem wewnętrznym państwa lub wręcz jako osobna działalność publiczna obok takich funkcji jak zarządzanie strategiczne, finansowe czy operacyjne.

¹⁴⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 5, ust. 1, 3 i 5).

¹⁴⁷ Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62, poz. 558 z późn. zm).

¹⁴⁸ Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. Nr 113, poz. 985 z późn. zm).

¹⁴⁹ Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. z 1991 r. Nr 81, poz. 351 z późn. zm).

¹⁵⁰ Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655 z późn. zm).

Podkreśla się tu często potrzebę integralności systemu – tzn. włączenia zarządzania kryzysowego we wszystkie poziomy planowania rozwoju i bezpieczeństwa (zasada „comprehensive approach”)¹⁵¹. K. Sienkiewicz-Małyjurek i F. R. Krynojewski wskazują, że skuteczne zarządzanie kryzysowe musi angażować zarówno sektor publiczny, jak i prywatny oraz obywateli, i obejmować wszystkie typy zagrożeń przy zastosowaniu jednej spójnej strategii. Oznacza to m.in., że procedury kryzysowe powinny być kompatybilne w różnych resortach i na różnych szczeblach władzy, a społeczeństwo powinno być świadome swojej roli (np. przestrzeganie poleceń, samoorganizacja, podstawowe przygotowanie indywidualne). W ten sposób zarządzanie kryzysowe staje się nie tylko reakcją na zdarzenie, ale też elementem polityki publicznej budującym odporność państwa i społeczeństwa na zagrożenia.

Trzecie podejście akcentuje wielopodmiotowy i sieciowy charakter współczesnego zarządzania kryzysowego, wpisując go w kontekst tzw. governance (współrządzenia) w obszarze bezpieczeństwa publicznego. W dobie złożonych zagrożeń (katastrofy naturalne o transgranicznych skutkach, pandemie, zagrożenia hybrydowe, cyberataki, itp.) żaden pojedynczy podmiot – nawet państwo – nie jest w stanie samodzielnie zapobiec kryzysom ani ich opanować. Dlatego zarządzanie kryzysowe postrzega się coraz częściej jako proces kolektywny, wymagający współdziałania administracji rządowej, samorządów, służb profesjonalnych, sektora prywatnego (przedsiębiorstw, operatorów infrastruktury krytycznej), organizacji pozarządowych, społeczności lokalnych, mediów, a niekiedy także instytucji międzynarodowych. W literaturze mówi się wręcz, że zarządzanie kryzysowe jest tradycyjnym elementem governance, jednym z mechanizmów pozwalających instytucjom publicznym i społeczeństwu przeciwdziałać zagrożeniom¹⁵². Oznacza to odejście od wąskiego postrzegania go jako domeny sztabów kryzysowych, a uznanie, że jest to obszar współzarządzania, gdzie kluczowe znaczenie mają partnerstwa i sieci współpracy. Przykładowo, koncepcja odporności (resilience) społeczności podkreśla, że zdolność skutecznego reagowania na kryzysy zależy od poziomu zorganizowania i zaangażowania

¹⁵¹ K. Sienkiewicz-Małyjurek, F. R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Warszawa, Difin, 2010.

¹⁵² O. Reznikova, *National Resilience in a Changing Security Environment*, Kyiv, National Institute for Strategic Studies, 2022.

wielu aktorów: lokalnego biznesu (który może dostarczać zasoby i usługi), organizacji wolontariackich i charytatywnych (udzielających wsparcia poszkodowanym), mediów i platform społecznościowych (ważnych dla komunikacji kryzysowej), środowisk naukowych (dostarczających ekspertyz, prognoz, innowacyjnych narzędzi, itp.). W tym ujęciu zarządzanie kryzysowe staje się częścią wielostronnego systemu bezpieczeństwa publicznego, gdzie administracja pełni rolę koordynatora i regulatora, ale efektywność działań zależy od sprawnego przepływu informacji i współpracy ze wszystkimi pozostałymi interesariuszami.

Na poziomie międzynarodowym również dostrzega się ten aspekt – organizacje takie jak NATO czy Unia Europejska traktują zarządzanie kryzysowe jako element szerszej architektury bezpieczeństwa, wymagający zintegrowanego podejścia polityczno-wojskowo-cywilnego¹⁵³. Przykładowo NATO zalicza crisis management do swoich podstawowych zadań obok obrony kolektywnej i bezpieczeństwa kooperacyjnego, podkreślając potrzebę komplementarności środków politycznych, militarnych i cywilnych w reagowaniu na współczesne kryzysy. Z kolei ONZ promuje ideę disaster risk governance, wskazując, że w obliczu systemowych zagrożeń konieczne jest włączenie zarządzania ryzykiem katastrof w ogólny system rządzenia i planowania rozwoju¹⁵⁴.

W ujęciu governance ważna staje się partycypacja społeczna w zarządzaniu kryzysowym. Społeczeństwo nie jest już traktowane jedynie jako bierny odbiorca poleceń czy ofiara wymagająca pomocy, ale również jako aktywny uczestnik – np. mieszkańcy mogą samorzutnie organizować pomoc sąsiedzką, społeczności lokalne mogą tworzyć plany awaryjne, a obywatele poprzez media społecznościowe często jako pierwsi przekazują informacje o sytuacji w terenie (tzw. crowdsourcing informacji kryzysowej). Dlatego nowoczesne zarządzanie kryzysowe obejmuje również zarządzanie komunikacją z ludnością oraz budowanie zaufania publicznego. Tylko wtedy, gdy obywatele ufają instytucjom i rozumieją zalecenia, można liczyć na sprawne wdrożenie działań (np. sprawna ewakuacja, stosowanie się do kwarantanny

¹⁵³ NATO, Crisis management, NATO, 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/crisis-management>, [dostęp: 22.09.2025].

¹⁵⁴ ONZ (UNISDR) – Sendai Framework for Disaster Risk Reduction 2015-2030. Geneva, UNDRR, 2015. (Ramowy program działania z Sendai 2015-2030).

podczas pandemii, itp.). Włączenie społeczeństwa w ten proces zwiększa też świadomość zagrożeń i skłonność do przygotowań na własną rękę (np. posiadanie domowych zestawów ratunkowych, ubezpieczeń, znajomość podstaw pierwszej pomocy). Zarządzanie kryzysowe w podejściu governance to zarządzanie siecią powiązań między wieloma aktorami, w którym kluczowe znaczenie ma koordynacja, współpraca i komunikacja. Kryzysy odsłaniają zależności między sektorami – np. awaria energetyczna wpływa na łączność i zaopatrzenie w wodę, kryzys zdrowotny (pandemia) oddziałuje na gospodarkę, edukację itd. – stąd efektywne przeciwdziałanie wymaga kompleksowego spojrzenia i współdziałania różnych instytucji. Zarządzanie kryzysowe jest tu elementem zarządzania publicznego w warunkach niepewności, które cechuje się koniecznością podejmowania decyzji przy niepełnych danych i dynamicznie zmieniających się okolicznościach. Niektórzy autorzy wskazują, że kształtowanie polityk publicznych powinno uwzględniać perspektywę ciągłego zagrożenia kryzysami – tzn. rezyliencja i gotowość kryzysowa powinny przenikać różne dziedziny zarządzania państwem (planowanie przestrzenne, politykę klimatyczną, politykę zdrowotną, edukację, itd.).

Zakres podmiotowy zarządzania kryzysowego odnosi się do tego, kto uczestniczy w procesie zarządzania sytuacjami kryzysowymi, zaś zakres przedmiotowy – czym jest zarządzane, czyli jakimi zasobami, wartościami i obszarami działania. Omówienie tych zakresów pozwala lepiej zrozumieć różnicę między zarządzaniem kryzysowym w sektorze publicznym a zarządzaniem kryzysem w organizacjach prywatnych, a także wskazać szczególne wyzwania stojące przed menedżerami kryzysowymi.

W administracji publicznej głównymi podmiotami odpowiedzialnymi za zarządzanie kryzysowe są – jak wspomniano – organy administracji rządowej i samorządowej z ustanowionymi strukturami sztabowymi. Na szczeblu centralnym w Polsce jest to m.in. Rada Ministrów (kierująca polityką bezpieczeństwa), Rządowy Zespół Zarządzania Kryzysowego z Premierem na czele, oraz Rządowe Centrum Bezpieczeństwa (RCB) jako organ pomocniczy zapewniający analizę i koordynację. Na poziomie terenowym rolę tę pełnią wojewodowie i wojewódzkie zespoły zarządzania kryzysowego, a niżej – starostowie i prezydenci miast (powiatowe/miejskie zespoły), wójtowie/burmistrzowie (gminne zespoły). Ponadto specjalne role pełnią służby ratownicze (Straż Pożarna, Policja, pogotowie ratunkowe), którym często

powierza się dowodzenie akcją ratunkową na miejscu zdarzenia. Wreszcie, jak podkreślono wcześniej, do kręgu podmiotów zalicza się także np. Siły Zbrojne (używane w sytuacjach kryzysowych, gdy inne siły są niewystarczające), podmioty prywatne (np. operatorów infrastruktury krytycznej, właścicieli zakładów – zobowiązanych do posiadania własnych planów awaryjnych) oraz organizacje pozarządowe (np. grupy poszukiwawczo-ratownicze, Polski Czerwony Krzyż, strażacy ochotnicy, grupy humanitarne). Współdziałanie tych wszystkich aktorów wymaga klarownych mechanizmów koordynacji – stąd w planach zarządzania kryzysowego dokładnie określa się strukturę dowodzenia i komunikacji. Zgodnie z zasadą subsydiarności, reagowanie odbywa się na najniższym możliwym szczeblu – tzn. drobne kryzysy lokalne obsługuje gmina/powiat własnymi siłami, a dopiero gdy ich skala przekracza możliwości, włącza się poziom wojewódzki lub krajowy. W organizacjach prywatnych (np. przedsiębiorstwach) zarządzanie kryzysem jest zwykle zadaniem kierownictwa firmy – często wyznacza się tzw. Crisis Management Team (Zespół Zarządzania Kryzysowego) złożony z menedżerów różnych działów (bezpieczeństwa, komunikacji, operacji, finansów), pod przewodnictwem prezesa lub innej osoby z najwyższego kierownictwa. Ich zadaniem jest przygotowanie firmy na różne scenariusze zakłóceń (np. plan ciągłości działania – Business Continuity Plan) oraz prowadzenie działań w razie kryzysu (awarii, skandalu wizerunkowego, nagłej utraty kluczowych zasobów). W sektorze prywatnym coraz bardziej docenia się rolę specjalistów od komunikacji kryzysowej (PR kryzysowy) – ponieważ dla firm kluczowe jest zarządzanie swoim wizerunkiem i relacjami z klientami, inwestorami podczas kryzysu¹⁵⁵. Należy jednak zaznaczyć, że zarządzanie kryzysowe w biznesie często różni się celem od zarządzania kryzysowego w administracji: celem firmy jest przetrwanie na rynku i ochrona wartości firmy (aktywów, dochodów, marki)¹⁵⁶, podczas gdy celem administracji jest ochrona życia, zdrowia obywateli i porządku publicznego. Te odmienne priorytety mogą wpływać na decyzje – np. firma może zdecydować o wycofaniu wadliwego produktu z rynku dla ratowania reputacji, co

¹⁵⁵ D. Tworzydło, A. Łaszyn, P. Szuba, Zarządzanie kryzysem w polskich przedsiębiorstwach. Podsumowanie 10 lat badań nad kryzysami, Rzeszów, Wydawnictwo Newsline, 2018.

¹⁵⁶ A. Bieńkowska, Z. Kral, A. Zabłocka-Kluczka, Istota i ewolucja zarządzania kryzysowego, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, 1092, 2005, s. 25-32.

jest działaniem kryzysowym biznesowym, ale nie ma odpowiednika w sektorze publicznym.

Analizując zagadnienie czym zarządza się w kryzysie, należy podkreślić, iż zakres przedmiotowy można ująć ogólnie jako trzy główne obszary: ludzie, zasoby, informacja. Po pierwsze, zarządzanie kryzysowe to zarządzanie bezpieczeństwem ludzi – ochrona życia i zdrowia jest nadrzędnym priorytetem. W sytuacji kryzysowej podejmuje się decyzje dotyczące ewakuacji ludności, udzielania pomocy medycznej, zapewnienia schronienia, zaopatrzenia w wodę, żywność i inne środki dla poszkodowanych. Po drugie, to zarządzanie zasobami materialnymi – obejmuje mobilizację i alokację sprzętu ratowniczego (np. pomp, łodzi, śmigłowców), środków transportu, pieniędzy (fundusze na akcje ratunkowe i odbudowę), oraz infrastruktury (np. przekierowanie dostaw energii, wykorzystanie budynków na schroniska). W warunkach kryzysu zasoby te są zwykle ograniczone, dlatego kluczowe jest szybkie ustalanie priorytetów i dystrybucja tam, gdzie potrzeby są największe. Po trzecie, to zarządzanie informacją – w czasie kryzysu rzetelna i szybka informacja bywa najcenniejszym „zasobem”. Decydenci muszą uzyskać jak najszybciej pełny obraz sytuacji (stąd rozwinięte systemy łączności, centra operacyjne, analizy danych), a społeczeństwo musi otrzymywać jasne komunikaty (ostrzegawcze, instruktażowe). Zarządzanie informacją obejmuje też przeciwdziałanie dezinformacji i plotkom, które w dobie mediów społecznościowych mogą się rozprzestrzeniać równie szybko co sam kryzys. Zacytowany wcześniej Clarke zwraca uwagę, że nadmiar nieprzefiltrowanych informacji może być paraliżujący – stąd potrzebne są procedury selekcji i wspomagania decyzji dla sztabów¹⁵⁷.

Przedmiotowy zakres zależy od rodzaju kryzysu: np. w kryzysie powodziowym zarządzamy pracą wałów przeciwpowodziowych, flotą pomp i worków z piaskiem, natomiast w kryzysie epidemicznym – dostawami leków, funkcjonowaniem szpitali, wdrażaniem ograniczeń sanitarnych. W każdym przypadku jednak wspólnym mianownikiem jest konieczność szybkiego przesuwania i użycia dostępnych sił i środków tam, gdzie są najbardziej potrzebne. Dlatego w zarządzaniu kryzysowym tak ważne jest posiadanie

¹⁵⁷ M. Clarke, Charakterystyka zachowania się w kryzysie, maszynopis wykładu wygłoszonego w Brukseli w 1995.

rezerw (rezerwowo sprzęt, fundusze, plany alternatywne) oraz możliwość eskalacji wsparcia – gdy lokalne zasoby się wyczerpią, powinny wkroczyć zasoby regionalne, krajowe, a nawet międzynarodowe (np. pomoc z UE lub od sojuszników).

Warto podkreślić, że podmiotowy i przedmiotowy wymiar zarządzania kryzysowego ściśle się ze sobą wiążą. Kto inny jest wiodącym podmiotem i czym innym zarządza się w kryzysie publicznym (np. powódź – wiodącym podmiotem będzie administracja państwowa, zarządzane są służby ratunkowe, infrastruktura, populacja regionu), a inaczej w kryzysie organizacji prywatnej (np. afera wizerunkowa firmy – wiodącym podmiotem jest zarząd firmy, zarządzane są informacje przekazywane mediom, działania PR, relacje z klientami). Niemniej zasady ogólne – takie jak potrzeba planu, koordynacji, szybkiego działania, komunikacji – pozostają podobne.

Istotne są różnice między zarządzaniem kryzysowym w administracji publicznej a zarządzaniem kryzysem w organizacjach (np. przedsiębiorstwach). Choć obie dziedziny dotyczą reagowania na sytuacje zagrożenia i zakłócenia, różnice wynikają z odmiennej specyfiki celów i uwarunkowań sektorów publicznego i prywatnego. W administracji publicznej zarządzanie kryzysowe, jak opisano, koncentruje się na ochronie ludności, mienia publicznego i porządku. Działania podejmowane są w imię dobra wspólnego, na podstawie prawa i w granicach uprawnień urzędowych. Struktury zarządzania kryzysowego są sformalizowane (ustawowe zespoły, plany), finansowane ze środków publicznych i rozliczane z zapewnienia bezpieczeństwa obywateli. Sukcesem jest minimalizacja strat społecznych i szybkie przywrócenie normalnego życia. W sektorze publicznym kryzysy często mają charakter sytuacji nadzwyczajnej (emergency), które mogą wymagać ogłoszenia stanów nadzwyczajnych i pociągać za sobą ograniczenie niektórych praw (np. czasowe ewakuacje, zakazy). Z kolei zarządzanie kryzysem w organizacjach prywatnych (czasem zwane corporate crisis management lub organizational crisis management) skupia się na przetrwaniu i kondycji danej organizacji. Kryzys w rozumieniu biznesowym może przybrać formę np. kryzysu finansowego (groźba bankructwa), kryzysu wizerunkowego (skandal, który podważa reputację firmy), awarii operacyjnej (przerwanie ciągłości działania, np. wskutek pożaru fabryki) czy konfliktu wewnętrznego. W takich sytuacjach zespół kryzysowy firmy dąży do ochrony kluczowych

wartości firmy – jej aktywów, wartości rynkowej, zaufania klientów i interesariuszy. W literaturze zarządzania podkreśla się, że zasadniczym celem jest zapewnienie przedsiębiorstwu przeżycia i niedopuszczenie do jego upadku. Działania kryzysowe firm obejmują np.: szybkie usuwanie usterek (jeśli produkt zawiódł – wycofanie wadliwej partii z rynku), przeprosiny i rekompensaty (gdy doszło do szkody klientów), kontrolę przekazu medialnego (aby ograniczyć szkody reputacyjne), mobilizację rezerw finansowych lub znalezienie inwestora ratunkowego. Firmy często angażują profesjonalistów PR w charakterze rzeczników kryzysowych, a także korzystają z usług doradców zewnętrznych (np. prawników, ekspertów technicznych) by opanować sytuację. Kluczowa różnica polega też na zakresie oddziaływania: kryzys przedsiębiorstwa najczęściej dotyka bezpośrednio głównie tę organizację (i ewentualnie jej klientów czy partnerów), natomiast kryzys publiczny (np. klęska żywiołowa) dotyczy całej społeczności lub znacznego obszaru. Stąd narzędzia i skala działań są inne. Firma może utrzymać kryzys w pewnej dozie prywatności (nie wszystkie działania kryzysowe są jawne, czasem wręcz próbuje się ograniczyć rozgłos), podczas gdy administracja działa zwykle pod lupą opinii publicznej i mediów, bo sprawy bezpieczeństwa są z natury publiczne.

Warto zaznaczyć, że te światy nie są całkiem rozłączne – w praktyce często się przenikają. Na przykład duża awaria przemysłowa (jak wyciek chemikaliów z zakładu) jest jednocześnie kryzysem przedsiębiorstwa i sytuacją kryzysową publiczną wymagającą interwencji władz. W takich sytuacjach władze publiczne i zarząd firmy muszą współpracować – administracja zarządza ewakuacją i zabezpiecza ludność, zaś firma dostarcza informacji o zagrożeniu, uruchamia własne służby i ponosi odpowiedzialność za szkody. Innym przykładem jest pandemia COVID-19 – zjawisko globalne, w którego zarządzanie byli zaangażowani zarówno rządzący (ustanawianie obostrzeń, organizacja opieki zdrowotnej), jak i przedsiębiorstwa (szybka zmiana trybu pracy, zabezpieczenie pracowników, utrzymanie łańcuchów dostaw) oraz całe społeczeństwo. Zarządzanie kryzysowe w administracji publicznej różni się od zarządzania kryzysem w organizacji prywatnej zakresem odpowiedzialności, priorytetami oraz ramami działania (legalnymi vs biznesowymi). Jednak w obu przypadkach wymagane są umiejętności przewodzenia w sytuacji presji, podejmowania decyzji pod niepewność,

komunikowania się w kryzysie oraz koordynowania wielodyscyplinarnych działań – co czyni z zarządzania kryzysowego odrębną dziedzinę wiedzy i praktyki.

Biorąc pod uwagę powyższy przegląd, na potrzeby niniejszej monografii przyjęto następującą własną definicję zarządzania kryzysowego: Zarządzanie kryzysowe to zorganizowany, ciągły proces realizowany przez uprawnione podmioty (przede wszystkim organy administracji publicznej we współpracy z innymi służbami, organizacjami i społecznością), obejmujący całość działań zmierzających do zapewnienia bezpieczeństwa w obliczu zagrożeń – od identyfikacji i redukcji ryzyka, poprzez przygotowanie planów i zasobów na wypadek kryzysu, skuteczne reagowanie w sytuacji kryzysowej, aż po odbudowę i odtworzenie normalnego funkcjonowania po kryzysie. Ta definicja podkreśla cykliczny charakter zarządzania kryzysowego (uwzględnia wszystkie fazy), jego podmiotowy aspekt (akcent na rolę organów publicznych, ale we współpracy z innymi), oraz przedmiotowy zakres (zarządzanie ryzykiem, zasobami i informacją w celu ochrony życia, zdrowia, mienia i środowiska). W dalszych częściach pracy termin „zarządzanie kryzysowe” będzie używany w tym szerokim znaczeniu, o ile kontekst nie będzie wymagał jego zawężenia do konkretnej domeny. Taka całościowa perspektywa pozwoli analizować zarówno zagadnienia teoretyczne, jak i praktyczne rozwiązania z zakresu nauk o bezpieczeństwie, odnoszące się do zapobiegania i radzenia sobie z kryzysami.

2.2. Zarządzanie kryzysowe w systemie nauk o bezpieczeństwie

Zarządzanie kryzysowe stanowi jeden z kluczowych obszarów badawczych w ramach nauk o bezpieczeństwie, zyskując status odrębnej specjalności naukowej tej dyscypliny¹⁵⁸. Jako dziedzina wiedzy koncentruje się na przygotowaniu, reagowaniu i odtwarzaniu funkcjonowania społeczeństwa i państwa w obliczu sytuacji kryzysowych – zdarzeń zagrażających życiu, mieniu, środowisku lub stabilności państwa. W odróżnieniu od rutynowe-

¹⁵⁸ J. W. Michniak, Zarządzanie kryzysowe jako specjalność w dyscyplinie naukowej – nauki o bezpieczeństwie, *Studia Bezpieczeństwa Narodowego*, 4(1), 2013, s. 69-85.

go zarządzania, zarządzanie kryzysowe dotyczy sytuacji nadzwyczajnych, charakteryzujących się wysokim poziomem niepewności, presją czasu oraz ryzykiem wystąpienia poważnych strat¹⁵⁹. W systemie nauk o bezpieczeństwie pełni ono rolę pomostową, łącząc zagadnienia bezpieczeństwa narodowego, wewnętrznego, publicznego i społecznego w spójny zakres badań i praktyki. Poniżej przedstawiono umiejscowienie zarządzania kryzysowego na tle różnych wymiarów bezpieczeństwa, jego interdyscyplinarny charakter, zakres przedmiotowy badań oraz główne paradygmaty naukowe i praktyczne podejścia. Omówiono także znaczenie tej subdyscypliny w edukacji wyższej i aktualnych badaniach naukowych.

Zarządzanie kryzysowe jest nierozdzielnie związane z zapewnianiem bezpieczeństwa państwa i obywateli na różnych poziomach. W kontekście bezpieczeństwa narodowego stanowi element przygotowania państwa na sytuacje zagrożeń niemilitarnych i hybrydowych, uzupełniając tradycyjne działania z obszaru obronności. Każdy nowoczesny system bezpieczeństwa narodowego obejmuje zarówno komponent militarny, jak i cywilny – ten drugi dotyczy właśnie reagowania kryzysowego na klęski żywiołowe, katastrofy techniczne, ataki terrorystyczne czy epidemie¹⁶⁰. Zarządzanie kryzysowe jest także integralną częścią bezpieczeństwa wewnętrznego, koncentrując się na ochronie porządku publicznego, życia i zdrowia obywateli oraz infrastruktury krytycznej w sytuacjach zagrożeń wewnętrznych (np. zamieszki, poważne wypadki, cyberataki). Poprzez planowanie i koordynację działań służb ratunkowych oraz administracji publicznej, zarządzanie kryzysowe przyczynia się do utrzymania ładu wewnętrznego państwa nawet w warunkach ekstremalnych¹⁶¹.

Istotne jest również powiązanie zarządzania kryzysowego z bezpieczeństwem publicznym i społecznym. Bezpieczeństwo publiczne odnosi się do powszechnego poczucia bezpieczeństwa obywateli w codziennym życiu, które może zostać zachwiane przez sytuacje kryzysowe, takie jak katastrofy

¹⁵⁹ M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>

¹⁶⁰ J. W. Michniak, Zarządzanie kryzysowe jako specjalność w dyscyplinie naukowej – nauki o bezpieczeństwie, *Studia Bezpieczeństwa Narodowego*, 4(1), 2013, s. 69-85.

¹⁶¹ A. Skrabacz, A. Pajka, B. Więckowski, Crisis Management as a Research Province of Security Science, *Roczniki Nauk Społecznych*, 52(1), 2024, s. 7-25. <https://doi.org/10.18290/rns2024.0010>

naturalne czy awarie przemysłowe. Sprawne zarządzanie kryzysowe minimalizuje skutki takich zdarzeń, przywracając normalne funkcjonowanie usług publicznych i porządku społecznego. Z kolei bezpieczeństwo społeczne (rozumiane jako odporność społeczeństwa na zagrożenia oraz ochrona jego podstawowych potrzeb i wartości) jest wzmacniane przez działania z zakresu zarządzania kryzysowego ukierunkowane na ochronę ludności i zapewnienie ciągłości infrastruktury krytycznej. Przykładowo, w sytuacji klęski żywiołowej zarządzanie kryzysowe koordynuje ewakuację ludności, organizację schronień, zaopatrzenie w wodę i żywność oraz pomoc medyczną – tym samym chroniąc integralność społeczeństwa i zapobiegając panice czy chaosowi¹⁶². Warto podkreślić, że zarządzanie kryzysowe w systemie bezpieczeństwa państwa działa zarówno w okresie pokoju, jak i podczas sytuacji szczególnych (stany nadzwyczajne, kryzysy polityczne czy konflikty poniżej progu wojny). Stanowi ono swoisty pomost między bezpieczeństwem zewnętrznym a wewnętrznym – gdy zagrożenia zewnętrzne (np. konflikty zbrojne, ataki terrorystyczne inspirowane z zagranicy) oddziałują na terytorium państwa, mechanizmy zarządzania kryzysowego angażują się w ochronę ludności cywilnej i zaplecza funkcjonowania państwa. Tak było np. w przypadku kryzysu migracyjnego na granicach Europy czy w czasie pandemii COVID-19, gdzie reagowanie kryzysowe wymagało zarówno elementów bezpieczeństwa wewnętrznego (działania policji, służb medycznych, administracji), jak i uwzględnienia szerszego kontekstu bezpieczeństwa międzynarodowego i społecznego.

Ze względu na swoją specyfikę, zarządzanie kryzysowe czerpie z dorobku wielu dziedzin naukowych. Można je uznać za obszar interdyscyplinarny, łączący wiedzę z nauk o bezpieczeństwie z teoriami i metodami innych dyscyplin. Nauki o obronności stanowią naturalny punkt odniesienia – zwłaszcza teoria sztuki wojennej i dowodzenia dostarcza koncepcji przydatnych w reagowaniu kryzysowym (strategia, taktyka działania w sytuacjach zagrożenia, zasady dowodzenia w akcjach ratunkowych). Nauki o zarządzaniu z kolei wpływają na cywilny wymiar zarządzania kryzysowego poprzez teorię organizacji, zarządzanie w administracji publicznej i metodykę

¹⁶² M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>

podejmowania decyzji. Wiedza z zakresu zarządzania pozwala usprawniać koordynację działań wielu podmiotów oraz efektywne wykorzystanie zasobów w sytuacji kryzysu. Prawo odgrywa istotną rolę ramową – to akty prawne regulują procedury w stanach nadzwyczajnych, kompetencje organów władzy w zarządzaniu kryzysowym oraz prawa i obowiązki obywateli w sytuacjach kryzysowych. Znajomość przepisów prawa administracyjnego, konstytucyjnego i specjalnych ustaw (np. ustawy o stanach nadzwyczajnych, ustawy o zarządzaniu kryzysowym) jest kluczowa dla badaczy i praktyków tej dziedziny. Socjologia i nauki społeczne dostarczają zaś wglądu w zachowania zbiorowe ludzi podczas kryzysów, mechanizmy paniki, sposoby komunikacji społecznej czy procesy podejmowania decyzji w warunkach stresu. Jak zauważa Michniak, zarządzanie kryzysowe jest związane nie tylko z naukami o bezpieczeństwie i obronności, lecz także z innymi naukami – na przykład z socjologią ze względu na badanie społeczności zaangażowanych w działania kryzysowe oraz ich zachowań¹⁶³. Socjologia służb mundurowych czy społeczności lokalnych w kryzysie stanowi wspólne pole badawcze dla socjologii, nauki o zarządzaniu i nauk o bezpieczeństwie. Również psychologia przyczynia się do zarządzania kryzysowego, szczególnie w obszarze interwencji kryzysowej i wsparcia psychologicznego dla ofiar oraz ratowników, a także w analizie procesów decyzyjnych pod presją czasu.

Warto podkreślić, że zarządzanie kryzysowe to teoria eklektyczna, czyli całościowy system wiedzy obejmujący wiele podsystemów wywodzących się z różnych dyscyplin¹⁶⁴. Michniak wymienia tu m.in. elementy matematyki (np. modelowanie zagrożeń, analizy ryzyka), nauk technicznych (systemy teleinformatyczne, inżynieria bezpieczeństwa), filozofii (np. etyka w działaniach ratowniczych, prakseologia), nauk politycznych (proces decyzyjny władz publicznych w kryzysie), wspomniane nauki o zarządzaniu, nauki o obronności, socjologię, psychologię oraz ekonomię. Taka wielodyscyplinowość oznacza, że badacze zarządzania kryzysowego muszą syntetyzować różnorodne podejścia. Granice między poszczególnymi naukami są tu płynne, a korzystanie z dorobku różnych dziedzin powinno być twórcze

¹⁶³ J. W. Michniak, Zarządzanie kryzysowe jako specjalność w dyscyplinie naukowej – nauki o bezpieczeństwie, *Studia Bezpieczeństwa Narodowego*, 4(1), 2013, s. 73.

¹⁶⁴ Tamże.

i dostosowane do specyfiki problemów kryzysowych – co sprzyja rozwojowi zarówno teorii, jak i usprawnieniu praktyki zarządzania kryzysowego.

Interdyscyplinarny charakter tej subdyscypliny dobrze ilustruje zakres treści programów kształcenia w tym kierunku. Na przykład, programy studiów w specjalności zarządzanie kryzysowe obejmują zagadnienia systemu bezpieczeństwa narodowego, teorii sztuki wojennej (obronność), wybrane zagadnienia prawa i politologii oraz nauk o zarządzaniu. Oznacza to, że przyszli specjaliści ds. zarządzania kryzysowego zdobywają wiedzę z zakresu strategii i taktyki (wywodzących się z nauk wojskowych), prawa dotyczącego stanów nadzwyczajnych, nauk politycznych (funkcjonowanie państwa i administracji w sytuacjach kryzysowych) oraz teorii organizacji i zarządzania. Ten szeroki fundament teoretyczny pokazuje, jak zarządzanie kryzysowe łączy różnorodne perspektywy w celu rozwiązywania złożonych problemów bezpieczeństwa. Poza ogólnymi powiązaniami instytucjonalnymi z innymi dyscyplinami, zarządzanie kryzysowe korzysta z konkretnych teorii i koncepcji wypracowanych w różnych dziedzinach. Jedną z nich jest teoria organizacji i zarządzania, która stanowi rdzeń naukowy zarządzania kryzysowego. Zajmuje się ona zasadami organizowania działań ludzi oraz funkcjonowaniem struktur organizacyjnych (np. urzędów, służb ratunkowych, zespołów kryzysowych). Badania w tym nurcie dostarczają zasad zorganizowanego działania, uniwersalnych dla różnych struktur – np. hierarchii dowodzenia, podziału zadań, zasad sprawnej koordynacji. Zarządzanie kryzysowe wykorzystuje te ustalenia, by efektywnie kierować wieloma podmiotami zaangażowanymi w akcję kryzysową, zapewnić klarowny przepływ informacji i skuteczne dowodzenie akcjami ratowniczymi.

Prakseologia – nauka o sprawnym działaniu – to kolejna ważna podstawa teoretyczna. Prakseologiczne pytanie „jak działać najskuteczniej?” jest bardzo zasadne w realiach kryzysowych, gdzie zasoby i czas są ograniczone. Zasady prakseologiczne (dotyczące doskonalenia efektywności działań i współdziałania ludzi) znajdują zastosowanie w doskonaleniu procedur kryzysowych na wszystkich szczeblach, od lokalnego po centralny.

Jak stwierdza Michniak, pominięcie dorobku prakseologii byłoby błędem, gdyż wnosi ona metody usprawniania działań bieżących w sytuacjach kryzysowych¹⁶⁵.

Z kolei cybernetyka i teoria systemów dostarczają narzędzi do analizy systemów zarządzania kryzysowego. Cybernetyka, badająca procesy sterowania i komunikacji w organizmach, maszynach i społeczeństwie, pomaga zrozumieć przepływ informacji w strukturach kryzysowych oraz optymalizować kanały komunikacji między służbami. Współczesne zarządzanie kryzysowe w dużym stopniu opiera się na efektywnej wymianie informacji (np. systemy wczesnego ostrzegania, centra zarządzania informacjami kryzysowymi) – teoria komunikacji i cybernetyki pozwala projektować te systemy tak, by były niezawodne i szybkie. Ogólna teoria systemów i analiza systemowa z kolei umożliwiają postrzeganie zarządzania kryzysowego jako złożonego systemu naczyń połączonych – sieci instytucji, ludzi, procedur i technologii, które muszą ze sobą współdziałać. Metodologie systemowe są wykorzystywane do badania funkcjonowania i projektowania systemów reagowania kryzysowego oraz ich doskonalenia (np. modelowanie struktur centrów zarządzania kryzysowego, integracja systemów łączności).

Teoria podejmowania decyzji (zarówno w ujęciu badań operacyjnych, jak i psychologicznym) również przenika do zarządzania kryzysowego. Sytuacje kryzysowe wymagają szybkiego podejmowania decyzji przy niepełnej informacji i wysokiej stawce, co stanowi wyzwanie opisywane w literaturze decyzyjnej¹⁶⁶. Badania operacyjne dostarczają metod wspomagających decyzje (np. algorytmy optymalizacyjne przy alokacji zasobów ratunkowych), zaś psychologia decyzji analizuje np. zjawiska błędów poznawczych, stresu czy pracy zespołowej w warunkach presji. Wiedza ta przekłada się na tworzenie procedur i systemów wsparcia decyzji dla sztabów kryzysowych – tak by decyzje były trafniejsze i podejmowane szybciej.

W kontekście zapobiegania kryzysom kluczowy wpływ wywarła dziedzina zarządzania ryzykiem (risk management). Koncepcje identyfikacji

¹⁶⁵ J. W. Michniak, Zarządzanie kryzysowe jako specjalność w dyscyplinie naukowej – nauki o bezpieczeństwie, *Studia Bezpieczeństwa Narodowego*, 4(1), 2013, s. 74.

¹⁶⁶ Z. Ciekankowski, S. Żurawski, Zarządzanie kryzysowe na szczeblu samorządowym na przykładzie gmin powiatu przemyskiego, Warszawa, Menedżerska Akademia Nauk Stosowanych w Warszawie, Wydawnictwo im. Profesora Leszka J. Krzyżanowskiego, 2022, s. 14.

ryzyka, analizy prawdopodobieństwa zdarzeń niepożądanych oraz planowania środków zaradczych wprost przeniknęły do zarządzania kryzysowego. Wiele procedur planowania kryzysowego rozpoczyna się od oceny ryzyka wystąpienia określonych zagrożeń (np. powodzi, ataku terrorystycznego) i przygotowania scenariuszy postępowania. Zarządzanie ryzykiem wypracowało standardy (takie jak ISO 31000) i metody analizy (np. macierze ryzyka, symulacje scenariuszy), które zwiększają proaktywność zarządzania kryzysowego – tj. nastawienie na przewidywanie zagrożeń i zapobieganie im zanim przekształcą się w pełnoskalowy kryzys. Jednocześnie, jak wskazują współczesne opracowania, dokonuje się ewolucja paradygmatu: od tradycyjnego modelu „przewidywania i zapobiegania” (predict and prevent) ku podejściu odporności (resilience), które zakłada konieczność radzenia sobie z nieuniknionymi jednak kryzysami i szybkiego regenerowania się po ich wystąpieniu. Interdyscyplinarność zarządzania kryzysowego oznacza zatem, że jego teoria i praktyka czerpią z wielu źródeł: nauk społecznych, technicznych, przyrodniczych (np. meteorologia w kontekście klęsk żywiołowych), a nawet humanistyki (np. etyka ratownictwa, historia wielkich katastrof). Ta szeroka baza teoretyczna przekłada się na bogaty aparat pojęciowy i metodologiczny wykorzystywany w badaniach. Efektem jest stopniowe wyodrębnianie się spójnego języka i metodyki nauki o zarządzaniu kryzysowym – choć eklektycznej, to jednak świadomie integrującej różne podejścia dla lepszego zrozumienia i rozwiązywania problemów kryzysowych.

Jako subdyscyplina nauk o bezpieczeństwie, zarządzanie kryzysowe posiada wyraźnie określony przedmiot badań, własny warsztat badawczy oraz aparat pojęciowy. Przedmiotem tym są wszelkie zjawiska związane z kryzysami i sytuacjami nadzwyczajnymi, struktury powołane do radzenia sobie z nimi, procesy działań kryzysowych oraz narzędzia służące ich realizacji. Można wyróżnić cztery główne kategorie badanych zagadnień:

- Zjawiska kryzysowe – obejmują badanie natury i dynamiki kryzysów: od katastrof naturalnych (powodzie, trzęsienia ziemi, huragany), przez katastrofy techniczne (awarie przemysłowe, skażenia środowiska), po kryzysy społeczne (zamieszki, masowe migracje, pandemie). Analizowane są przyczyny takich zjawisk, mechanizmy ich eskalacji, a także ich skutki dla społeczeństwa, gospodarki i bezpieczeństwa państwa. Naukowcy starają się tworzyć typologie kryzysów, modele

ich przebiegu oraz wskaźniki pozwalające ocenić skalę i powagę sytuacji kryzysowej. Przedmiotem badań są również warunki, w których zwykle zagrożenie przeradza się w kryzys – np. rola mediów i paniki społecznej w amplifikacji zagrożeń. Badania zjawisk kryzysowych często mają charakter multidyscyplinarny: np. łączą wiedzę z sejsmologii i urbanistyki w badaniach nad trzęsieniami ziemi, czy epidemiologii i socjologii w badaniach nad pandemią.

- Struktury i systemy zarządzania kryzysowego – to drugi obszar badawczy, skupiający się na analizie organizacyjnej strony reagowania kryzysowego. W jego ramach badane są systemy zarządzania kryzysowego na różnych poziomach: od krajowego systemu (obejmującego centralne i terenowe organy władzy publicznej, służby ratownicze, siły zbrojne w zakresie wsparcia niemilitarnego, organizacje pozarządowe, wolontariat), przez systemy regionalne i lokalne (wojewódzkie, powiatowe, gminne centra zarządzania kryzysowego), aż po sieci współpracy międzynarodowej w sytuacjach transgranicznych zagrożeń (np. mechanizmy Unii Europejskiej w zakresie ochrony ludności, współpraca NATO w reagowaniu na katastrofy). Badacze analizują struktury formalne tych systemów (np. skład i kompetencje zespołów zarządzania kryzysowego, schematy dowodzenia, procedury współdziałania między instytucjami) oraz struktury sieciowe – nieformalne relacje i powiązania między aktorami biorącymi udział w reagowaniu (np. współpraca między administracją a organizacjami społecznymi, partnerstwo publiczno-prywatne w sytuacjach kryzysowych). Ważnym zagadnieniem jest tu wydajność i spójność systemu: na ile poszczególne elementy (instytucje, służby) potrafią skutecznie współdziałać w warunkach kryzysu. Analizowane są studia przypadków dużych katastrof w celu identyfikacji barier i ułatwień w kooperacji (np. problemy z wymianą informacji między policją a strażą pożarną podczas akcji ratunkowych). Wreszcie, w zakres badań strukturalnych wchodzi infrastruktura kryzysowa – systemy łączności, centra operacyjne, rezerwy materiałowe – czyli materialne zaplecze funkcjonowania systemu.

- Procesy zarządzania kryzysowego – obejmują całokształt działań podejmowanych w ramach cyklu zarządzania kryzysowego. Cykl ten klasycznie dzieli się na fazy: zapobieganie (prewencja), przygotowanie, reagowanie oraz odbudowę (odtworzenie). W literaturze nowszej dodaje się także fazę oceny i wyciągania wniosków (learning), która zamyka cykl, tworząc sprzężenie zwrotne prowadzące do ulepszenia przyszłych działań¹⁶⁷. Badania naukowe analizują każdą z tych faz. W fazie planowania i przygotowania (prewencji) – przedmiotem zainteresowania jest planowanie cywilne na wypadek sytuacji kryzysowych, tworzenie planów zarządzania kryzysowego na różnych szczeblach, systemy wczesnego ostrzegania, szkolenia i ćwiczenia służb oraz populacji. Badane są metody skutecznej edukacji społecznej o zachowaniu w razie zagrożenia, a także integracja planów kryzysowych z politykami rozwoju (np. planowanie przestrzenne uwzględniające ryzyko powodzi). W fazie reagowania – analiza dotyczy przebiegu akcji ratunkowych, skuteczności interwencji służb, decyzji podejmowanych pod presją czasu, komunikacji kryzysowej z ludnością oraz współdziałania między podmiotami w czasie realnego zdarzenia. Badacze starają się zidentyfikować najlepsze praktyki skracające czas reakcji i ratujące życie, a także bariery (np. brak interoperacyjności radiowej między służbami, chaos kompetencyjny) pogarszające odpowiedź na kryzys. Ważnym tematem jest również komunikacja kryzysowa – tj. przekazywanie rzetelnych informacji społeczeństwu w trakcie kryzysu, co ma wpływ na zachowanie spokoju publicznego i współpracę obywateli z władzami. W fazie odbudowy i rekonstrukcji – badania dotyczą zarządzania procesem powrotu do normalności po kryzysie. Obejmuje to zagadnienia takie jak odbudowa infrastruktury, pomoc poszkodowanym (mieszkania zastępcze, odszkodowania), wsparcie psychologiczne, przywracanie usług komunalnych, a także uczenie się na błędach – instytucjonalne dochodzenia powypadkowe, raporty komisji badających przyczyny katastrof i wydających

¹⁶⁷ A. Skrabacz, A. Pajka, B. Więckowski, Crisis Management as a Research Province of Security Science, *Roczniki Nauk Społecznych*, 52(1), 2024, s. 7-25. <https://doi.org/10.18290/rns2024.0010>

rekomendacje na przyszłość. Szczególnie koncepcja rezyliencji (odporności) kładzie nacisk na tę fazę, postulując aby proces odbudowy jednocześnie wzmacniał system na wypadek kolejnych kryzysów.

- Narzędzia zarządzania kryzysowego – czwarty obszar zainteresowań badawczych stanowią środki i instrumenty wykorzystywane w procesach zarządzania kryzysowego. Należą do nich m.in. systemy informacji kryzysowej (bazy danych o zagrożeniach, platformy wymiany informacji między służbami), procedury operacyjne (standardowe procedury postępowania – tzw. SOPy, instrukcje działania centrów kryzysowych), a także plany zarządzania kryzysowego i plany ciągłości działania instytucji publicznych i firm. Badacze oceniają jakość i skuteczność tych narzędzi, poszukując najlepszych praktyk ich tworzenia i wdrażania. Coraz istotniejszym narzędziem są także symulacje komputerowe i gry decyzyjne służące szkoleniu kadr oraz testowaniu gotowości na wypadek kryzysu. W dobie transformacji cyfrowej rozwijane są nowoczesne technologie wspierające zarządzanie kryzysowe, takie jak systemy GIS do mapowania zagrożeń, sztuczna inteligencja do prognozowania rozwoju sytuacji czy media społecznościowe jako źródło informacji o sytuacji w terenie. Naukowcy analizują, jak skutecznie integrować te narzędzia w istniejących strukturach i jak wpływają one na dynamikę reagowania kryzysowego.

Przedmiot badań zarządzania kryzysowego jest szeroki i obejmuje zarówno kwestie poznawcze (zrozumienie natury kryzysów, ich prawidłowości i uwarunkowań), jak i praktyczne (opracowanie metod, procedur i narzędzi pozwalających lepiej radzić sobie z kryzysami). Celem nauki w tej dziedzinie jest nie tylko opis i wyjaśnienie zjawisk, ale również formułowanie zaleceń usprawniających realne systemy reagowania. W zakres funkcji naukowych zarządzania kryzysowego wchodzi więc funkcje deskryptywne i eksplikatywne (opis i wyjaśnianie kryzysów), prognostyczne (przewidywanie przebiegu zdarzeń), diagnostyczne (identyfikacja słabości systemu reagowania), a także normatywne (formułowanie zasad i procedur optymalnego działania) oraz metodologiczne (opracowywanie narzędzi badawczych dla tej dziedziny). Dzięki temu zarządzanie kryzysowe rozwija się jako

subdyscyplina o własnej tożsamości, ale jednocześnie głęboko zakorzeniona w praktyce rozwiązywania realnych problemów bezpieczeństwa.

Na przestrzeni rozwoju tej dyscypliny wykształciły się różne paradygmaty badawcze – zestawy założeń i podejść metodologicznych – poprzez które uczeni patrzą na problematykę kryzysów. Do najważniejszych należą:

- **Podejście systemowe** – traktuje zarządzanie kryzysowe jako system złożony z wielu elementów (instytucji, ludzi, procedur, technologii) powiązanych siecią relacji. Paradygmat systemowy zakłada, że kryzys jest zdarzeniem oddziałującym na cały system społeczny lub organizacyjny, a skuteczność reakcji zależy od sprawności całego układu, nie zaś tylko pojedynczych jego części. Badania systemowe wykorzystują m.in. modelowanie systemowe, analizę sieciową i teorię systemów do identyfikacji kluczowych węzłów i przepływów informacji w zarządzaniu kryzysowym. Dzięki temu można wskazać np. krytyczne punkty w systemie (bottlenecks) ograniczające sprawność reakcji lub zrozumieć efekt domina, w którym awaria jednej infrastruktury (np. energetycznej) powoduje lawinę kolejnych problemów (transport, łączność itd.). Podejście systemowe akcentuje także konieczność holistycznego ujęcia procesu kryzysowego – czyli badania go od fazy prewencji aż po odbudowę w ramach jednolitej koncepcji zarządzania. W literaturze przedmiotu często podkreśla się, że brak spojrzenia systemowego prowadzi do wąskich specjalizacji niezdolnych ogarnąć złożoności realnych kryzysów¹⁶⁸. Stąd paradygmat ten jest dominujący np. w analizach critical infrastructure protection – gdzie sieć wzajemnie zależnych systemów (energia, telekomunikacja, woda, transport) wymaga systemowego zabezpieczenia i reagowania.
- **Podejście funkcjonalne** – koncentruje się na podstawowych funkcjach i zadaniach zarządzania kryzysowego, niezależnie od tego, kto je wykonuje. W tym ujęciu analizuje się kolejno funkcje: monitorowanie zagrożeń, ostrzeganie, alarmowanie, ewakuacja, ratownictwo, opieka nad poszkodowanymi, przywracanie porządku, odbudowa itp. Każda

¹⁶⁸ L. K. Comfort, T. A. Birkland, B. A. Cigler, E. Nance, Retrospectives and Prospectives on Hurricane Katrina: Five Years and Counting, *Public Administration Review*, 70(5), 2010, s. 669-678.

z tych funkcji może być realizowana przez różne podmioty, ale ważne jest badanie, jak powinna przebiegać dana funkcja, aby była skuteczna. Na gruncie funkcjonalnego podejścia powstało np. wiele standardów i doktryn planowania kryzysowego opartych o fazy/funkcje – np. koncepcja Integrated Emergency Management rozwinięta w USA czy krajowy system planowania cywilnego w Polsce. Badacze porównują, jak poszczególne funkcje są realizowane w różnych krajach lub sektorach, co pozwala wyciągać wnioski o skuteczności różnych rozwiązań organizacyjnych. Przykładem może być analiza funkcji ostrzegania ludności przed zagrożeniem – która w jednym kraju opiera się na scentralizowanych alertach SMS, a w innym na lokalnych systemach syren i komunikatach radiowych, podejście funkcjonalne umożliwia ocenę, który model jest bardziej niezawodny w różnych warunkach.

- **Podejście organizacyjne** – zakłada, że aby zrozumieć zarządzanie kryzysowe, trzeba przyrzeć się poszczególnym organizacjom i instytucjom zaangażowanym w ten proces. Ten paradygmat skupia się na przygotowaniu organizacji (np. straży pożarnej, szpitala, urzędu miasta) do działania w sytuacji kryzysowej, na ich kulturze organizacyjnej, strukturze wewnętrznej, procesach decyzyjnych i możliwościach adaptacji. Badania w tym nurcie często korzystają z teorii zarządzania (np. zarządzania strategicznego, teorii przywództwa, zarządzania zasobami ludzkimi) i stosują je do kontekstu kryzysowego. Przykładowo, analizuje się style przywództwa w warunkach kryzysu – co decyduje o skuteczności dowódcy akcji ratunkowej lub lidera politycznego w czasie sytuacji nadzwyczajnej¹⁶⁹. Podejście organizacyjne obejmuje też badania nad uczeniem się organizacyjnym po kryzysie – tj. jak instytucje wyciągają wnioski ze swoich doświadczeń kryzysowych i wdrażają zmiany poprawiające ich przyszłą gotowość. Wreszcie, w tym paradygmacie mieszczą się studia nad kulturą bezpieczeństwa organizacji, odpornością organizacyjną (organizational resilience) czy też nad rolą sektora prywatnego w zarządzaniu kryzysowym (w tym

¹⁶⁹ A. Boin, P. 't Hart, E. Stern, B. Sundelius, *The Politics of Crisis Management: Public Leadership under Pressure*, Cambridge, Cambridge University Press, 2005. <https://doi.org/10.1017/CBO9780511490880>

analiza planów ciągłości działania przedsiębiorstw, współpracy firm z administracją w ramach partnerstwa publiczno-prywatnego podczas klęsk).

- Podejście sieciowe (governance network) – względnie nowe podejście wynikające z obserwacji, że we współczesnych kryzysach uczestniczy bardzo wiele podmiotów połączonych w wielostronne sieci współpracy. Paradygmat sieciowy zakłada odejście od myślenia wyłącznie w kategoriach hierarchii rządowej, zamiast tego postuluje analizę współzarządzania kryzysowego (crisis governance), w którym uczestniczą agencje rządowe różnych szczebli, samorządy, organizacje pozarządowe, społeczności lokalne, a nieraz także biznes i media¹⁷⁰. Badania sieciowe koncentrują się na relacjach między tymi aktorami: przepływie informacji, zaufaniu, koordynacji oddolnej i horyzontalnej. Wykorzystuje się tu często analizę sieci społecznych (SNA), modelowanie współpracy międzyinstytucjonalnej oraz teorie zarządzania publicznego nastawione na współdziałanie (collaborative public management)¹⁷¹. Przykładowe pytania badawcze to: Jak zbudować efektywną sieć współpracy w mieście dotkniętym klęską żywiołową, aby organizacje pozarządowe uzupełniały działania administracji? albo Jak formalne struktury (np. sztab kryzysowy) łączą się z oddolnymi inicjatywami społecznymi (wolontariat, pomoc sąsiedzka) w trakcie kryzysu? Badania wykazują, że silne sieci współpracy mogą zwiększać zdolność reagowania i odporność społeczeństwa na kryzysy, ale z drugiej strony złożoność sieci stawia wyzwania w zakresie koordynacji¹⁷². Paradygmat sieciowy wpisuje się ogólnie w nurt governance, czyli zarządzania poprzez współdziałanie wielu partnerów, i w kontekście sytuacji kryzysowych wydaje się coraz bardziej adekwatny, zwłaszcza w obliczu wyzwań przekraczających granice

¹⁷⁰ K. Sienkiewicz-Małyjurek, Inter-organizational collaboration and public sector innovativeness – the case of Poland, *International Journal of Contemporary Management*, 12(30), 2013, s. 8-25.

¹⁷¹ H. Güreşci, R.S. Arpat, Usage of Social Network Analysis (SNA) in Crisis Management, *Journal on Baltic Security*, 2016, s. 72-88.

¹⁷² N. Kapucu, R. B. Dougherty, Q. Hu, Network Governance for Coordinated Disaster Response, *Public Administration Quarterly*, 46(4), 2022, s. 309-333. <https://doi.org/10.37808/paq.46.4.2>

administracyjne czy państwowe (np. kryzysy klimatyczne, pandemie, cyberzagrożenia).

- Podejście zorientowane na odporność (resilience) – najnowszy z wyróżnianych paradygmatów, zdobywający popularność zwłaszcza w ostatnich latach na fali doświadczeń przewlekłych kryzysów (pandemia COVID-19, zmiany klimatu). Paradygmat rezyliencji zmienia akcent z samego reagowania na kryzys na zdolność systemu lub społeczności do adaptacji i odrodzenia się po kryzysie¹⁷³. W tym ujęciu kluczowe staje się wzmacnianie zdolności przetrwania i odbudowy – zarówno w wymiarze infrastrukturalnym, jak i społecznym. Badania resilience analizują m.in. czynniki warunkujące odporność społeczności (np. kapitał społeczny, samoorganizacja mieszkańców) oraz mechanizmy adaptacyjne w administracji i gospodarce. Rezyliencja dostarcza też nowego języka normatywnego: mówi się o budowaniu „kultury odporności”, strategiach odpornościowych miast i państw, testowaniu systemów poprzez scenariusze skrajne (stress tests). W praktyce oznacza to, że zarządzanie kryzysowe nie jest postrzegane jedynie jako reagowanie na najgorsze chwile, ale jako ciągły proces przygotowywania się na nieznane zagrożenia i uczenia się na doświadczeniach. Stępka podkreśla, że rezyliencja inspirowa do zmiany myślenia o zarządzaniu kryzysowym: zakłada rozproszenie odpowiedzialności (nie tylko instytucje państwa, ale każdy obywatel i społeczność lokalna mają rolę do odegrania), uznanie nieuchronności pewnych zagrożeń (nie można zapobiec wszystkim kryzysom, więc trzeba nauczyć się z nimi żyć) oraz skupienie uwagi na mechanizmach adaptacji i powrotu do normalności¹⁷⁴. Paradygmat ten promuje także proaktywne działania zwiększające odporność – inwestycje w infrastrukturę krytyczną odporną na awarie, dywersyfikację źródeł zaopatrzenia, edukację społeczeństwa w zakresie samopomocy i pierwszej reakcji. W nauce o bezpieczeństwie podejście rezyliencyjne jest coraz częściej

¹⁷³ M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>

¹⁷⁴ M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 108. <https://doi.org/10.14746/pp.2021.26.2.7>

wykorzystywane do analiz polityk publicznych i strategii bezpieczeństwa¹⁷⁵. Pewnym wyzwaniem jest jednak operacjonalizacja pojęcia „odporności” – trwają dyskusje, jak mierzyć poziom rezyliencji i jak przekładać tę koncepcję na konkretne wskaźniki i działania.

Należy zaznaczyć, że wymienione paradygmaty nie są wzajemnie sprzeczne – raczej kładą nacisk na różne aspekty i uzupełniają się w ogólnym obrazie. Naukowiec zajmujący się zarządzaniem kryzysowym może łączyć elementy tych podejść, np. badając sieci współpracy (podejście sieciowe) w ramach szerszego systemu reagowania (podejście systemowe) albo analizując funkcję informowania ludności (podejście funkcjonalne) przez pryzmat kształtowania odporności społecznej (podejście resilience). Wybór paradygmatu zależy często od skali analizy (systemowy na makropoziomie, organizacyjny na mezopoziomie, funkcjonalny na mikropoziomie konkretnego procesu) oraz od celów badania (czy chodzi o wyjaśnienie działania systemu, usprawnienie danej funkcji, czy ocenę zdolności adaptacyjnych). Różnorodność podejść świadczy o bogactwie teoretycznym subdyscypliny, która w ciągu kilkudziesięciu lat wypracowała własne ramy pojęciowe do analizowania kryzysów i reagowania na nie.

Dynamiczny rozwój zarządzania kryzysowego jako obszaru badawczego znajduje odzwierciedlenie zarówno w systemie edukacji wyższej, jak i w liczbie publikacji naukowych. Od lat 90. XX wieku, kiedy to pojęcie zarządzania kryzysowego zostało zaadaptowane w Polsce z praktyki amerykańskiej (m.in. FEMA – Federalna Agencja Zarządzania Kryzysowego) i włączone do systemu ochrony ludności, obserwuje się stopniowe instytucjonalizowanie tej dziedziny¹⁷⁶. W 2011 r. nauki o bezpieczeństwie uzyskały w Polsce status odrębnej dyscypliny nauk społecznych, co otworzyło drogę do wyodrębniania wewnątrz niej specjalności takich jak zarządzanie kryzysowe. Od tego czasu na uczelniach powstały liczne kierunki i specjalizacje poświęcone tej tematyce.

¹⁷⁵ P. Bourbeau, *Resiliencism and security studies: initiating a dialogue, Contesting Security: Strategies and Logics*, red. T. Balzacq. London-New York, Routledge 2014, s. 1-15.

¹⁷⁶ A. Skrabacz, A. Pajka, B. Więckowski, *Crisis Management as a Research Province of Security Science*, *Roczniki Nauk Społecznych*, 52(1), 2024, s. 7-25. <https://doi.org/10.18290/rns2024.0010>

Kształcenie akademickie w zakresie zarządzania kryzysowego prowadzą zarówno uniwersytety cywilne, jak i uczelnie o profilu wojskowym lub służb mundurowych. Przykładowo, specjalność zarządzanie kryzysowe oferowana jest na kierunkach bezpieczeństwo narodowe czy wewnętrzne m.in. na Uniwersytecie Warszawskim, Wojskowej Akademii Technicznej w Warszawie, Akademii Wojsk Lądowych we Wrocławiu, wielu akademiach zawodowych oraz prywatnych szkołach wyższych. Część uczelni utworzyła także osobne kierunki studiów pierwszego i drugiego stopnia wprost nazwane „zarządzanie kryzysowe”. Programy tych studiów łączą wiedzę teoretyczną z praktycznymi elementami, jak np. gry decyzyjne, ćwiczenia sztabowe, wizyty studyjne w centrach zarządzania kryzysowego czy w resortowych jednostkach (np. Rządowe Centrum Bezpieczeństwa, Wojewódzkie Centra Zarządzania Kryzysowego). W ramach zajęć studenci uczą się nie tylko teorii bezpieczeństwa, ale i konkretnych umiejętności: analizy ryzyka, opracowywania planów reagowania, komunikacji w sytuacji kryzysowej, podstaw ratownictwa, a nawet elementów psychologii kryzysu. Tak wszechstronne wykształcenie odpowiada interdyscyplinarnej naturze tej dziedziny. Ponadto, istnieje bogata oferta studiów podyplomowych dla osób już pracujących w administracji publicznej czy służbach – np. podyplomowe studia z zarządzania kryzysowego organizowane przez Akademię Sztuki Wojennej czy Szkołę Główną Służby Pożarniczej. Świadczy to o zapotrzebowaniu praktyki na aktualizację wiedzy i doskonalenie kadr w tym obszarze.

Na arenie międzynarodowej rozwój edukacji w dziedzinie zarządzania kryzysowego (emergency management) również jest widoczny. W USA i Kanadzie istnieje wiele programów Emergency Management na poziomie bachelor i master, a nawet dedykowane wydziały. Organizacje takie jak FEMA opracowały standardy kształcenia i certyfikacji (np. Certified Emergency Manager). W Europie zarządzanie kryzysowe bywa częścią programów z bezpieczeństwa cywilnego, ochrony ludności lub zarządzania publicznego. Ujednoliceniu podejścia sprzyjają projekty w ramach UE (np. programy szkoleniowe civil protection). Dzięki temu wykształciła się społeczność ekspertów w tej dziedzinie, wymieniająca się doświadczeniami na konferencjach (jak International Disaster and Risk Conference, konferencje IAEM – International Association of Emergency Managers) oraz publikacjach naukowych.

Badania naukowe nad zarządzaniem kryzysowym również intensywnie się rozwijają. Świadczy o tym rosnąca liczba publikacji: według najnowszych analiz bibliometrycznych, od początku XXI wieku nastąpił gwałtowny wzrost liczby artykułów na ten temat, szczególnie w ostatnich dwóch dekadach. Kryzysy takie jak ataki terrorystyczne 2001 r., huragan Katrina (2005 r.), pandemia COVID-19 (2020 r.+) generowały fale zainteresowania badaczy, owocując nowymi studiami przypadku i teoriami. W globalnej literaturze dominują publikacje anglojęzyczne – prym wiedzie dorobek ze Stanów Zjednoczonych. Szacuje się, że ok. 23% wszystkich publikacji naukowych dotyczących zarządzania kryzysowego pochodzi od autorów z USA, podczas gdy na drugim miejscu plasują się Chiny (~7%), a dalsze miejsca zajmują m.in. Wielka Brytania, Kanada, Niemcy. Wyraźnie pokazuje to, że ośrodki anglojęzyczne nadają ton badaniom (co wynika też z faktu, że językiem nauki jest angielski i większość czasopism wydawana jest w tym języku). Mniejszy udział krajów takich jak Polska wiąże się z krótszą tradycją badań w tym zakresie oraz barierą językową (wiele polskich opracowań ukazuje się po polsku, poza globalnymi bazami danych). Początki rodzimej refleksji naukowej nad zarządzaniem kryzysowym sięgają przełomu wieków i miały związek z reformami systemu reagowania kryzysowego oraz wejściem Polski do NATO.

Do najważniejszych pól badawczych we współczesnych badaniach nad zarządzaniem kryzysowym należą m.in.:

- zarządzanie kryzysowe a zmiany klimatu (jak przygotować się na rosnącą częstość ekstremalnych zjawisk pogodowych),
- terroryzm i zdarzenia asymetryczne (np. reagowanie na ataki CBRN – chemiczne, biologiczne, radiologiczne, nuklearne),
- zarządzanie kryzysowe w systemie miejskim (tzw. urban resilience – odporność miast),
- rola nowych technologii (systemy GIS, Big Data, media społecznościowe i ich wykorzystanie w wykrywaniu i reagowaniu na kryzysy),
- psychospołeczne aspekty kryzysów (trauma po katastrofach, zachowanie tłumu, komunikacja ryzyka),
- koordynacja międzynarodowa (mechanizmy pomocy międzynarodowej, rola ONZ i UE w dużych katastrofach),

- kryzysy zdrowotne (pandemie, bioterroryzm – co szczególnie zyskało na znaczeniu po 2020 r.),
- oraz aspekty etyczno-prawne (dylematy etyczne w alokacji ograniczonych zasobów ratunkowych, równowaga między bezpieczeństwem a prawami jednostki w sytuacjach nadzwyczajnych).

Tak szeroki wachlarz tematów będzie omawiany bardziej szczegółowo w dalszych częściach pracy. Już na tym etapie jednak widać, że zarządzanie kryzysowe ugruntowało swoją tożsamość naukową. Posiada własne stowarzyszenia eksperckie i naukowe (np. Polskie Towarzystwo Bezpieczeństwa Narodowego tworzące sekcje tematyczne, w tym zarządzania kryzysowego), a także znaczący wpływ na praktykę – wyniki badań przekładają się na doskonalenie systemów reagowania (poprzez rekomendacje legislacyjne, wytyczne dla administracji, nowe rozwiązania techniczne). Zarządzanie kryzysowe w systemie nauk o bezpieczeństwie wyewoluowało od domeny praktyków (ratowników, wojskowych, urzędników) ku pełnoprawnej subdyscyplinie akademickiej o interdyscyplinarnym charakterze. Łączy ono teorię i praktykę, uczelnię i służbę publiczną, perspektywę globalną (np. zmiany klimatu) z lokalną (społeczności dotknięte kryzysem). Jego interdyscyplinarność i praktyczna użyteczność sprawiają, że zajmuje dziś ważne miejsce zarówno w edukacji dla bezpieczeństwa, jak i w badaniach naukowych nad złożonymi zagrożeniami współczesnego świata.

2.3. Geneza i ewolucja zarządzania kryzysowego w Polsce i na świecie

Po II wojnie światowej koncepcja obrony cywilnej (civil defense) stała się podstawą ochrony ludności w obliczu konfliktów zbrojnych. Już Protokołem Dodatkowym I do Konwencji Genewskich z 12 sierpnia 1949 r. społeczność międzynarodowa formalnie ustanowiła obronę cywilną jako zbiór działań mających chronić ludność cywilną podczas wojny¹⁷⁷. W okresie zimnej wojny obrona cywilna koncentrowała się głównie na przygotowaniach do ataku zbrojnego (zwłaszcza nuklearnego). Budowano systemy schronów,

¹⁷⁷ Protokół Dodatkowy (I) do Konwencji Genewskich z 1949 r. – art. 61.

alarmowania i ćwiczone ewakuację ludności, a większość zadań OC miała charakter wojenny – jedynie niewielka część dotyczyła współdziałania przy klęskach żywiołowych w czasie pokoju. Struktury OC były podporządkowane resortom obrony i przewidywane do działania wyłącznie na czas konfliktu zbrojnego.

W drugiej połowie XX wieku nastąpiła jednak stopniowa ewolucja podejścia od obrony cywilnej ku szerszemu zarządzaniu sytuacjami kryzysowymi. Zmieniający się charakter zagrożeń – rozwój cywilizacyjny, awarie technologiczne, katastrofy przemysłowe – wymusił odejście od czysto militarnego patrzenia na ochronę ludności. Po zakończeniu zimnej wojny (lata 90.) zmniejszyło się zagrożenie globalnym konfliktem nuklearnym, a w wielu krajach służby obrony cywilnej przekształcono w agencje zarządzania kryzysowego o profilu all-hazards. Na przykład w Stanach Zjednoczonych zadania obrony cywilnej przejęła Federalna Agencja Zarządzania Kryzysowego (FEMA), która pod koniec lat 70. zaczęła integrować różne programy reagowania na klęski żywiołowe i awarie (formalnie utworzona w 1979 r.). W wielu państwach zamiast terminu civil defense upowszechniło się pojęcie “disaster management” / “emergency management”, odzwierciedlające szerszy zakres – od przygotowania i zapobiegania po reagowanie na wszelkie poważne zagrożenia.

Kluczowe katastrofy na świecie w drugiej połowie XX i na początku XXI wieku pełniły rolę katalizatorów zmian w podejściu do ochrony ludności i zarządzania kryzysowego. Można wskazać następujące przełomowe wydarzenia, które uwidoczniły braki istniejących systemów i wymusiły reformy:

- Awaria w elektrowni jądrowej Three Mile Island (USA, 1979 r.) – Częściowe stopienie rdzenia reaktora nie spowodowało wprawdzie ofiar śmiertelnych, ale obnażyło poważne luki w procedurach bezpieczeństwa i zarządzania sytuacją awaryjną. W rezultacie wprowadzono – według amerykańskiej Komisji NRC – „szeroko zakrojone i trwałe zmiany” w przepisach i praktykach przemysłu jądrowego¹⁷⁸. Udoskonalono plany reagowania kryzysowego wokół elektrowni

¹⁷⁸ D. Dalton, Three Mile Island Led To “Sweeping And Permanent” Changes, NucNet Bulletin, 23 Mar 2009.

atomowych, podniesiono standardy szkolenia operatorów, wprowadzono stałe dyżury centrów reagowania, a przemysł powołał własny instytut nadzoru bezpieczeństwa (INPO). Wypadek TMI wymusił także większą międzynarodową współpracę w zakresie bezpieczeństwa jądrowego – m.in. zainicjowano misje inspekcyjne OSART w ramach MAEA (od 1982 r.) oraz zaczęto powszechniej stosować analizy ryzyka technologicznego.

- Katastrofa chemiczna w Bhopalu (Indie, 1984 r.) – Uwolnienie ok. 40 ton toksycznego izocyjanianu metylu z fabryki pestycydów Union Carbide spowodowało natychmiastową śmierć około 3,8 tys. osób, zaś w kolejnych tygodniach i latach skutki zatrucia przyczyniły się do śmierci dziesiątek tysięcy kolejnych ofiar¹⁷⁹. Bhopal uznawany jest za najtragiczniejszą awarię przemysłową w historii. Wydarzenie to ujawniło dramatyczny brak przygotowania na tego typu zdarzenia – zarówno po stronie zakładu (niesprawne systemy bezpieczeństwa), jak i władz lokalnych. W skali globalnej wskazało to na konieczność wprowadzenia międzynarodowych standardów bezpieczeństwa przemysłowego, skuteczniejszych strategii prewencji oraz planów awaryjnych na wypadek awarii chemicznych. Społeczność międzynarodowa dostrzegła potrzebę egzekwawalnych norm ochrony środowiska i ludności przed podobnymi zdarzeniami. W następstwie tragedii wiele państw zaostrzyło regulacje dotyczące zakładów o dużym ryzyku (np. w USA uchwalono prawo EPCRA w 1986 r., zobowiązujące firmy do informowania społeczności o zagrożeniach chemicznych), a w Europie zaktualizowano tzw. dyrektywę Seveso dotyczącą kontroli poważnych awarii przemysłowych. Katastrofa w Bhopalu stała się też impulsem do szerszego wdrażania zasad planowania na wypadek awarii przemysłowych oraz uwzględniania tzw. zagrożeń transgranicznych w bezpieczeństwie chemicznym.
- Ataki terrorystyczne z 11 września 2001 r. (USA) – Zamachy na World Trade Center i Pentagon były punktem zwrotnym, który

¹⁷⁹ E. Broughton, The Bhopal disaster and its aftermath: a review, *Environmental Health*, 4(1), 2005, s. 6. <https://doi.org/10.1186/1476-069X-4-6>

rozszerzył zakres zarządzania kryzysowego o zupełnie nowy wymiar: zagrożenia terrorystyczne i bezpieczeństwo wewnętrzne. W odpowiedzi Stany Zjednoczone przeprowadziły największą reorganizację instytucjonalną od czasów II wojny światowej – w 2003 r. utworzono Departament Bezpieczeństwa Krajowego (DHS), który skonsolidował działania kilkudziesięciu różnych służb i agencji (w tym FEMA) w ramach nowej koncepcji „homeland security”. Terroryzm z priorytetu dotychczas marginalnego stał się zagrożeniem numer jeden dla instytucji odpowiedzialnych za bezpieczeństwo cywilne. Skala i szok zamachów ujawniły również problemy w łączności i koordynacji służb ratowniczych – np. zawiodła wówczas współpraca systemów radiowych różnych służb. W kolejnych latach nastąpiło zatarcie tradycyjnych podziałów między klasycznym zarządzaniem kryzysowym a działaniami antyterrorystycznymi. Rozwijano systemy wczesnego ostrzegania przed atakami, zintegrowane centra reagowania (jak choćby rozbudowa FBI Joint Terrorism Task Forces) oraz usprawniono infrastrukturę łączności kryzysowej na wypadek zamachów¹⁸⁰. Także w innych krajach wydarzenia z 9/11 stały się impulsem do przeglądu systemów reagowania: w Wielkiej Brytanii utworzono po 2001 r. rządowe centrum koordynacji kryzysowej COBR(A) (Cabinet Office Briefing Rooms), które zapewnia bieżącą współpracę służb podczas sytuacji nadzwyczajnych (po atakach z 11 września w ramach COBR podjęto m.in. decyzję o natychmiastowym zamknięciu przestrzeni powietrznej nad UK). Na forum międzynarodowym zacieśniono wymianę informacji wywiadowczych i ratowniczych w obliczu globalnego zagrożenia terrorystycznego.

- Huragan Katrina (USA, 2005 r.) – Katastrofalne skutki tego huraganu (ponad 1800 ofiar śmiertelnych, ogromne zniszczenia materialne, w tym zalanie Nowego Orleanu) obnażyły słabości ówczesnego systemu reagowania kryzysowego nawet w wysoko rozwiniętym kraju. Ujawniono m.in. opieszałość decyzyjną, brak klarownego podziału

¹⁸⁰ C. B. Rubin, *Emergency Management in the 21st Century: Dealing with Al Qaeda*, Tom Ridge, and Julie Gerberding, Working Paper #108, The Natural Hazards Center, Boulder, University of Colorado, 2004.

kompetencji między władzami federalnymi a stanowymi oraz niewystarczające przygotowanie planów ewakuacji i zabezpieczenia infrastruktury krytycznej. Katrina unaoczniała potrzebę gotowości na katastrofy o skali regionalnej oraz konieczność usprawnienia komunikacji i koordynacji działań ratunkowych. W odpowiedzi w USA zreformowano FEMA (przyjęto Post-Katrina Emergency Management Reform Act z 2006 r.), opracowano zupełnie nowy Narodowy Plan Reagowania (National Response Framework), a także zainwestowano miliardy dolarów w modernizację systemów ochrony przeciwpowodziowej (m.in. wzmocnienie wałów wokół Nowego Orleanu). Huragan Katrina stał się również ważnym punktem odniesienia w globalnej dyskusji o zmianach klimatu – pokazał, że wzrastająca częstotliwość ekstremalnych zjawisk pogodowych będzie coraz większym wyzwaniem. Od tego czasu zarządzanie kryzysowe coraz silniej integruje się z polityką redukcji ryzyka klęsk żywiołowych (disaster risk reduction), kładąc nacisk na działania prewencyjne.

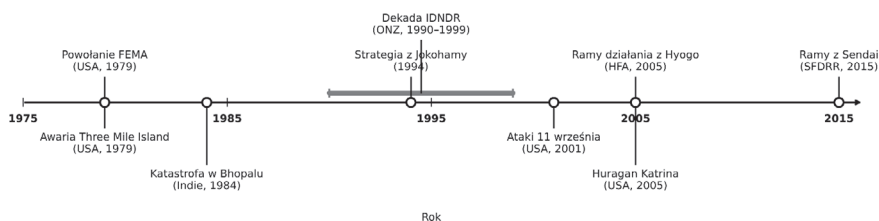
Od lat 90. XX w. wyraźnie przesuwano się akcent z reaktywnego podejścia response & recovery (reagowanie i odbudowa) na podejście proaktywne, czyli redukcję ryzyka i budowanie odporności (resilience) społeczeństw na wypadek katastrof. Ważnym symbolem tej zmiany było ogłoszenie przez ONZ Międzynarodowej Dekady Ograniczania Skutków Klęsk Żywiołowych (IDNDR) w latach 1990-1999, która promowała globalną współpracę w dziedzinie zapobiegania klęskom. Jej zwieńczeniem była Światowa Konferencja w Jokohamie (1994 r.), gdzie przyjęto Strategię z Jokohamy podkreślającą znaczenie prewencji i gotowości na wypadek klęsk. Następnie, po doświadczeniach katastrofalnego tsunami na Oceanie Indyjskim (grudzień 2004 r.), społeczność międzynarodowa wypracowała pierwsze kompleksowe ramy redukcji ryzyka katastrof – Hyogo Framework for Action 2005-2015 (HFA), przyjęte na Światowej Konferencji w Kobe w styczniu 2005 r. Dokument ten ustanawiał cel budowania odporności narodów i społeczności na katastrofy oraz wskazywał pięć priorytetów działania (m.in. uczynienie redukcji ryzyka priorytetem na szczeblu narodowym i lokalnym, rozwijanie systemów wczesnego ostrzegania, wykorzystanie edukacji do budowy kultury bezpieczeństwa itp.). W kolejnej dekadzie wiele państw (w tym Polska)

opracowało własne narodowe strategie ograniczania ryzyka klęsk zgodnie z tymi wytycznymi HFA. Kontynuacją globalnych wysiłków jest obecnie Sendai Framework for Disaster Risk Reduction 2015-2030, przyjęty na III Światowej Konferencji ONZ w Sendai w marcu 2015 r. Ramy z Sendai wyznaczyły siedem globalnych celów do 2030 r. (m.in. redukcję liczby ofiar i strat ekonomicznych, zwiększenie dostępu do systemów ostrzegania, opracowanie krajowych strategii redukcji ryzyka) oraz cztery priorytety działania: (1) lepsze rozumienie ryzyka, (2) wzmocnienie zarządzania ryzykiem, (3) inwestowanie w redukcję ryzyka dla zwiększenia odporności, (4) poprawa przygotowania na wypadek katastrof (w tym idea Build Back Better przy odbudowie). Sendai podkreśla konieczność zaangażowania całego społeczeństwa – administracji, samorządów, sektora prywatnego, świata nauki i organizacji pozarządowych – we wspólne budowanie kultury bezpieczeństwa i odporności na zagrożenia. Rezyliencja (odporność) stała się wręcz nowym paradygmatem myślenia o bezpieczeństwie w czasach przewlekłych kryzysów¹⁸¹, oferując podejście skupione na zdolności społeczności do adaptacji, przetrwania i szybkiego powrotu do normalności po wstrząsach (zamiast polegania wyłącznie na reakcji instytucji państwa). Koncepcja ta zyskuje coraz większą popularność zarówno w praktyce, jak i w badaniach nad bezpieczeństwem, co odzwierciedlają liczne opracowania naukowe inicjujące tzw. „resiliencism” w studiach nad bezpieczeństwem.

Ewolucja światowego zarządzania kryzysowego przebiegała od zimnowojennej obrony cywilnej (skoncentrowanej na ochronie przed skutkami konfliktu zbrojnego) ku holistycznemu systemowi disaster risk management. Kluczowe katastrofy – zarówno naturalne, jak i spowodowane przez człowieka – wymuszały poszerzenie zakresu działań (od reagowania na zagrożenia wojenne po reagowanie na katastrofy techniczne, ekologiczne czy terrorystyczne) oraz zmianę filozofii z podejścia reaktywnego na proaktywne. Innymi słowy, dokonano się przejście od „civil defense” do „disaster risk reduction” – od ochrony przed skutkami wojny do budowania społecznej odporności na wszelkie zagrożenia. Oś czasu przedstawiona na rysunku 6 ilustruje globalne przemiany, ukazując m.in.: instytucjonalizację obrony

¹⁸¹ M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>

cywilnej. Na osi poziomej zaznaczono kluczowe wydarzenia – u góry kamienie milowe instytucjonalne i międzynarodowe inicjatywy, a u dołu największe katastrofy.



Rysunek 6. Globalne przemiany w podejściu do redukcji ryzyka katastrof (lata 1979-2015)

Źródło: opracowanie własne.

Analizując rozwój wspólnych mechanizmów w Europie i Unii Europejskiej, można zauważyć, że Europa w drugiej połowie XX wieku również wypracowywała stopniowo kooperacyjne podejście do ochrony ludności, ucząc się na kolejnych tragediach. Wydarzenia takie jak katastrofa jądrowa w Czarnobylu (1986 r.), która skażeniem dotknęła wielu państw, wielkie powodzie (np. powódź tysiąclecia na Odrze w 1997 r. oraz powódź na Dunaju w 2002 r.), czy ekstremalne zjawiska pogodowe (huragany, wichury w północnej Europie) uświadomiły rządów, że zagrożenia nie respektują granic. Niezbędna stała się zatem współpraca transgraniczna w działaniach ratunkowych i wymiana informacji o ryzykach. W latach 80. państwa Europy zaczęły zawierać pierwsze porozumienia bilateralne o wzajemnej pomocy w razie klęsk żywiołowych, a na forum Wspólnot Europejskich pojawiły się inicjatywy wymiany informacji o zagrożeniach (np. system wczesnego powiadamiania o awariach jądrowych ECURIE, uruchomiony po Czarnobylu w 1987 r.). Przełomowym krokiem było jednak utworzenie w październiku 2001 r. Mechanizmu Ochrony Ludności Unii Europejskiej (Union Civil Protection Mechanism – UCPM) na mocy decyzji Rady UE. Mechanizm ten został powołany, aby usprawnić współpracę między krajowymi służbami ochrony ludności, ułatwić szybkie i skoordynowane reagowanie w razie poważnych zagrożeń oraz umożliwić wzajemną pomoc państwom członkowskim. Odpowiedzialność podstawowa za ochronę ludności spoczywa na państwie dotkniętym katastrofą, ale gdy sytuacja je przerasta, może ono zwrócić

się o wspólnotowe wsparcie. Każde państwo na świecie (nie tylko należące do UE) może poprosić o pomoc poprzez Mechanizm – a koordynacją działań zajmuje się wtedy Komisja Europejska we współpracy z uczestniczącymi państwami. Od początku udział w Mechanizmie wzięły nie tylko kraje UE, ale też kilka państw spoza Unii (dziś jest 9 takich uczestników, m.in. Norwegia, Turcja, Serbia, Ukraina). Operacyjne serce Mechanizmu stanowi utworzone wraz z nim w 2001 r. Centrum Monitorowania i Informacji (Monitoring and Information Centre, MIC) – niewielka jednostka w strukturze Komisji (DG ECHO) pełniąca rolę całodobowego punktu kontaktowego. MIC zbierał zgłoszenia o nadzwyczajnych zdarzeniach i dystrybuował prośby o pomoc do wszystkich państw uczestniczących. W 2013 r., w ramach reformy prawnej Mechanizmu, MIC przekształcono w nowocześniejsze Centrum Koordynacji Reagowania Kryzysowego (Emergency Response Coordination Centre, ERCC). Obecnie ERCC działa 24/7 w Brukseli, monitorując sytuacje nadzwyczajne na świecie i koordynując oferty pomocy z państw europejskich. Dzięki dedykowanej platformie komunikacyjnej (CECIS) państwo zgłaszające kryzys oraz państwa oferujące pomoc mogą w trybie ciągłym wymieniać informacje o potrzebach i dostępnych zasobach, co bardzo usprawnia mobilizację wsparcia. Mechanizm dysponuje także tzw. Europejską Pulą Ochrony Ludności – są to deklarowane przez państwa zasoby (moduły ratownicze, zespoły ekspertów, specjalistyczny sprzęt), utrzymywane w gotowości do natychmiastowego użycia w razie aktywacji Mechanizmu. Koszty transportu i operacji w ramach Mechanizmu są współfinansowane ze środków Komisji – obecnie Unia pokrywa co najmniej 75% kosztów wysłania pomocy międzynarodowej, co zachęca kraje do dzielenia się zasobami¹⁸².

W pierwszych latach funkcjonowania UCPM był wielokrotnie uruchamiany – m.in. podczas reagowania na trzęsienie ziemi w Algierii (2003 r.), ogromne tsunami na Oceanie Indyjskim (2004 r.), huragan Katrina w USA (2005 r.) czy pożary lasów w Grecji (2007 r.). Doświadczenia te wykazały potrzebę wzmocnienia Mechanizmu. W 2007 r. znowelizowano decyzję ramową, a kompleksowa reforma nastąpiła w grudniu 2013 r. wraz z przyjęciem

¹⁸² F. Iannuli, EU Civil Protection Mechanism: History and Perspectives, TEMA Project, 11.05.2023, <https://tema-project.eu/articles/eu-civil-protection-mechanism-history-and-perspectives>, [dostęp: 22.09.2025].

decyzji nr 1313/2013/UE, która ujednoliciła przepisy dotyczące zapobiegania, gotowości i reagowania na katastrofy w UE. Wprowadzono m.in. obowiązek sporządzania przez państwa krajowych ocen ryzyka i planów zarządzania ryzykiem (aby ujednolicić podejście do analiz zagrożeń), a także utworzono program wspólnych szkoleń i ćwiczeń finansowanych przez UE. Decyzja 1313 umocniła również rolę ERCC oraz ustanowiła podstawy prawne do stworzenia dodatkowej rezerwy zasobów na poziomie unijnym.

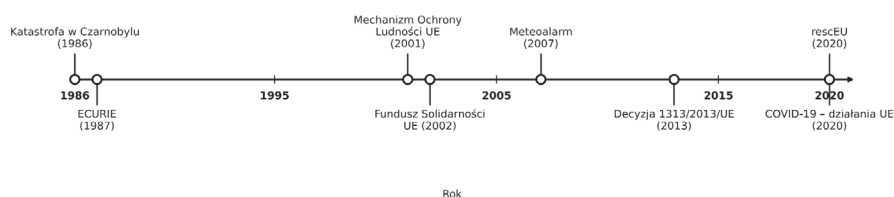
Najnowszym etapem rozwoju jest inicjatywa rescEU uruchomiona w 2019 r. – stanowi ona ponadnarodową europejską rezerwę najcenniejszych środków ratunkowych, w pełni finansowaną z budżetu UE. Pomysł rescEU zrodził się po serii katastrofalnych pożarów lasów w Europie (m.in. w Portugalii w 2017 r.), gdy okazało się, że suma krajowych zasobów gaśniczych bywa niewystarczająca. W ramach rescEU Unia zakupiła wspólną flotę samolotów i śmigłowców gaśniczych do zwalczania pożarów – w 2022 r. dostępnych było 12 samolotów i 1 śmigłowiec rozlokowanych w kilku państwach europejskich. Utworzono także strategiczne rezerwy sprzętu medycznego, kontenerowych szpitali polowych i mobilnych laboratoriów CBRN, co okazało się niezwykle przydatne w czasie pandemii COVID-19 (mechanizm rescEU dostarczał m.in. maseczki, respiratory i szczepionki do państw najbardziej dotkniętych). RescEU stanowi zabezpieczenie ostatniej instancji – jest uruchamiany, gdy zdolności reagowania państw członkowskich zostaną przekroczone, zapewniając bezpośrednio ze szczebla unijnego brakujące zasoby. Drugim filarem europejskiej współpracy jest wczesne ostrzeganie i prewencja ryzyka. Po doświadczeniach niszczycielskich powodzi z lat 90. (kulminacja – wielka powódź w dorzeczu Łaby i Dunaju w 2002 r.) uznano, że brakowało skoordynowanych prognoz hydrologicznych obejmujących cały kontynent. W konsekwencji Komisja Europejska sfinansowała stworzenie już w 2002 r. Europejskiego Systemu Ostrzegania Przeciwpowodziowego (EFAS). Jego zadaniem jest dostarczanie kilkudniowych ostrzeżeń o groźbie powodzi na dużych rzekach oraz przygotowywanie jednolitych map zagrożenia powodziowego dla obszaru Europy. Projekt EFAS rozwinęło unijne Centrum Badawcze JRC, a od 2012 r. system jest prowadzony operacyjnie przez Centrum Prognoz Pogody ECMWF w Reading. Dzięki EFAS powodzie o charakterze transgranicznym można przewidywać z większym wyprzedzeniem i skuteczniej informować zagrożone kraje. Równolegle UE uruchomiła system

monitorowania pożarów lasów (European Forest Fire Information System – EFFIS), system Meteoalarm integrujący ostrzeżenia meteorologiczne z całej Europy oraz rozwinęła sieć centrów reagowania na zagrożenia zdrowotne (np. dla epidemii). W 2012 r. zintegrowano wiele z tych usług w programie Copernicus Emergency Management Service, który udostępnia dane satelitarne i analizy (np. mapy sytuacyjne, oceny zniszczeń) na potrzeby służb kryzysowych. Ważną inicjatywą było również ustanowienie w 2002 r. Funduszu Solidarności UE, z którego udzielana jest pomoc finansowa krajom dotkniętym klęskami żywiołowymi o dużej skali. Fundusz ten wspiera odbudowę infrastruktury i pokrycie najpilniejszych wydatków po katastrofach – Polska kilkakrotnie korzystała z tych środków (np. po powodzi w 2010 r.). Warto podkreślić, że mechanizm solidarności finansowej uzupełnia mechanizm operacyjny UCPM: tam gdzie brakuje zasobów – przychodzi wsparcie eksperckie i rzeczowe z Mechanizmu, tam gdzie brakuje funduszy na odbudowę – pomocny jest Fundusz Solidarności¹⁸³.

Dzięki opisanym działaniom Europa wypracowała unikalny model współpracy w dziedzinie ochrony ludności. Mechanizm Ochrony Ludności UE do końca 2023 r. był aktywowany setki razy – zarówno wewnątrz Unii (m.in. przy pożarach Szwecji w 2018 r., trzęsieniu ziemi we Włoszech w 2016 r., podczas pandemii COVID-19 od 2020 r. czy po rosyjskiej agresji na Ukrainę w 2022 r.), jak i poza jej granicami (np. pomoc ofiarom trzęsienia ziemi na Haiti w 2010 r., epidemii eboli w Afryce, eksplozji w Bejrucie 2020 r.). W ramach Mechanizmu kraje UE nieodpłatnie udostępniają sobie nawzajem wyspecjalizowane moduły ratownicze (np. grupy poszukiwawczo-ratownicze USAR, wysoko wydajne pompy, medyczne zespoły ratunkowe, pontony, mosty tymczasowe itd.), co znacząco podnosi zdolność reagowania w pierwszych dniach kryzysu. Wspólne europejskie podejście sprzyja też uczeniu się na doświadczeniach – po każdej dużej operacji ratowniczej prowadzone są analizy i raporty, na podstawie których udoskonala się procedury i standardy szkolenia. Można zatem mówić o swoistym „europejskim systemie zarządzania kryzysowego”, który stale się doskonali i integruje, zachowując jednocześnie subsydiarność (wsparcie trafia tam, gdzie jest potrzebne, ale nie zastępuje działań lokalnych władz).

¹⁸³ The European Flood Awareness System (EFAS) at ECMWF: towards operational implementation, ECMWF Newsletter, 131, 2012.

Na rysunku 7 zobrazowano najważniejsze etapy rozwoju europejskiego systemu ochrony ludności: od pierwszych inicjatyw (Czarnobyl w 1986 r., porozumienia dwustronne), poprzez utworzenie Mechanizmu Ochrony Ludności (2001 r.) i jego reformy (2007 r., 2013 r.), aż po inaugurację programu rescEU (2019 r.) i operacje w okresie pandemii COVID-19. Dodatkowo zaznaczono rozwój systemów wczesnego ostrzegania (EFAS od 2003 r., Meteoalarm w 2007 r., Copernicus EMS w 2012 r.) oraz ustanowienie Funduszu Solidarności (2002 r.).



Rysunek 7. Kluczowe etapy rozwoju europejskiego systemu ochrony ludności

Źródło: opracowanie własne.

Kolejnym punktem rozważań jest geneza i ewolucja zarządzania kryzysowego w Polsce. W Polsce system ochrony ludności przez większą część XX wieku opierał się na modelu Obrony Cywilnej (OC) kształtowanym według wzorców bloku wschodniego. Od 1951 r. funkcjonowała formacja OC podporządkowana Ministerstwu Obrony Narodowej, której głównym celem była ochrona ludności i dóbr na wypadek konfliktu zbrojnego, zwłaszcza ataku nuklearnego. Zgodnie z definicją przyjętą w protokołach dodatkowych do Konwencji Genewskich (Polska ratyfikowała Protokoły I i II z 1977 r.), do zadań obrony cywilnej należało m.in. ostrzeganie i alarmowanie, organizowanie ewakuacji, zapewnienie schronów, zaciemnianie, ratownictwo i pierwsza pomoc, a także doraźna likwidacja skażeń i uszkodzeń infrastruktury. W praktyce jednak w okresie PRL OC była strukturą o charakterze wojskowym i hierarchicznym – istniały oddziały OC przewidziane głównie do działania w czasie wojny, a w czasie pokoju rola OC w reagowaniu na klęski żywiołowe czy awarie przemysłowe była ograniczona i drugorzędna. Obrona cywilna koncentrowała się na przygotowaniach do potencjalnej wojny (np. budowa schronów, ćwiczenia ludności w zakresie obrony przed bronią masowego rażenia), zaś reagowanie na katastrofy w czasie pokoju

pozostawiano przede wszystkim straży pożarnej i innym służbom resortu spraw wewnętrznych. OC posiadała rozbudowaną strukturę – od Szefa OC Kraju (będącego wiceministrem obrony) po szefów OC województw, miast i gmin. Formalnie zadania OC obejmowały również współdziałanie w zwalczaniu klęsk żywiołowych w czasie pokoju, ale – co znamienne – większość uwagi i zasobów skupiano na scenariuszu konfliktu zbrojnego.

Po przełomie 1989 r. Polska stanęła przed koniecznością dostosowania systemu ochrony ludności do nowych realiów politycznych i zagrożeń. Pojawiło się pytanie, czy reformować istniejącą obronę cywilną, czy też budować zupełnie nowy system na wzór rozwiązań zachodnich (gdzie rozwijały się już koncepcje cywilnego zarządzania kryzysowego). Przez pierwsze lata transformacji OC nadal podlegała MON, jednak jej znaczenie malało – brakowało środków na jej utrzymanie, a społeczeństwo i media coraz krytyczniej patrzyły na archaiczną formację przygotowującą się na wojnę nuklearną, podczas gdy realnie groziły nam powodzie, awarie i inne klęski. Przełomowym momentem okazała się katastrofalna „powódź tysiąclecia” z lipca 1997 r. Klęska ta, dotycząca południową i zachodnią Polskę (Odra i dopływy), obnażyła poważne braki w istniejącym systemie reagowania: nieskuteczny obieg informacji, spóźnione ostrzeganie ludności, słabą koordynację działań straży, wojska i władz lokalnych. W obliczu tej tragedii rząd podjął decyzję o radykalnych zmianach. Jeszcze w 1997 r. wyłączono obronę cywilną spod nadzoru MON i podporządkowano ją resortowi spraw wewnętrznych (MSWiA). Szefem Obrony Cywilnej Kraju mianowano gen. brygadiera Feliksa Delę – dotychczasowego Komendanta Głównego Państwowej Straży Pożarnej, odznaczonego za dowodzenie akcjami podczas powodzi. Był to wyraźny sygnał zmiany podejścia: postawiono na fachowość służb ratowniczych i integrację OC z systemem bezpieczeństwa wewnętrznego państwa. Gen. Dela, jako Szef OC Kraju w latach 1997-1998, opracował założenia przekształcenia tradycyjnej OC w nowoczesny, powszechny system ochrony ludności oparty na zasadzie, że główną siłą wykonawczą stanowią zawodowe służby ratownicze (PSP, Policja, pogotowie, wyznaczone jednostki wojskowe), wspierane przez formacje OC oraz organizacje społeczne (OSP, PCK, itd.). Rozpoczęto też zmiany organizacyjne: w miejsce wojskowego Sztabu OC utworzono w MSWiA cywilny Urząd Szefa Obrony Cywilnej Kraju (później przemianowany na Urząd Zarządzania Kryzysowego i Ochrony Ludności). Na szczeblu

terenowym planowano stworzyć sieć centrów zarządzania kryzysowego pracujących w trybie ciągłym. Część z tych zamierzeń udało się zrealizować pod koniec lat 90. Wprowadzona od 1 stycznia 1999 r. reforma administracyjna (utworzenie 16 województw i powiatów) posłużyła do zmian struktur OC/zarządzania kryzysowego. Zlikwidowano wówczas dawne Wojewódzkie Inspektoraty OC, a ich zadania przejęły Wydziały Bezpieczeństwa i Zarządzania Kryzysowego w urzędach wojewódzkich. W każdym powiecie utworzono zaś Powiatowe Centrum Zarządzania Kryzysowego (PCZK) – początkowo w formie małego zespołu dyżurnych, często ulokowanego przy komendzie Państwowej Straży Pożarnej. Były to pierwsze załączki lokalnych centrów reagowania kryzysowego, choć początkowo brak im było pełnego umocowania prawnego. Niemniej od 1999 r. na poziomie powiatów zaczął funkcjonować stały mechanizm monitorowania zagrożeń i alarmowania służb. Gen. Dela zapoczątkował też opracowanie założeń pierwszej ustawy o stanie klęski żywiołowej – zanim jednak doszło do jej uchwalenia, nastąpiła zmiana rządu. W październiku 1998 r. nowy rząd odwołał Feliksa Delę ze stanowiska Szefa OC Kraju (przeszedł on w stan spoczynku). Mimo to kierunek reformy został utrzymany – stopniowo budowano zręby systemu zarządzania kryzysowego, choć brakowało jeszcze kompleksowych regulacji.

Pierwszym ważnym aktem prawnym była ustawa z 18 kwietnia 2002 r. o stanie klęski żywiołowej, będąca jedną z trzech ustaw o stanach nadzwyczajnych przewidzianych w nowej Konstytucji (obok stanu wyjątkowego i wojennego). Ustawa ta wprowadziła definicję stanu klęski żywiołowej oraz procedury jego wprowadzania i znoszenia. Określiła m.in. zasady działania władz w sytuacji poważnej katastrofy naturalnej lub awarii technicznej – w tym katalog dopuszczalnych ograniczeń praw obywateli na zagrożonym obszarze. Przewidziano np. możliwość przymusowej ewakuacji, całkowitej lub częściowej reglamentacji zaopatrzenia, zakazu podwyższania cen, obowiązku świadczeń rzeczowych i osobistych, a także innych ingerencji koniecznych do opanowania sytuacji. Ustawa zobowiązała też państwo do rekompensaty strat poniesionych wskutek takich działań. Choć akt ten dotyczył jedynie stanu nadzwyczajnego, jego uchwalenie wymusiło doprecyzowanie kompetencji organów w sytuacjach kryzysowych i stało się impulsem do budowy stałych struktur planistyczno-decyzyjnych (takich jak zespoły zarządzania kryzysowego na wszystkich szczeblach).

Kulminacją procesu tworzenia nowego systemu była ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, która weszła w życie w 2007/2008 i kompleksowo uregulowała organizację, zasady działania oraz kompetencje organów w systemie zarządzania kryzysowego (SZK). Ustawa ta zdefiniowała najważniejsze pojęcia – m.in. zarządzanie kryzysowe jako działalność organów władzy publicznej, będącą elementem kierowania bezpieczeństwem narodowym, polegającą na zapobieganiu sytuacjom kryzysowym, przygotowaniu się na wypadek ich wystąpienia, reagowaniu na nie oraz odtwarzaniu infrastruktury i zasobów. Wprowadziła również definicję sytuacji kryzysowej – rozumianej jako sytuacja negatywnie wpływająca na bezpieczeństwo ludzi, mienia lub środowiska, charakteryzująca się znacznym ograniczeniem w działaniu właściwych organów administracji wobec nieadekwatności posiadanych sił i środków. Pojęcie to stało się kluczowe dla uruchamiania procedur kryzysowych (nie każda awaria czy zdarzenie jest sytuacją kryzysową – tylko takie, które przekracza rutynowe możliwości reagowania). Ustawa z 2007 r. zdefiniowała ponadto infrastrukturę krytyczną jako systemy i powiązane z nimi obiekty, urządzenia i usługi kluczowe dla bezpieczeństwa państwa i obywateli, m.in. zaopatrzenia w energię, paliwa, żywność, wodę, łączności i telekomunikacji, finansowe, ochrony zdrowia, transportowe, ratownicze czy systemy zaopatrywania w środki chemiczne i promieniotwórcze. Ochrona infrastruktury krytycznej stała się nowym priorytetem – ustawa nałożyła na jej operatorów obowiązek przygotowywania planów ochrony i utrzymywania zapasowych rozwiązań (opracowano później Narodowy Program Ochrony IK).

Ustawa o zarządzaniu kryzysowym ustanowiła czteropoziomowy układ organizacyjny SZK: poziom centralny (krajowy), wojewódzki, powiatowy i gminny – przypisując każdemu z nich właściwe organy oraz zadania. Organami właściwymi w sprawach zarządzania kryzysowego zostali: na poziomie kraju – Rada Ministrów (lub w sytuacjach pilnych Minister Spraw Wewnętrznych), w województwie – wojewoda, w powiecie – starosta, w gminie – wójt/burmistrz/prezydent miasta. Przy tych organach zaczęły funkcjonować zespoły zarządzania kryzysowego (odpowiednio: Rządowy Zespół Zarządzania Kryzysowego przy RM, wojewódzkie, powiatowe i gminne ZZK) jako ciała opiniotawczo-doradcze złożone z przedstawicieli służb, inspekcji i ekspertów. Ustawa formalnie usankcjonowała też istnienie

centrów zarządzania kryzysowego na każdym szczeblu (Rządowe Centrum Bezpieczeństwa, Wojewódzkie, Powiatowe i – opcjonalnie – Gminne CZK) działających w trybie całodobowym. Wprowadziła ponadto obowiązek opracowywania planów zarządzania kryzysowego – na poziomie krajowym (Krajowy Plan Zarządzania Kryzysowego zatwierdzany przez RM) oraz w każdym województwie, powiecie i gminie. Dokumenty te, aktualizowane co dwa lata, zawierają scenariusze zagrożeń, procedury reagowania i zasady współdziałania wszystkich zaangażowanych podmiotów. Ustawa z 2007 r. wraz z aktami wykonawczymi (np. rozporządzeniem PRM z lipca 2008 r. ws. organizacji RCB) stworzyła zatem formalne podstawy nowoczesnego systemu ochrony ludności i zarządzania kryzysowego w Polsce.

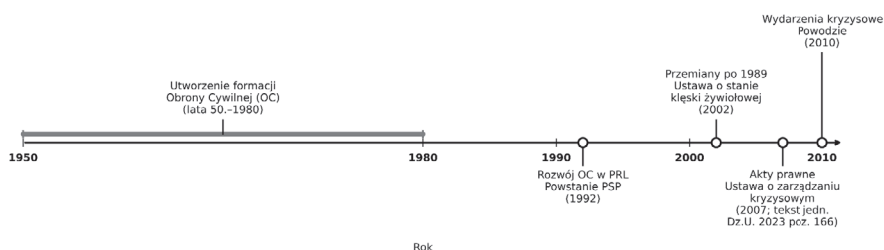
Od czasu wejścia w życie ustawy SZK w praktyce przechodzi systematyczny sprawdzian i ewolucję. Już w maju-czerwcu 2010 r. kraj doświadczył największej od lat powodzi (Wisła, Odra i ich dorzecza), która była testem dla nowych struktur. Skoordynowana akcja ratownicza z udziałem tysięcy strażaków PSP i OSP, wojska, policji i administracji pokazała zasadność wprowadzonych zmian – choć ujawniła też obszary do poprawy (np. niedostatki lokalnych systemów ostrzegania powodziowego czy potrzebę lepszego planowania ewakuacji dużej liczby ludzi i zwierząt). W następstwie powodzi 2010 r. rząd przeznaczył znaczne środki na modernizację infrastruktury przeciwpowodziowej (wałów, polderów), a także wdrożył Regionalny System Ostrzegania (RSO) – platformę powiadamiania SMS i poprzez telewizję o lokalnych zagrożeniach. W kolejnych latach wzrosła świadomość nowych typów zagrożeń: terrorystycznych i asymetrycznych. Choć Polska nie padła ofiarą spektakularnego zamachu, to zamachy w Madrycie (2004 r.), Londynie (2005 r.), a następnie w Paryżu, Brukseli, Berlinie (2015-2016 r.) spowodowały uwzględnienie scenariuszy ataków terrorystycznych (w tym z użyciem broni CBRN) w krajowych planach zarządzania kryzysowego. Przed turniejem EURO 2012 w Polsce kładziono szczególny nacisk na przygotowanie służb na wypadek zamachu podczas imprezy masowej – zorganizowano m.in. wieloszczeblowe ćwiczenie COBRA-2010 symulujące atak terrorystyczny w trakcie meczu piłkarskiego. W 2016 r. uchwalono zaś specjalną ustawę antyterrorystyczną, która wzmocniła uprawnienia ABW i Policji w zakresie zapobiegania i reagowania na zagrożenia terrorystyczne.

Niezwyczajnym wyzwaniem okazała się pandemia COVID-19 od marca 2020 r. – kryzys długotrwały, o charakterze globalnym, którego nie ogłoszono formalnie jako stanu klęski żywiołowej, ale de facto zarządzano nim w trybie nadzwyczajnym (wprowadzono stan zagrożenia epidemicznego, a następnie stan epidemii na podstawie specustawy z 2 marca 2020 r.). Rządowy Zespół Zarządzania Kryzysowego zbierał się niemal codziennie, a Rządowe Centrum Bezpieczeństwa koordynowało działania międzyresortowe: od zamknięcia granic, przez organizację szpitali tymczasowych, po dystrybucję masek i szczepionek. Kryzys ujawnił wagę posiadania rezerw strategicznych – w 2021 r. utworzono Agencję Rezerw Strategicznych, która przejęła zadania gromadzenia i wydawania rezerw państwowych (nie tylko medycznych). Pandemia wykazała też znaczenie współpracy międzynarodowej – Polska skorzystała z pomocy UE (mechanizm rescEU dostarczył m.in. sprzęt medyczny), a jednocześnie wysłała własne zespoły medyczne do krajów takich jak Włochy.

Obecnie polski system zarządzania kryzysowego jest rozbudowany i wielosektorowy, oparty na zasadach decentralizacji i pomocniczości. Na wszystkich szczeblach administracji funkcjonują zespoły zarządzania kryzysowego (krajowy, 16 wojewódzkich, powiatowe, gminne), a w urzędach – centra zarządzania kryzysowego zapewniające całodobowy przepływ informacji o zagrożeniach. Zasadą jest, że kryzysem zarządza ten szczebel, na którym on wystąpił, a wyższe szczeble włączają się tylko gdy środki lokalne są niewystarczające (to realizacja konstytucyjnej zasady pomocniczości). W razie największych katastrof wojewoda może przejąć koordynację działań i wydawać wiążące polecenia niższym organom (tzw. zasada jednolitego kierownictwa w sytuacji kryzysowej). W działania kryzysowe angażują się wszystkie podstawowe służby ratownicze: Państwowa Straż Pożarna (i Ochotnicze Straże Pożarne jako element Krajowego Systemu Ratowniczo-Gaśniczego), Policja, Państwowe Ratownictwo Medyczne, a także inspekcje (sanitarna, weterynaryjna, ochrony środowiska) oraz wojsko (Siły Zbrojne RP mogą być użyte do wsparcia cywilnych służb na mocy art. 26 ustawy o zarządzaniu kryzysowym). Coraz istotniejszą rolę w systemie ochrony ludności odgrywa społeczeństwo obywatelskie, w szczególności organizacje pozarządowe oraz wolontariusze. Ich zaangażowanie widoczne było m.in. podczas kryzysu uchodźczego w latach 2021-2022, kiedy to

tysiące obywateli spontanicznie udzielało wsparcia uchodźcom z Ukrainy, skutecznie uzupełniając działania instytucjonalne. System podlega stałemu doskonaleniu – w odpowiedzi na pojawiające się zagrożenia, takie jak cyberataki, dezinformacja czy działania o charakterze hybrydowym, opracowywane są nowe procedury i plany reagowania. Choć eksperci zwracają uwagę na pewne wyzwania, takie jak nadmierna sformalizowana struktura, silne podziały resortowe czy wpływy polityczne w niektórych obszarach, przyjęty model organizacyjny – oparty na jednoosobowym kierownictwie i podziale terytorialnym – wykazuje ogólną skuteczność i funkcjonalność w ostatnich kilkunastu latach. Potwierdzeniem skuteczności były zarówno akcje przeciwpowodziowe, zabezpieczenie wielkich imprez jak Euro w 2012 r., jak i zarządzanie niefortunną sytuacją pandemiczną. Można więc stwierdzić, że Polska zbudowała nowoczesny system zarządzania kryzysowego, spójny z systemem bezpieczeństwa narodowego i zdolny do reagowania na zróżnicowane zagrożenia – od klęsk żywiołowych, przez awarie techniczne, po wyzwania związane z bezpieczeństwem zdrowotnym czy migracyjnym¹⁸⁴.

Na rysunku 4 przedstawiono oś czasu kluczowych etapów ewolucji polskiego systemu zarządzania kryzysowego: utworzenie formacji OC (lata 50.), rozwój OC w PRL, przemiany po 1989 r. (powstanie PSP w 1992 r., reforma OC w latach 1997-1999, powódź w 1997 r. jako katalizator zmian), następnie akty prawne (ustawa o stanie klęski w 2002 r., ustawa o ZK w 2007 r.) oraz główne testy systemu w praktyce (powódzie w 2010 r., przygotowania antyterrorystyczne w 2012 r., pandemia w 2020 r.).



Rysunek 8. Ewolucja polskiego systemu zarządzania kryzysowego

Źródło: opracowanie własne.

¹⁸⁴ M. Stępka, Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, *Przegląd Politologiczny*, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>

Kolejnym ważnym elementem są podstawy prawne i instytucjonalne zarządzania kryzysowego w Polsce. Fundamentem prawnym polskiego systemu zarządzania kryzysowego jest Konstytucja RP z 1997 r., która w art. 5 zobowiązuje państwo do strzeżenia bezpieczeństwa obywateli¹⁸⁵. Konstytucja przewiduje możliwość wprowadzenia trzech stanów nadzwyczajnych: stanu wojennego, stanu wyjątkowego oraz stanu klęski żywiołowej. Każdy z tych stanów uruchamia się w sytuacjach szczególnego zagrożenia, gdy zwykle środki konstytucyjne są niewystarczające. Ustawa zasadnicza określa ogólne ramy tych stanów – ich doprecyzowanie nastąpiło w ustawach zwykłych na początku lat 2000.

Warto krótko scharakteryzować stany nadzwyczajne z perspektywy zarządzania kryzysowego:

1. Stan wojenny – może być wprowadzony w razie zewnętrznej agresji na terytorium RP lub gdy z umów sojuszniczych wynika zobowiązanie do obrony wspólnie z innym państwem napadniętym. Wprowadza się go na części lub całości terytorium państwa na mocy rozporządzenia Prezydenta RP (na wniosek Rady Ministrów). Ten stan, najcięższy, nie jest bezpośrednio narzędziem zarządzania kryzysowego (dotyczy bezpieczeństwa państwa, a nie klęsk żywiołowych).
2. Stan wyjątkowy – przeznaczony na sytuacje zagrożenia ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego o charakterze wewnętrznym (np. zamieszki, próba zamachu stanu). Wprowadza go Prezydent RP na wniosek Rady Ministrów, na czas do 90 dni (z możliwością jednorazowego przedłużenia za zgodą Sejmu o maks. 60 dni). Stan wyjątkowy wiąże się z ograniczeniem niektórych wolności (np. wolności zgromadzeń, działalności organizacji, swobody poruszania się na danym obszarze), lecz zakres tych ograniczeń musi odpowiadać skali zagrożenia i podlega kontroli parlamentu. Stan ten nie był dotąd w III RP wprowadzony (nie licząc lokalnego stanu wyjątkowego na pograniczu polsko-białoruskim w 2021 r. podczas kryzysu migracyjnego).

¹⁸⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228).

3. Stan klęski żywiołowej – ma kluczowe znaczenie dla zarządzania kryzysowego, bo dotyczy poważnych katastrof naturalnych lub awarii technicznych noszących znamiona klęski. Wprowadza go Rada Ministrów w drodze rozporządzenia, na czas do 30 dni (przedłużenie wymaga zgody Sejmu). Stan klęski żywiołowej pozwala legalnie sięgnąć po nadzwyczajne środki – np. ewakuację przymusową ludności z zagrożonego obszaru, de facto przejęcie przez władze dystrybucji podstawowych dóbr (żywność, woda) poprzez reglamentację, zakaz podwyższania cen na towary pierwszej potrzeby, kierowanie pracowników do określonych zadań czy użycie cudzej własności (nieruchomości, pojazdów) do akcji ratunkowej. Wszystkie te ograniczenia wolności i praw muszą być wyszczególnione w rozporządzeniu o wprowadzeniu stanu i obowiązywać tylko na obszarze dotkniętym klęską. Stan klęski żywiołowej w III RP ogłaszano kilkakrotnie lokalnie (np. podczas powodzi w 1997 i 2010 r. nie ogłaszano, ale w 2024 r. wprowadzono go na terenie części woj. dolnośląskiego, opolskiego i śląskiego dotkniętych powodzią – po raz pierwszy na większą skalę). Jest to środek ostateczny – w praktyce większość sytuacji kryzysowych udaje się opanować bez sięgania po stan nadzwyczajny, na podstawie zwykłych procedur i ustaw.

W kontekście prawnym należy wspomnieć, że wprowadzenie stanu nadzwyczajnego (zwłaszcza stanu klęski żywiołowej) ma pewne następstwa – np. przesunął termin wyborów, jeśli miałyby się odbyć w trakcie lub 90 dni po stanie¹⁸⁶. Z punktu widzenia zarządzania kryzysowego, ważne jest jednak to, że nawet bez ogłoszenia stanu klęski, organy władzy mają dziś szeroki wachlarz instrumentów do reagowania (co pokazała pandemia COVID-19, którą formalnie zarządzano bez stanu nadzwyczajnego, wykorzystując ustawę o chorobach zakaźnych). Stan klęski żywiołowej pozostaje więc swoistą „polisą awaryjną” na sytuacje absolutnie skrajne, gdy trzeba by sięgnąć po najbardziej radykalne ograniczenia praw (np. obowiązek świadczeń osobistych – czyli przymus pracy na potrzeby akcji ratunkowej czy odbudowy).

¹⁸⁶ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228).

Na co dzień natomiast zarządzanie kryzysowe odbywa się w trybie „zwykłym” – na podstawie wspomnianej ustawy z 2007 r. oraz szeregu ustaw sektorowych.

Poza ustawami o stanach nadzwyczajnych, centralnym aktem prawnym w tej dziedzinie jest wspomniana ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (wielokrotnie nowelizowana)¹⁸⁷. To ona utworzyła zintegrowany system czterech szczebli, określiła zadania poszczególnych organów i zasady ich współdziałania. Na podstawie delegacji z tej ustawy wydano liczne rozporządzenia uszczegóławiające – np. rozporządzenie PRM z 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa¹⁸⁸ (określające wewnętrzną strukturę RCB i jego komórki takie jak: wydział monitorowania zagrożeń, wydział planowania cywilnego, wydział infrastruktury krytycznej itd.), czy rozporządzenie MSWiA z 18 stycznia 2011 r. w sprawie form i zakresu dokumentacji planistycznej¹⁸⁹ (standaryzujące zawartość planów zarządzania kryzysowego). Wiele przepisów z zakresu zarządzania kryzysowego znajduje się też w ustawach branżowych regulujących funkcjonowanie poszczególnych służb. Należy tu wymienić choćby: ustawę o Państwowej Straży Pożarnej z 1991 r.¹⁹⁰ (PSP jest zawodową formacją ratowniczą przewidzianą do reagowania na pożary, klęski żywiołowe i inne miejscowe zagrożenia), ustawę o Policji z 1990 r.¹⁹¹ (Policja odpowiada za bezpieczeństwo i porządek publiczny, w sytuacjach kryzysowych prowadzi np. ewakuację, ochronę porządku, akcje poszukiwawcze), ustawę o Państwowym Ratownictwie Medycznym z 2006 r.¹⁹² (regulującą system PRM – karetki i LPR – niosący pomoc medyczną poszkodowanym), ustawę Prawo atomowe z 2000 r.¹⁹³ (określającą system reagowania

¹⁸⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm).

¹⁸⁸ Rozporządzenie PRM z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (Dz.U. z 2008 r. Nr 128, poz. 821).

¹⁸⁹ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2011 r. w sprawie form i zakresu dokumentacji planistycznej.

¹⁹⁰ Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz.U. z 1991 r. Nr 88, poz. 400).

¹⁹¹ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 1990 r. Nr 30, poz. 179).

¹⁹² Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2006 r. Nr 191, poz. 1410).

¹⁹³ Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe (Dz.U. z 2001 r. Nr 3, poz. 18).

na zdarzenia radiacyjne), ustawę o ochronie przeciwpożarowej¹⁹⁴, Prawo wodne¹⁹⁵ (plany zarządzania ryzykiem powodziowym) i inne. Szczególne znaczenie ma też ochrona infrastruktury krytycznej – oprócz zapisów ustawy o ZK powstał Narodowy Program Ochrony IK¹⁹⁶, a właściciele obiektów IK zobowiązani są do przygotowywania szczegółowych planów ciągłości działania i procedur awaryjnych.

Struktura systemu zarządzania kryzysowego w Polsce odpowiada podziałowi administracyjnemu kraju i ma charakter wyraźnie hierarchiczny – od szczebla centralnego, poprzez wojewódzki i powiatowy, aż po poziom gminny. Na poziomie centralnym zlokalizowane są organy odpowiedzialne za strategiczne planowanie, koordynację oraz współpracę międzynarodową. Naczelnym organem jest Rada Ministrów z Prezesem Rady Ministrów na czele, wspierana przez Rządowy Zespół Zarządzania Kryzysowego oraz Rządowe Centrum Bezpieczeństwa, które pełni funkcję krajowego centrum zarządzania kryzysowego, prowadzi całodobowy monitoring zagrożeń, koordynuje ochronę infrastruktury krytycznej i utrzymuje stałą łączność z wojewódzkimi centrami zarządzania kryzysowego. Na poziomie resortowym funkcjonują z kolei centra i zespoły zarządzania kryzysowego poszczególnych ministrów, odpowiedzialne za zagrożenia sektorowe (zdrowotne, transportowe, środowiskowe itp.), współdziałające z RCB i strukturami terenowymi. Poziom wojewódzki reprezentowany jest przez wojewodę jako przedstawiciela rządu w terenie. Wojewoda odpowiada za zarządzanie kryzysowe w skali regionu – zarówno w fazie przygotowania (plany, ćwiczenia, nadzór nad powiatami), jak i reagowania, zwłaszcza gdy zdarzenie obejmuje więcej niż jeden powiat lub przekracza możliwości szczebla powiatowego. Wsparcie zapewniają Wojewódzki Zespół Zarządzania Kryzysowego oraz Wojewódzkie Centrum Zarządzania Kryzysowego pełniące dyżur 24/7 i będące węzłem wymiany informacji między powiatami a poziomem centralnym. Na szczeblu powiatowym organem właściwym jest starosta (lub prezydent miasta na prawach powiatu), który koordynuje działania służb na obszarze powiatu, integruje działania poszczególnych gmin i – przez

¹⁹⁴ Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. z 1991 r. Nr 81, poz. 351).

¹⁹⁵ Ustawa z dnia 18 lipca 2001 r. – Prawo wodne (Dz.U. z 2001 r. Nr 115, poz. 1229).

¹⁹⁶ Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) – dokument rządowy przyjęty uchwałą Rady Ministrów w dniu 26 marca 2013 r.

Powiatowy Zespół oraz Centrum Zarządzania Kryzysowego – zapewnia przepływ informacji oraz wsparcie tam, gdzie możliwości pojedynczej gminy są niewystarczające. Poziom gminny, jako najbliższy obywatelom, pełni funkcję pierwszego reagenta w sytuacjach kryzysowych. To wójt, burmistrz lub prezydent miasta odpowiada za bezpośrednie ostrzeżenie i alarmowanie mieszkańców, organizację ewentualnej ewakuacji, zabezpieczenie podstawowych potrzeb poszkodowanych oraz za bieżącą współpracę z lokalnymi służbami i organizacjami społecznymi. Administracja powiatowa integruje działania jednostek samorządu niższego szczebla, natomiast szczebel wojewódzki koordynuje działania w skali regionalnej oraz zapewnia komunikację z administracją rządową. Całość systemu opiera się na zasadzie subsydiarności – zarządzanie kryzysowe prowadzi się na możliwie najniższym szczeblu, przy uruchamianiu wyższych poziomów tylko wtedy, gdy skala zagrożenia przekracza lokalne możliwości. W literaturze przedmiotu podkreśla się, że skuteczność tego modelu zależy w dużej mierze od sprawnej wymiany informacji oraz wzajemnego zaufania pomiędzy poszczególnymi poziomami administracji. W Polsce proces budowy tego zaufania przebiegał stopniowo, przy czym nadal mogą występować napięcia w relacjach pomiędzy administracją rządową a samorządową – zwłaszcza w kontekście sytuacji o charakterze politycznie wrażliwym, takich jak kryzys migracyjny na granicy państwowej w 2021 r. Niemniej jednak model funkcjonujący w Polsce bywa wskazywany jako przykład relatywnie udanej adaptacji zachodnich koncepcji zarządzania kryzysowego do warunków krajowych, łączący elementy centralizacji z uwzględnieniem lokalnej specyfiki i potrzeb.

Efektywność działań kryzysowych zależy nie tylko od przepisów i struktury, ale też od dostępności środków finansowych i rzeczowych. W Polsce finansowanie zarządzania kryzysowego odbywa się na zasadzie kombinacji budżetów centralnych i samorządowych, ze wsparciem funduszy celowych oraz pomocy międzynarodowej.

Kluczowe mechanizmy finansowe to m.in.:

- Rezerwy celowe budżetu państwa – co roku w ustawie budżetowej wyodrębnia się rezerwę na przeciwdziałanie i usuwanie skutków klęsk żywiołowych. Na 2025 r. rząd zaplanował taką rezerwę w wysokości 3,191 mld zł (zwiększoną w trakcie prac budżetowych w związku z powodziami w 2024 r.). Środki z tej rezerwy uruchamiane są decyzją

Premiera (na wniosek MSWiA lub wojewody) i trafiają np. do samorządów na odbudowę zniszczonych mostów, wałów, dróg czy na zasiłki dla poszkodowanych rodzin. Dodatkowo istnieje odrębna rezerwa na usuwanie skutków powodzi (tzw. rezerwa przeciwpowodziowa). Rezerwy niewykorzystane w danym roku często są odnawiane w kolejnym.

- Budżety jednostek samorządu terytorialnego – każda gmina, powiat i województwo wyodrębnia środki na zarządzanie kryzysowe. Nie są one duże (często to kilkadziesiąt czy kilkaset tysięcy zł rocznie na gminę, kilka milionów na województwo), ale pozwalają na bieżące działania prewencyjne (np. czyszczenie rowów melioracyjnych), utrzymanie centrów kryzysowych czy magazynów przeciwpowodziowych, a także na lokalne ćwiczenia i szkolenia. W razie kryzysu samorządy pokrywają pierwsze wydatki (np. koszty ewakuacji i zakwaterowania ludzi, paliwo dla strażaków) ze swoich budżetów, a potem mogą ubiegać się o dotacje z budżetu państwa.
- Fundusz Solidarności UE (FSUE) – jako państwo członkowskie Polska korzysta z mechanizmu solidarnościowego Unii. Jeśli katastrofa naturalna wyrządzi straty przekraczające określony próg (ok. 0,64% PKB lub 1,5% PKB regionu), rząd może wystąpić do Komisji Europejskiej o pomoc z FSUE. Polska otrzymała takie wsparcie m.in. po powodzi w 2010 r. (ok. 105 mln euro) oraz po suszy rolniczej w 2015 r. Środki te idą na odbudowę infrastruktury publicznej, ale są refundowane post factum (czyli najpierw wydatki ponosi budżet krajowy, później następuje zwrot części kosztów z Brukseli).
- Unijny Mechanizm Ochrony Ludności – jak opisano wyżej, mechanizm ten oferuje głównie wsparcie rzeczowe i eksperckie. Finansowo istotne jest jednak to, że UE pokrywa co najmniej 75% kosztów transportu pomocy (np. samoloty transportowe, ciężarówki) oraz częściowo koszty operacyjne zespołów ratowniczych. Dla Polski oznacza to, że wysyłając moduł za granicę odzyskuje większość wydatków, a w drugą stronę – gdy do nas przyjeżdża pomoc, koszty te nie obciążają budżetu krajowego. Ponadto program rescEU w całości jest finansowany przez UE – np. jeśli polski samolot gaśniczy został kupiony z puli rescEU, to utrzymanie i użycie go w ramach unijnej misji jest refundowane.

- Fundusze celowe i ubezpieczenia – istnieją także krajowe fundusze celowe mogące wspierać działania kryzysowe, np. Fundusz Ochrony Gruntów Rolnych (czasem finansuje usuwanie skutków susz i powodzi rolniczych), Fundusz Zapobiegania i Likwidacji Skutków Klęsk Żywiolowych (w BGK), czy rezerwy w dyspozycji ministrów (np. rezerwa ministra rolnictwa na zwalczanie chorób zwierzęcych). Coraz większą rolę mogą odgrywać ubezpieczenia – np. samorządy zaczynają ubezpieczać infrastrukturę od powodzi, co w razie szkód zmniejsza obciążenie budżetu państwa.
- Zasoby sprzętowe i ludzkie – finansowanie to jedno, ale ważne jest też posiadanie odpowiednich zasobów. Polska dysponuje znaczną liczbą profesjonalnych jednostek ratowniczych: PSP to ok. 30 tys. zawodowych strażaków i 500 specjalistycznych pojazdów ratowniczo-gaśniczych (plus tysiące OSP), Policja ok. 100 tys. funkcjonariuszy, wojsko – kilkanaście tys. żołnierzy w jednostkach mogących wspierać akcje, 21 Brygada WOT dedykowana reagowaniu kryzysowemu itp. Utrzymanie tych sił odbywa się z odpowiednich budżetów formacji (MSWiA finansuje PSP i Policję – co rok ustawa budżetowa zapewnia środki na ich gotowość). Na wypadek kryzysów medycznych rozbudowano rezerwy Agencji Rezerw Strategicznych (maski, szczepionki, leki przeciwpromienne) – to również element zabezpieczenia zasobowego systemu.

Mechanizm finansowania zarządzania kryzysowego jest zatem wieloskładnikowy. Państwo zabezpiecza rezerwy centralne na najpoważniejsze klęski, samorządy utrzymują gotowość na poziomie lokalnym, a Unia Europejska stanowi istotne zaplecze zarówno finansowe (Fundusz Solidarności), jak i operacyjne (Mechanizm OC). W razie dużych katastrof budżet państwa może nowelizować plan finansowy, aby przesunąć dodatkowe środki – przykładowo w 2024 r. po powodzi rząd zwiększył pulę na usuwanie jej skutków o ponad 2 mld zł. Wydatki na zapobieganie (np. budowa wałów, polderów, systemów alarmowych) są częściowo finansowane z funduszy unijnych (Fundusz Spójności, Fundusz Ochrony Środowiska). Ogółem, z ekonomicznego punktu widzenia, rosnąca świadomość ryzyka przekłada się na coraz większe nakłady na redukcję ryzyka katastrof (DRR) – co jest zgodne

z globalnymi tendencjami (inwestowanie w prewencję opłaca się bardziej niż samo reagowanie). Mimo pewnych ograniczeń budżetowych, polski system zdołał zapewnić finansowanie podstawowych potrzeb – co widać po stale rosnących kwotach rezerw kryzysowych (w 2010 r. rezerwa klęskowa wynosiła ok. 1 mld zł, w 2025 r. planuje się już ponad 3 mld zł). Dzięki temu zarządzanie kryzysowe może działać szybciej i skuteczniej, nie czekając na doraźne zbiórki czy pożyczki. Na zakończenie należy wspomnieć, że ważnym uzupełnieniem są mechanizmy międzynarodowe: poza pomocą z UE, Polska współpracuje w ramach NATO (cywilne planowanie awaryjne, ćwiczenia międzynarodowe, np. CMX), a także w regionalnych inicjatywach (np. Grupa Wyszehradzka organizuje wspólne ćwiczenia ratownicze). To wszystko sprawia, że system zarządzania kryzysowego jest stale rozwijany w duchu kooperacji i wymiany doświadczeń – tak by sprostać wyzwaniom, jakie niosą zarówno tradycyjne zagrożenia naturalne, jak i nowe, dynamicznie pojawiające się ryzyka XXI wieku.

2.4. Podstawy prawne i instytucjonalne zarządzania kryzysowego

Fundamentem prawnym polskiego systemu zarządzania kryzysowego jest Konstytucja RP z 1997 r., która w art. 5 zobowiązuje państwo do zapewnienia bezpieczeństwa obywateli. Co istotne, Konstytucja przewiduje możliwość wprowadzenia trzech stanów nadzwyczajnych: stanu wojennego, stanu wyjątkowego oraz stanu klęski żywiołowej¹⁹⁷. Każdy z tych stanów wprowadza się w sytuacjach szczególnego zagrożenia, gdy zwykłe środki konstytucyjne okazują się niewystarczające. Stan wyjątkowy może być wprowadzony przez Prezydenta RP na wniosek Rady Ministrów w razie zagrożenia ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego – na czas do 90 dni (z możliwością jednorazowego przedłużenia o maksymalnie 60 dni za zgodą Sejmu). Z kolei stan klęski żywiołowej wprowadzany jest przez Radę Ministrów w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz ich usunięcia, na

¹⁹⁷ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 228).

okres nie dłuższy niż 30 dni (przedłużenie wymaga zgody Sejmu). Przepisy o stanach nadzwyczajnych określają dopuszczalne ograniczenia wolności i praw obywatelskich oraz szczególne kompetencje organów władzy na czas trwania takich stanów. W kontekście zarządzania kryzysowego szczególne znaczenie ma stan klęski żywiołowej, który może być wprowadzony w przypadku katastrof i klęsk przekraczających możliwości rutynowego reagowania. Podstawowe regulacje dotyczące stanu klęski żywiołowej zawiera Ustawa z 18 kwietnia 2002 r. o stanie klęski żywiołowej¹⁹⁸, która określa tryb wprowadzenia tego stanu, szczegółowy katalog dopuszczalnych ograniczeń praw (np. ewakuacja, obowiązek świadczeń rzeczowych i osobistych) oraz zasady rekompensaty strat. Rozdział XI Konstytucji oraz ustawa z 2002 r. zapewniają zatem ramy prawne do podejmowania nadzwyczajnych działań w obliczu największych katastrof i kryzysów. Warto podkreślić, że ogłoszenie stanu nadzwyczajnego jest rozwiązaniem ostatecznym – w pierwszej kolejności państwo stara się reagować na kryzysy w trybie zwykłych przepisów, a dopiero eskalacja zagrożenia uzasadnia sięgnięcie po reżim stanu wyjątkowego czy klęski żywiołowej.

Centralnym aktem prawnym, który kompleksowo reguluje zarządzanie kryzysowe, jest Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym¹⁹⁹. Ustawa ta utworzyła zintegrowany, wieloszczeblowy system zarządzania kryzysowego, obejmujący administrację rządową i samorządową, a także wybrane podmioty prywatne (np. właścicieli infrastruktury krytycznej). Ustawa z 2007 r. określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania. Wprowadza również legalne definicje najważniejszych pojęć z tej dziedziny, takich jak sytuacja kryzysowa czy infrastruktura krytyczna²⁰⁰. Co więcej, ustawa formułuje zasady finansowania zadań zarządzania kryzysowego – stanowi m.in., że działania te finansowane są z budżetu państwa oraz budżetów jednostek samorządu terytorialnego, z uwzględnieniem rezerw celowych przewidzianych na cele

¹⁹⁸ Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62 poz. 558).

¹⁹⁹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

²⁰⁰ S. Frankiewicz, Zarządzanie w sytuacjach kryzysowych, w: System zarządzania kryzysowego w Polsce. Wybrane aspekty, J. Piwowarski (red.), Kraków-Katowice, Instytut Badań Bezpieczeństwa i Obronności, 2018, s. 9-66, s. 11.

zarządzania kryzysowego. Ustawa o zarządzaniu kryzysowym była nowelizowana, m.in. w 2009 r., kiedy doprecyzowano zakres zadań i wzmocniono rolę Rządowego Centrum Bezpieczeństwa (RCB). Na podstawie ustawy wydano też szereg aktów wykonawczych uszczegóławiających organizację systemu – np. rozporządzenie Prezesa Rady Ministrów z 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa²⁰¹, które określiło strukturę wewnętrzną RCB (m.in. utworzenie w RCB wyspecjalizowanych biur: Monitorowania i Analizy Zagrożeń, Ochrony Infrastruktury Krytycznej itp.). Kolejne rozporządzenia dotyczyły m.in. organizacji zespołów zarządzania kryzysowego²⁰² oraz zasad opracowywania planów zarządzania kryzysowego na różnych poziomach administracji²⁰³. System zarządzania kryzysowego opiera się na wykorzystaniu istniejących struktur państwa oraz na kompetencjach instytucji odpowiedzialnych za bezpieczeństwo i reagowanie na zagrożenia. Dlatego poza ww. ustawami horyzontalnymi istotną rolę odgrywają ustawy sektorowe, regulujące funkcjonowanie służb i podmiotów zaangażowanych w działania kryzysowe. Należą do nich przede wszystkim: Ustawa o Państwowej Straży Pożarnej z 24 sierpnia 1991 r.²⁰⁴ wraz z późniejszymi zmianami – określająca organizację i zadania PSP, która stanowi profesjonalną formację ratowniczą przeznaczoną m.in. do zwalczania pożarów, klęsk żywiołowych i innych miejscowych zagrożeń, Ustawa o Policji z 6 kwietnia 1990 r.²⁰⁵ – regulująca działalność Policji, odpowiedzialnej za utrzymanie bezpieczeństwa i porządku publicznego, w tym uczestniczącej w akcjach ratunkowych i ewakuacyjnych podczas kryzysów, Ustawa o Państwowym Ratownictwie Medycznym z 8 września 2006 r.²⁰⁶ – tworząca system ratownictwa medycznego zapewniający niesienie pomocy ofiarom wypadków i katastrof, a także przepisy dotyczące

²⁰¹ Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (Dz.U. z 2008 r. Nr 128, poz. 821).

²⁰² Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (M.P. 2014 poz. 926).

²⁰³ Rozporządzenie Rady Ministrów z dnia 11 grudnia 2020 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. z 2020 r. poz. 2344).

²⁰⁴ Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz.U. z 1991 r. Nr 88, poz. 400 z późn. zm.).

²⁰⁵ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 1990 r. Nr 30, poz. 179 z późn. zm.).

²⁰⁶ Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2006 r. Nr 191, poz. 1410 z późn. zm.).

innych służb, inspekcji i straży np. ustawy o Inspekcji Sanitarnej²⁰⁷, o Inspekcji Ochrony Środowiska²⁰⁸, a także przepisy dotyczące ochrony ludności i obrony cywilnej obecnie ujęte w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej²⁰⁹. Ponadto szczególne znaczenie ma ochrona infrastruktury krytycznej, uregulowana w ustawie o zarządzaniu kryzysowym oraz w dokumentach strategicznych (jak Narodowy Program Ochrony Infrastruktury Krytycznej)^{210,211}. Zgodnie z ustawą z 2007 r., właściciele i operatorzy obiektów infrastruktury krytycznej zobowiązani są do przygotowania planów ochrony tych obiektów i utrzymywania ich w gotowości²¹². Taka wielopoziomowa podstawa prawna zapewnia zarówno tryb zwyczajny reagowania kryzysowego, jak i tryb nadzwyczajny na wypadek największych zagrożeń.

Ustawa o zarządzaniu kryzysowym wprowadziła jednolite definicje kluczowych pojęć, stanowiące podstawę teoretyczną i organizacyjną systemu. Zarządzanie kryzysowe zostało zdefiniowane jako działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, polegająca na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli poprzez zaplanowane działania, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej²¹³. Definicja ta podkreśla ciągłość procesu zarządzania kryzysowego, obejmującego cztery podstawowe fazy: zapobieganie, przygotowanie, reagowanie i odbudowę. Ważnym elementem jest wskazanie, że zarządzanie kryzysowe stanowi część systemu kierowania bezpieczeństwem narodowym – a więc jest komplementarne wobec innych działań państwa w zakresie bezpieczeństwa

²⁰⁷ Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz.U. z 1985 r. Nr 12, poz. 49 z późn. zm.).

²⁰⁸ Ustawa z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz.U. z 1991 r. Nr 77, poz. 335 z późn. zm.).

²⁰⁹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

²¹⁰ Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r. Nr 83, poz. 541).

²¹¹ Narodowy Program Ochrony Infrastruktury Krytycznej, przyjęty uchwałą Rady Ministrów, Warszawa, Rządowe Centrum Bezpieczeństwa, 2020.

²¹² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 6-6b).

²¹³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 2).

(takich jak obrona narodowa czy porządek publiczny). Integralną częścią definicji jest również odtwarzanie infrastruktury krytycznej, co akcentuje znaczenie zapewnienia ciągłości kluczowych usług i systemów dla funkcjonowania społeczeństwa po kryzysie.

Powiązany pojęciem jest sytuacja kryzysowa, rozumiana jako sytuacja negatywnie wpływająca na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków²¹⁴. Innymi słowy, sytuacja kryzysowa to stan zagrożenia (np. katastrofa naturalna, awaria techniczna, atak terrorystyczny), w którym normalne zasoby i procedury reagowania okazują się niewystarczające, przez co konieczne jest uruchomienie nadzwyczajnych działań i mechanizmów koordynacyjnych. Ta definicja podkreśla dwie cechy kryzysu: skalę skutków (zagrożenie życia, zdrowia, mienia lub środowiska na dużą skalę) oraz trudności w reagowaniu zwykłymi siłami (niewystarczające siły i środki lokalnych organów). Pojęcie sytuacji kryzysowej wyznacza przesłanki do uruchomienia procedur zarządzania kryzysowego – nie każda niebezpieczna sytuacja nim skutkuje, a tylko taka, która przekracza typowe zdolności reagowania właściwych służb.

Kolejnym kluczowym terminem jest infrastruktura krytyczna. Zgodnie z art. 3 ust. 2 ustawy o zarządzaniu kryzysowym, infrastrukturą krytyczną są systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty – w tym obiekty budowlane, urządzenia, instalacje – oraz usługi kluczowe dla bezpieczeństwa państwa i jego obywateli, a także służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, oraz instytucji i przedsiębiorców²¹⁵. Do infrastruktury krytycznej zalicza się m.in. systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatyczne, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, oraz systemy produkcji, magazynowania i stosowania substancji chemicznych i promieniotwórczych. Utrata lub poważne

²¹⁴ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 3 pkt 1).

²¹⁵ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 3 pkt 2).

zakłócenie działania elementów infrastruktury krytycznej może wywołać efekty kaskadowe i poważny kryzys, stąd ich ochrona ma priorytetowe znaczenie. Ustawa nakłada na organy administracji obowiązek sporządzenia Krajowego Programu Ochrony Infrastruktury Krytycznej oraz zobowiązuje właścicieli takich obiektów do przygotowania planów ochrony. Włączenie infrastruktury krytycznej w ramy zarządzania kryzysowego odzwierciedla rosnącą zależność bezpieczeństwa państwa od niezawodności kluczowych usług (energia, telekomunikacja, finanse, itd.).

Warto wyjaśnić również pojęcie organów właściwych w sprawach zarządzania kryzysowego. Tak ustawa określa organy administracji publicznej, na których spoczywa odpowiedzialność za podejmowanie decyzji i kierowanie działaniami kryzysowymi na poszczególnych poziomach. Zgodnie z art. 4 ustawy, organami właściwymi są: Rada Ministrów (na poziomie krajowym, w sytuacjach nagłych rolę tę wykonuje minister właściwy ds. wewnętrznych, informując niezwłocznie Prezesa RM), wojewoda (w województwie), starosta (w powiecie) oraz wójt, burmistrz lub prezydent miasta (w gminie)²¹⁶. Organy te odpowiadają za kierowanie działaniami z zakresu zarządzania kryzysowego na swoim obszarze lub w ramach swojego zakresu kompetencji. W praktyce oznacza to, że np. na szczeblu lokalnym to wójt/burmistrz inicjuje i koordynuje działania ratownicze na terenie gminy, a w razie eskalacji problemu wojewoda może przejąć koordynację w skali regionu. Zasadą jest subsydiarność terytorialna – zarządzanie kryzysowe odbywa się na najniższym szczeblu administracji, który jest w stanie skutecznie reagować (tzw. zasada prymatu układu terytorialnego). Wyższe szczeble (wojewoda, rząd) wkraczają dopiero, gdy skala zagrożenia przekracza możliwości poziomu niższego lub gdy potrzebna jest pomoc z zewnątrz.

Istotnym elementem systemu są również organy pomocnicze i plany. Ustawa przewiduje tworzenie zespołów zarządzania kryzysowego – opiniodawczo-doradczych ciał, które wspierają jednoosobowe organy decyzyjne (premiera, wojewodę, starostę, wójta) w analizie sytuacji i opracowaniu propozycji działań²¹⁷. Na każdym poziomie funkcjonuje zespół zarządza-

²¹⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 3 pkt 4).

²¹⁷ M. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021. <https://doi.org/10.3390/en14248286>

nia kryzysowego: Rządowy Zespół Zarządzania Kryzysowego przy Radzie Ministrów, zespoły wojewódzkie, powiatowe i gminne – w skład których wchodzi przedstawiciele kluczowych służb, inspekcji i straży, eksperci oraz urzędnicy właściwi dla danego szczebla. Ponadto działają Centra Zarządzania Kryzysowego zapewniające całodobową łączność, monitoring i przepływ informacji. Na system składa się także dokumentacja planistyczna – przede wszystkim plany zarządzania kryzysowego opracowywane na poziomie kraju, województw, powiatów i gmin. Krajowy Plan Zarządzania Kryzysowego (KPZK) sporządza Rządowe Centrum Bezpieczeństwa we współpracy z ministrami, centralnymi urzędami i wojewodami²¹⁸. Jest on co najmniej co 2 lata aktualizowany i zatwierdzany przez Radę Ministrów. KPZK stanowi swoistą matrycę dla niższych planów – wyznacza jednolite standardy i scenariusze, które wojewodowie, starostowie i wójtowie muszą uwzględnić w swoich planach. Plany zarządzania kryzysowego zawierają m.in. ocenę ryzyka wystąpienia zagrożeń na danym terenie, zadania i procedury reagowania dla poszczególnych podmiotów, zasady alarmowania i wymiany informacji, tryb uruchamiania sił i środków zewnętrznych, a także plany odtworzeniowe po ustąpieniu zagrożenia. Dzięki hierarchicznemu systemowi planowania cywilnego, działania kryzysowe mogą być lepiej skoordynowane między poziomami administracji (plan krajowy wyznacza wspólne ramy, a plany lokalne konkretyzują je z uwzględnieniem specyfiki terenu). Definicje i zasady wynikające zatem z ustawy – takie jak pojęcie sytuacji kryzysowej, subsydiarność reakcji, rola organów właściwych i zespołów doradczych, obowiązek planowania – tworzą spójny szkielet doktrynalny polskiego systemu zarządzania kryzysowego²¹⁹.

System zarządzania kryzysowego w Polsce ma charakter wieloszczeblowy, ściśle powiązany z podziałem administracyjnym państwa. Obejmuje on cztery zasadnicze poziomy: krajowy (centralny), wojewódzki, powiatowy i gminny, przy czym poziom krajowy sprawuje głównie funkcje strategiczne i koordynacyjne, zaś poziom lokalny – funkcje operacyjne bezpośredniej reakcji. Na każdym z tych szczebli działa organ zarządzania kryzysowego

²¹⁸ Rządowe Centrum Bezpieczeństwa, Krajowy Plan Zarządzania Kryzysowego 2025, część A, lipiec 2025, s. 2.

²¹⁹ B. Wiśniewski, B. Kaczmarczyk (red.), Zarządzanie kryzysowe. Uwarunkowania teoretyczne, prawne i organizacyjne, Legnica, Wydawnictwo PWSZ im. Witelona, 2012, s. 86.

(jednoosobowy decydent), organ opiniotawczo-doradczy (zespół zarządzania kryzysowego) oraz centrum zarządzania kryzysowego zapewniające zaplecze organizacyjne i informacyjne. Struktura ta jest zobrazowana schematycznie na rysunku 9. Warto zaznaczyć, że poza pionem terytorialnym, ustawa wyodrębnia również poziom resortowy – każdy minister kierujący działem administracji rządowej oraz szef centralnego urzędu ma obowiązek powołać własny zespół zarządzania kryzysowego i centrum zarządzania kryzysowego na potrzeby danego resortu. Dzięki temu system łączy perspektywę terytorialną (województwa, powiaty, gminy) z branżową (resorty odpowiadające za poszczególne sektory, np. energetykę, zdrowie, transport). Poniżej omówiono podstawowe elementy instytucjonalne systemu na poszczególnych poziomach.



Rysunek 9. Struktura systemu zarządzania kryzysowego w Polsce od szczybla centralnego do gminnego (schemat hierarchiczny)

Źródło: opracowanie własne.

Na każdym poziomie wyróżniony jest organ zarządzający (czarny prostokąt), organ doradczy (jasnoszary) oraz centrum zarządzania kryzysowego (ciemnoszary). Strzałki wskazują podporządkowanie terytorialne i przepływ decyzji.

Poziom centralny (krajowy). Naczelnym organem odpowiedzialnym za zarządzanie kryzysowe w skali kraju jest Rada Ministrów, kierowana przez Prezesa Rady Ministrów. Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium RP, określa politykę w tym zakresie, wydaje decyzje dotyczące użycia centralnych zasobów oraz – w razie potrzeby – rekomenduje wprowadzenie stanu nadzwyczajnego. W sytuacjach nagłych, gdy nie ma czasu na zwołanie całego rządu, rolę organu kierującego przejmuje minister spraw wewnętrznych i administracji (MSWiA), który może podejmować niezbędne działania, informując następnie Premiera. MSWiA koordynuje też na co dzień funkcjonowanie systemu – nadzoruje wojewodów i Rządowe Centrum Bezpieczeństwa. Przy Radzie Ministrów działa stały Rządowy Zespół Zarządzania Kryzysowego (RZZK) – kolegialny organ opiniotawczo-doradczy. W skład RZZK wchodzi kluczowi ministrowie (m.in. obrony, spraw wewnętrznych, administracji, zdrowia, środowiska), szefowie służb (np. komendant PSP, policji) oraz przedstawiciele innych podmiotów w zależności od potrzeb. Posiedzeniom RZZK przewodniczy Premier lub wyznaczony minister (z reguły MSWiA). Zespół ten monitoruje bieżącą sytuację zagrożeń, identyfikuje strategie i rekomenduje Radzie Ministrów optymalne rozwiązania w sytuacjach kryzysowych. RZZK pełni ważną rolę w zapewnianiu współdziałania między resortami – np. gdy kryzys dotyka kilku sektorów jednocześnie, Zespół wypracowuje skoordynowane działania. Kluczową instytucją na szczeblu centralnym jest Rządowe Centrum Bezpieczeństwa (RCB) – krajowe centrum zarządzania kryzysowego. RCB zostało utworzone na mocy ustawy z 2007 r. jako wyspecjalizowana jednostka podległa bezpośrednio Premierowi. Zapewnia ono obsługę merytoryczno-techniczną Rady Ministrów, Prezesa RM oraz Rządowego Zespołu Zarządzania Kryzysowego we wszystkich sprawach związanych z zarządzaniem kryzysowym. RCB jest czynne 24/7 i utrzymuje stałą łączność ze wszystkimi resortami oraz województwami. Do jego zadań należy m.in.: monitorowanie zagrożeń w kraju i za granicą, prowadzenie krajowego punktu kontaktowego w ramach unijnego mechanizmu ochrony ludności,

gromadzenie i analiza informacji o sytuacjach kryzysowych, zapewnienie sprawnego obiegu informacji między organami administracji (od poziomu centralnego po gminny), a także inicjowanie uruchamiania procedur reagowania (np. uruchomienie rezerw strategicznych, alarmowanie społeczeństwa poprzez SMS-owy Alert RCB). RCB opracowuje również projekty strategicznych dokumentów (np. Krajowego Planu Zarządzania Kryzysowego, Raportu o zagrożeniach bezpieczeństwa narodowego) i koordynuje ochronę infrastruktury krytycznej na poziomie krajowym (utrzymuje bazę obiektów IK, współpracuje z ich operatorami). Można zatem powiedzieć, że RCB integruje informacje i wspomaga decydentów w szybkim reagowaniu na wszelkie nadzwyczajne zdarzenia. Pod względem organizacyjnym RCB dzieli się na wydziały tematyczne (monitorowania zagrożeń, planowania cywilnego, infrastruktury krytycznej, analiz itd.), co wynika z rozporządzenia z 2008 r. W strukturze centralnej istotną rolę odgrywają także ministerstwa i urzędy centralne – każde z nich posiada własne komórki odpowiedzialne za zarządzanie kryzysowe w zakresie swojej właściwości. Zgodnie z ustawą, ministrowie i szefowie urzędów centralnych powołują zespoły zarządzania kryzysowego (resortowe) oraz centra zarządzania kryzysowego działające przy resortach. Przykładowo Minister Zdrowia ma centrum monitorujące zdarzenia zagrażające zdrowiu publicznemu, Minister Infrastruktury – centrum ds. sytuacji w transporcie itd. Te resortowe struktury współpracują z RCB oraz z odpowiednimi wydziałami wojewódzkimi. Poziom centralny koncentruje się więc na strategicznym planowaniu, alokacji zasobów (np. uruchomieniu centralnej rezerwy przeciwpowodziowej), współpracy międzynarodowej (np. w ramach NATO czy UE) oraz wspieraniu działań wojewodów, gdy skala kryzysu tego wymaga²²⁰.

Poziom wojewódzki. Organem zarządzania kryzysowego na terenie każdego z 16 województw jest wojewoda – przedstawiciel Rady Ministrów w terenie. Wojewoda odpowiada za koordynację działań kryzysowych na obszarze całego województwa, zwłaszcza gdy kryzys przekracza granice jednego powiatu lub wymaga wsparcia służb spoza powiatu dotkniętego zdarzeniem. Wojewoda realizuje swoje zadania przy pomocy Wojewódzkiego

²²⁰ M. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021. <https://doi.org/10.3390/en14248286>

Zespołu Zarządzania Kryzysowego (WZZK) oraz Wojewódzkiego Centrum Zarządzania Kryzysowego (WCZK), które zazwyczaj jest ulokowane w strukturze urzędu wojewódzkiego (np. jako całodobowe centrum w Wydziale Bezpieczeństwa i Zarządzania Kryzysowego). WZZK jest organem doradczym wojewody – w jego skład wchodzi m.in.: komendanci wojewódzcy Państwowej Straży Pożarnej, Policji, przedstawiciele wojska (dowódcy garnizonów), wojewódzcy inspektorzy (sanitarni, weterynaryjni, ochrony środowiska), dyrektorzy wydziałów urzędu wojewódzkiego i inni specjaliści. Wojewoda, zwołując zespół, może również zapraszać ekspertów zewnętrznych lub reprezentantów przedsiębiorstw (np. spółek energetycznych w razie blackoutu). Wojewódzki Zespół analizuje rozwój sytuacji, ocenia potrzeby np. wsparcia poszkodowanych powiatów, proponuje działania (np. uruchomienie odwodów PSP z innych powiatów, wnioskuje do premiera o pomoc wojska, uruchomienie rezerw państwowych) i wymienia informacje między powiatami. Wojewódzkie Centrum Zarządzania Kryzysowego pełni funkcję operacyjno-informacyjną: przyjmuje zgłoszenia o poważnych zdarzeniach, utrzymuje łączność z powiatowymi centrami, przekazuje informacje do RCB, sporządza raporty dobowe o stanie bezpieczeństwa w województwie²²¹. WCZK dysponuje stanowiskami pracy wyposażonymi w środki łączności (telefony alarmowe, łącza radiowe, systemy teleinformatyczne). W razie kryzysu wojewoda może uruchomić w ramach WCZK tryb pracy ciągłej z udziałem przedstawicieli wszystkich kluczowych służb (dyżury multidyscyplinarne). Należy dodać, że wojewoda ma szczególne uprawnienia w sytuacjach klęsk żywiołowych – może wydawać polecenia obowiązujące organy administracji samorządowej (starostów, wójtów) oraz kierowników służb i inspekcji na terenie województwa, a polecenia te z mocy prawa podlegają natychmiastowemu wykonaniu i mogą być egzekwowane nawet wbrew kompetencjom organów samorządu²²². To tzw. zasada jednolitego kierownictwa w sytuacji kryzysu – wojewoda przejmuje wówczas wiodącą rolę wykonawczą²²³. Na co dzień jednak wojewoda głównie nadzoruje

²²¹ W. Otwinowski, *Podstawy zarządzania kryzysowego i systemu obronnego*, Poznań, Wydawnictwo Naukowe Wyższej Szkoły Handlu i Usług, 2015.

²²² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 25, ust. 1).

²²³ B. Wiśniewski, B. Kaczmarczyk (red.), *Zarządzanie kryzysowe. Uwarunkowania teoretyczne, prawne i organizacyjne*, Legnica, Wydawnictwo PWSZ im. Witelona, 2012, s. 88.

przygotowania do zarządzania kryzysowego w regionie (m.in. zatwierdza Wojewódzki Plan Zarządzania Kryzysowego, prowadzi treningi i ćwiczenia, kontroluje gotowość powiatów) oraz wspiera reagowanie kryzysowe w powiatach, jeśli te zgłaszają zapotrzebowanie na pomoc spoza własnych zasobów.

Poziom powiatowy. Na obszarze powiatu (ziemskiego lub grodzkiego) za działania kryzysowe odpowiada starosta (w powiecie ziemskim) lub prezydent miasta na prawach powiatu (w tzw. powiecie grodzkim – mieście wydzielonym). Starosta przewodniczy Powiatowemu Zespołowi Zarządzania Kryzysowego (PZZK) i korzysta ze wsparcia Powiatowego Centrum Zarządzania Kryzysowego (PCZK). Powiatowy Zespół obejmuje m.in.: komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej, komendanta powiatowego Policji, przedstawicieli powiatowego inspektoratu sanitarnego, powiatowego lekarza weterynarii, zarządców dróg, a także wójtów lub burmistrzów z terenu powiatu (jeśli zdarzenie dotyczy ich gmin). Zadaniem PZZK jest ocena sytuacji na poziomie powiatu, uzgadnianie pomocy między gminami (np. przekierowanie sił OSP z jednej gminy do sąsiedniej), a także opiniowanie decyzji starosty dotyczących np. ogłaszania alarmu powodziowego czy zarządzenia ewakuacji na większą skalę. Starosta nie posiada tak szerokich uprawnień nadzwyczajnych jak wojewoda, ale może wydawać polecenia służbom powiatowym i koordynować ich działania. Powiatowe Centrum Zarządzania Kryzysowego zwykle zorganizowane jest przy komendzie powiatowej PSP lub w strukturze starostwa (w zależności od lokalnych ustaleń). PCZK zapewnia przepływ informacji między gminami a województwem – zbiera raporty z gminnych centrów, przekazuje je do WCZK, alarmuje służby na szczeblu powiatowym. W trakcie zdarzenia kryzysowego PCZK sporządza okresowe meldunki o rozwoju sytuacji, potrzebach i działaniach podejmowanych przez poszczególne służby. Powiat jest szczeblem pośrednim – odgrywa rolę koordynatora działań kilku gmin, ale także łącznika przekazującego wsparcie od wojewody w dół. Przykładowo, gdy powódź dotyka wielu gmin w powiecie, starosta może uruchomić odwoły PSP z komendy powiatowej, zorganizować wspólny magazyn pomocy (np. worków z piaskiem) oraz poprosić wojewodę o dodatkowe siły (wojska obrony terytorialnej, posiłki PSP z innych powiatów). Zgodnie z ustawą, to starosta jako pierwszy reaguje, jeśli otrzyma informację o zagrożeniu

– powinien niezwłocznie podjąć działanie, a jednocześnie zawiadomić wojewodę i okoliczne gminy, przedstawiając ocenę sytuacji i już podjęte środki. Ta reguła („kto pierwszy wie – działa i informuje”) ma zapobiec opóźnieniom w reagowaniu poprzez zbędne oczekiwanie na dyspozycje z góry.

Na najniższym szczeblu administracji publicznej – w gminie – za zarządzanie kryzysowe odpowiada jednoosobowo wójt (burmistrz, prezydent miasta). Gmina jest pierwszą linią reakcji na większość zagrożeń, gdyż to tu następuje bezpośrednie zetknięcie z obywatelami dotkniętymi np. pożarem, podtopieniem czy innym miejscowym zagrożeniem. Wójt lub burmistrz przewodniczy Gminnemu Zespołowi Zarządzania Kryzysowego (GZZK), w skład którego zazwyczaj wchodzi: sekretarz gminy, kierownicy gminnych jednostek organizacyjnych (ośrodka pomocy społecznej, zakładu komunalnego, itp.), przedstawiciele lokalnych służb (np. komendant gminny OSP, dzielnicowy policji), czasem dyrektorzy szkół (istotne przy planowaniu np. wykorzystania szkół jako miejsc schronienia) oraz inne osoby przydatne w zależności od charakteru zagrożeń na terenie gminy. Zadaniem GZZK jest przede wszystkim opracowanie Gminnego Planu Zarządzania Kryzysowego i jego aktualizacja, a także doradzanie wójtowi w trakcie realnych zdarzeń. Na poziomie gminy tworzenie stałego Gminnego Centrum Zarządzania Kryzysowego (GCZK) nie jest obowiązkowe – ustawa daje tu pewną elastyczność, wskazując, że mogą być tworzone centra gminne według potrzeb. W praktyce wiele większych gmin (zwłaszcza miejskich) powołuje własne centra kryzysowe lub przynajmniej całodobowe stanowiska dyżurne (często w ramach lokalnej straży miejskiej lub OSP), natomiast w mniejszych gminach rolę tę pełnią osoby na dyżurach telefonicznych. Gmina dysponuje na co dzień jednostkami Ochotniczej Straży Pożarnej, ewentualnie strażą gminną, lokalnymi zasobami sprzętu (np. pompy, pługi śnieżne) oraz siecią instytucji mogących wesprzeć mieszkańców (szkoły, które mogą posłużyć za miejsca schronienia, gminne magazyny przeciwpowodziowe itp.). W razie wystąpienia zagrożenia wójt uruchamia te lokalne siły – alarmuje OSP, powiadamia mieszkańców (np. poprzez system SMS, syreny), organizuje ewakuację lub wydawanie wody pitnej itp. Jeśli sytuacja przekracza możliwości gminy, wójt zwraca się o pomoc do starosty (powiatowego centrum kryzysowego). Mimo ograniczonych zasobów, poziom gminny jest niezwykle ważny ze względu na bliskość problemu – to gmina zna najlepiej lokalne

uwarunkowania terenu i potrzeby mieszkańców, stąd dobrze opracowany gminny plan i sprawnie działający zespół kryzysowy mogą znacznie zredukować straty już na wstępnym etapie reagowania²²⁴. Gmina jest również odpowiedzialna za informowanie ludności o zagrożeniach (np. komunikaty o jakości wody, ostrzeżenia powodziowe) i prowadzenie edukacji społecznej w zakresie zachowania na wypadek klęsk.

Instytucjonalna struktura zarządzania kryzysowego ma charakter wieloszczeblowy: od władz centralnych wyznaczających ramy działania i zapewniających wsparcie, poprzez wojewodów koordynujących działania w regionach oraz starostów integrujących działania gmin, aż po wójtów realizujących zadania z zakresu reagowania kryzysowego na poziomie lokalnym. Każdy szczebel ma określoną samodzielność decyzyjną, ale też obowiązek współdziałania z pozostałymi. Dzięki temu możliwe jest zarówno szybkie podjęcie akcji ratunkowej lokalnie, jak i skierowanie większych sił z zewnątrz, gdy skala kryzysu tego wymaga. Tę konstrukcję wspierają organy doradcze (zespoły) i centra operacyjne na każdym poziomie, co czyni system elastycznym i zdolnym do funkcjonowania całą dobę. Ekspertci zauważają jednak, że w praktyce polski system bywa krytykowany za re-sortowość, upolitycznienie i czasami nieskuteczną koordynację. Niemniej formalnie przyjęty model – oparty na zasadach terytorialności, jednoosobowego kierownictwa i subsydiarności – tworzy spójny mechanizm instytucjonalny, który z perspektywy kilkunastu lat od uchwalenia ustawy zasadniczo się sprawdził, m.in. podczas powodzi (2010 r.), katastrof budowlanych czy sytuacji związanych z pandemią.

Skuteczność zarządzania kryzysowego zależy nie tylko od przepisów i struktur, ale również od dostępności odpowiednich środków finansowych i materialnych. Ustawa o zarządzaniu kryzysowym wskazuje ogólne zasady finansowania zadań – są one realizowane ze środków budżetu państwa oraz budżetów samorządów, zgodnie z podziałem zadań (krajowe – z budżetu centralnego, lokalne – z budżetów gmin/powiatów, a zadania wspólne – odpowiednio współfinansowane). Na szczeblu centralnym, co roku w ustawie budżetowej wyodrębnia się rezerwy celowe na zapobieganie i usuwanie

²²⁴ M. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021. <https://doi.org/10.3390/en14248286>

skutków klęsk żywiołowych. Przykładowo, w budżecie państwa na rok 2025 rezerwa celowa na przeciwdziałanie i usuwanie skutków klęsk żywiołowych została ustalona na kwotę około 3,19 mld zł²²⁵. Środki z tej rezerwy mogą być uruchamiane przez Prezesa Rady Ministrów (na wniosek właściwego ministra lub wojewody) w razie wystąpienia poważnych zdarzeń, takich jak powódź, wichura czy osuwiska, celem sfinansowania doraźnej pomocy poszkodowanym oraz odbudowy zniszczonej infrastruktury. Dodatkowo w budżecie państwa funkcjonuje ogólna rezerwa na zarządzanie kryzysowe (często przeznaczona np. na współfinansowanie ćwiczeń, zakup sprzętu ratowniczego, rozwój systemów wczesnego ostrzegania). Na poziomie województw i powiatów również tworzone są rezerwy kryzysowe w budżetach samorządowych – zwykle mniejsze, ale pozwalające na podjęcie pierwszych działań ratowniczych (zakup paliwa dla strażaków, materiałów przeciwpowodziowych itp.). Poza mechanizmami krajowymi, Polska korzysta również z międzynarodowych instrumentów wsparcia. W ramach Unii Europejskiej istnieje Fundusz Solidarności UE udzielający pomocy finansowej państwom dotkniętym katastrofami naturalnymi o dużej skali – Polska kilkakrotnie aplikowała o takie środki (np. po powodzi w 2010 r.). Ponadto działa Unijny Mechanizm Ochrony Ludności, w którym Polska partycypuje – umożliwia on uzyskanie szybkiej pomocy międzynarodowej (sprzętu, zespołów ratowniczych) w razie katastrofy, a także zobowiązuje Polskę do utrzymywania pewnych zdolności (np. modułów ratowniczych) gotowych do wsparcia innych państw. Choć mechanizmy te mają bardziej charakter logistyczny niż finansowy, stanowią istotne uzupełnienie krajowego systemu w sytuacjach najpoważniejszych kryzysów. W kontekście finansowania należy wspomnieć, że zarządzanie kryzysowe to nie tylko reagowanie, ale i wydatki na zapobieganie i przygotowanie. Samorządy lokalne mogą sięgać po fundusze na inwestycje redukujące ryzyko (np. wały przeciwpowodziowe, systemy alarmowe, szkolenia ludności), często we współpracy z administracją rządową. Przykładowo, od kilku lat funkcjonuje program dofinansowania budowy i modernizacji systemów ostrzegania i alarmowania ludności, finansowany z budżetu państwa przy udziale samorządów. Ponadto służby ratownicze

²²⁵ Polska Agencja Prasowa, Budżet 2025. Jest decyzja rządu, <https://www.money.pl/gospodarka/budzet-2025-jest-decyzja-rzadu-7075937101695840a.html>, [dostęp: 30.09.2025].

(PSP, Policja, ratownictwo medyczne) posiadają własne budżety na utrzymanie gotowości operacyjnej – ich wyposażenie i wyszkolenie jest de facto elementem nakładów na system zarządzania kryzysowego. Finansowanie zarządzania kryzysowego opiera się na budżetowych rezerwach celowych oraz środkach bieżących odpowiednich instytucji. W razie wystąpienia katastrofy, rząd uruchamia specjalne pule środków na pomoc i odbudowę, co w ostatnich latach stanowiło istotną pozycję wydatkową (np. setki milionów złotych rocznie na usuwanie skutków klęsk w infrastrukturze samorządowej). Mechanizmy solidarnościowe (państwo – samorząd, pomoc międzynarodowa) pozwalają rozłożyć ciężar finansowy reagowania na kryzysy. Aspekt finansowy jest rozwijany szerzej w dalszych rozdziałach (zwłaszcza w kontekście logistyki reagowania), tutaj zaś zaznaczono, że ramy prawne systemu obejmują również kwestie ekonomicznego zabezpieczenia działań na wypadek klęsk. Warto pamiętać, że skuteczne zarządzanie kryzysowe wymaga nie tylko sprawnych struktur i planów, ale też adekwatnych zasobów materialnych – stąd ciągłe doskonalenie systemu idzie w parze z inwestycjami w sprzęt ratowniczy, infrastrukturę informatyczną centrów kryzysowych oraz fundusze rezerwowe na nieprzewidziane zdarzenia.

2.5. Kluczowe zasady i funkcje zarządzania kryzysowego

Zarządzanie kryzysowe stanowi istotny element systemu bezpieczeństwa narodowego, obejmujący koordynację działań organów administracji publicznej, służb ratowniczych oraz innych podmiotów w obliczu różnorodnych zagrożeń. Skuteczne funkcjonowanie systemu zarządzania kryzysowego opiera się na przestrzeganiu określonych zasad oraz realizacji działań w ramach uporządkowanych faz postępowania. W niniejszym podrozdziale przedstawiono kluczowe zasady funkcjonowania systemu oraz omówiono podstawowe fazy zarządzania kryzysowego.

System zarządzania kryzysowego w Polsce zorganizowany jest w oparciu o fundamentalne zasady, których przestrzeganie ma zapewnić skuteczność i sprawność działania w sytuacjach zagrożeń. Do najważniejszych zasad należą:

- Zasada prymatu układu terytorialnego – Uznaje podział terytorialny państwa za podstawę organizacji zarządzania kryzysowego. Oznacza to, że kompetencje decyzyjne i odpowiedzialność spoczywają głównie na organach administracji ogólnej właściwych dla danego terenu (wójt/burmistrz, starosta, wojewoda, premier), a układ branżowy (resortowy) pełni funkcję pomocniczą. Innymi słowy, w sytuacji kryzysowej istotniejsze jest działanie władz lokalnych i regionalnych zgodnie z podziałem terytorialnym niż resortowa podległość służb.
- Zasada jednoosobowego kierownictwa – Gwarantuje jasność dowodzenia i szybkość reakcji poprzez powierzenie uprawnień decyzyjnych jednoosobowym organom władzy na danym szczeblu. Decyzje w kryzysie podejmuje zatem jedna osoba (np. wójt, starosta czy wojewoda), która ponosi za nie pełną odpowiedzialność. Zasada ta odpowiada znanej w teorii zarządzania zasadzie „jednoosobowego dowodzenia” (unity of command) i zapobiega chaosowi decyzyjnemu.
- Zasada odpowiedzialności organów władzy publicznej – Określa, że organy administracji rządowej i samorządowej ponoszą ustawową odpowiedzialność za zarządzanie w sytuacjach kryzysowych na podległym im obszarze. Każdy szczebel władzy ma obowiązek usuwania zagrożeń i zapewnienia bezpieczeństwa w swoim zakresie działania²²⁶. Oznacza to m.in., że w razie kryzysu to urzędy gminy, powiatu czy województwa muszą podjąć określone działania, a zaniechanie może rodzić konsekwencje prawne i polityczne.
- Zasada subsydiarności (pomocniczości) – W zarządzaniu kryzysowym oznacza, że reakcja na zagrożenia powinna następować na możliwie najniższym szczeblu administracji, który jest w stanie sobie z nimi poradzić. Wyższy szczebel włącza się dopiero, gdy zakres kryzysu przekracza możliwości niższego szczebla. Zasadę tę *expressis verbis* wprowadza Ustawa o zarządzaniu kryzysowym – zgodnie z nią organy wyższego rzędu wspierają działania niższych jednostek, zamiast je zastępować. W praktyce zasada subsydiarności oznacza kluczową rolę

²²⁶ A. Nowak, Rola i zadania Wojewódzkiego Centrum Zarządzania Kryzysowego, Zeszyty Naukowe WSOSP 4, 2019, s. 67-80.

samorządów lokalnych (gmin i powiatów), które są najbliższej mieszkańców i najlepiej znają lokalne potrzeby oraz specyfikę zagrożeń. Dopiero gdy ich zasoby są niewystarczające, do akcji wkraczają władze centralne, zapewniając pomoc i dodatkowe środki.

- Zasada zespolenia administracji i służb – Zakłada podporządkowanie wszelkich służb, inspekcji i straży funkcjonujących na danym terenie wspólnemu kierownictwu administracji ogólnej. W myśl tej zasady organ administracji zespolonej (np. wojewoda) otrzymuje uprawnienia władcze wobec administracji niezespolonej i wszystkich podległych służb na swoim obszarze. Celem jest integracja wysiłków różnych podmiotów – zarówno cywilnych, jak i wojskowych, państwowych i samorządowych – w spójny system reagowania. Zespolenie zapewnia, że w sytuacji kryzysu wszystkie służby (policja, straż pożarna, wojsko, inspekcje itp.) działają pod jednolitym dowództwem i realizują jednolity plan, co zwiększa efektywność reagowania²²⁷.
- Zasada kategoryzacji zagrożeń – Polega na podziale potencjalnych zagrożeń na odpowiednie kategorie (grupy) według ustalonych kryteriów – najczęściej rodzaju zagrożenia (np. naturalne, techniczne, terrorystyczne) oraz skali (zasięgu, intensywności). Każdej kategorii przypisuje się określone procedury prawne, organizacyjne i finansowe adekwatne do charakteru zagrożenia. Innymi słowy, system zarządzania kryzysowego definiuje różne rodzaje sytuacji kryzysowych i dla każdej opracowuje dedykowane rozwiązania – dzięki temu reakcja może być bardziej precyzyjna i proporcjonalna. Przykładowo inne działania przewiduje się dla klęski żywiołowej (np. powódź), a inne dla zamachu terrorystycznego czy awarii przemysłowej, przy czym zawczasu wiadomo, jakie mechanizmy uruchomić w danej kategorii przypadku.
- Zasada powszechności (partycypacji społecznej) – Podkreśla, że zarządzanie kryzysowe jest zadaniem powszechnym, angażującym wszystkie podmioty i członków społeczeństwa w miarę ich możliwości

²²⁷ J. Gryz, W. Kitler (red.), System reagowania kryzysowego, Toruń, Wydawnictwo Adam Marszałek, 2007.

i kompetencji. Władze publiczne organizują działania kryzysowe we współpracy z wyspecjalizowanymi instytucjami, organizacjami pozarządowymi oraz ogółem obywateli. Społeczeństwo nie jest tu jedynie biernym odbiorcą pomocy – istotna jest jego mobilizacja i udział, np. poprzez wolontariat, samopomoc sąsiedzką, stosowanie się do poleceń służb, a także poprzez udział sektora prywatnego. Powszechność wynika z założenia, że tylko wykorzystanie całego potencjału społecznego – od administracji rządowej po obywateli – pozwala skutecznie zapobiegać i reagować na sytuacje kryzysowe (por. koncepcja „whole community” w zarządzaniu kryzysowym).

- Zasada jawności i komunikacji – Odnosi się do obowiązku transparentności działań organów publicznych oraz efektywnej komunikacji w sytuacjach kryzysowych. Jawność oznacza zapewnienie obywatelom względnie swobodnego dostępu do informacji pozostających w dyspozycji władz publicznych. W kontekście kryzysowym przejawia się to m.in. w rzetelnym informowaniu społeczeństwa o występujących zagrożeniach, wydawanych zaleceniach i podejmowanych działaniach. Zasada komunikacji akcentuje zaś konieczność sprawnego przepływu informacji zarówno wewnątrz systemu (między służbami i organami), jak i na zewnątrz – do mediów i obywateli. Warto podkreślić, że faza reagowania na kryzys ma charakter najbardziej medialny i znajduje się w centrum uwagi opinii publicznej, dlatego odpowiednie informowanie społeczeństwa o rozwoju sytuacji jest niezmiernie ważne. Przestrzeganie zasady jawności i skuteczna komunikacja kryzysowa budują zaufanie obywateli do instytucji oraz ułatwiają realizację działań (mieszkańcy świadomi zagrożenia chętniej podporządkują się decyzjom o ewakuacji czy innym poleceniom). Zapis prawa do informacji publicznej²²⁸ oraz ustawa o dostępie do informacji publicznej stanowią prawne ramy realizacji tej zasady w administracji, także w obszarze zarządzania kryzysowego.

²²⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483, art. 61).

Powyższe zasady tworzą fundament organizacyjny, na którym opiera się cały system zarządzania kryzysowego w Polsce. Ich przestrzeganie ma gwarantować, że w obliczu kryzysu działania będą skoordynowane, szybkie i adekwatne do sytuacji, z jasno określoną odpowiedzialnością za podejmowane decyzje.

Zarządzanie kryzysowe jak zostało już wspomniane jest procesem cyklicznym, obejmującym szereg następujących po sobie faz działań, od przygotowań podejmowanych przed wystąpieniem sytuacji kryzysowej, poprzez działania w trakcie kryzysu, aż po aktywności podejmowane po jego ustąpieniu w celu przywrócenia normalności. Ustawa o zarządzaniu kryzysowym już w definicji legalnej wskazuje na takie ramy. W literaturze przedmiotu i praktyce najczęściej wyróżnia się cztery podstawowe fazy zarządzania kryzysowego: zapobieganie, przygotowanie, reagowanie oraz odbudowę (usuwanie skutków).

Zarządzanie kryzysowe opiera się na określonych zasadach organizacyjnych oraz przebiega w ramach cyklicznego procesu fazowego. Taki model zapewnia systematyczność i kompleksowość podejścia do zagrożeń: od działań proaktywnych przed wystąpieniem kryzysu, poprzez efektywną reakcję w jego trakcie, aż po działania naprawcze i wyciąganie wniosków po zdarzeniu. W kolejnych rozdziałach pracy poszczególne fazy cyklu zarządzania kryzysowego zostaną omówione bardziej szczegółowo, z uwzględnieniem konkretnych narzędzi, procedur i przykładów praktycznych realizacji zadań w Polsce i na świecie. Powyższe ogólne ramy stanowią fundament dla tych pogłębionych analiz – ukazują one, w jaki sposób i na jakich zasadach zbudowany jest system, który ma chronić społeczeństwo przed skutkami różnorodnych kryzysów oraz minimalizować ich negatywne skutki dla bezpieczeństwa.

Rozdział III.

Fazy i procesy zarządzania kryzysowego

3.1. Identyfikacja i ocena zagrożeń

Pierwszym etapem cyklu zarządzania kryzysowego jest identyfikacja zagrożeń i ocena ryzyka – kluczowy proces umożliwiający podjęcie działań zapobiegawczych i przygotowawczych zanim wystąpi sytuacja kryzysowa. Identyfikacja zagrożeń polega na rozpoznaniu wszystkich potencjalnych zdarzeń i zjawisk mogących negatywnie wpłynąć na bezpieczeństwo ludzi, mienia lub środowiska w danym obszarze²²⁹. Ważne jest uwzględnienie zarówno zagrożeń już historycznie odnotowanych, jak i *emerging threats*, które jeszcze się nie wydarzyły, ale są przewidywalne na podstawie obserwowanych trendów (np. zmiany klimatyczne, rozwój technologiczny)²³⁰. Ocena ryzyka natomiast to analiza prawdopodobieństwa wystąpienia danego zdarzenia oraz potencjalnej skali jego skutków, prowadząca do określenia poziomu ryzyka i hierarchizacji. Innymi słowy, ryzyko często definiuje się jako kombinację (iloczyn) prawdopodobieństwa wystąpienia zdarzenia i skutków tego zdarzenia^{231,232}. Taki właśnie probabilistyczno-konsekwencyjny opis ryzyka

²²⁹ U. Kąkol, M. Marczewski, *Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym*, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

²³⁰ Rządowe Centrum Bezpieczeństwa (RCB), *Ocena ryzyka na potrzeby zarządzania kryzysowego*, Warszawa, 2013.

²³¹ U. Kąkol, M. Marczewski, *Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym*, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

²³² Rządowe Centrum Bezpieczeństwa (RCB), *Ocena ryzyka na potrzeby zarządzania kryzysowego*, Warszawa, RCB, 2013.

przyjęty jest m.in. w europejskich standardach zarządzania ryzykiem²³³. Rezultatem oceny jest zwykle przypisanie zagrożeniom określonych poziomów ryzyka (np. niskie, średnie, wysokie), co stanowi podstawę do ustalenia priorytetów w planowaniu kryzysowym. Przykładowe kategorie zagrożeń i ich atrybuty (częstość, skala, zasięg) w Polsce zostały przedstawione w tabeli 3.

Tabela 3. Przykładowe kategorie zagrożeń i ich atrybuty (częstość, skala, zasięg) w Polsce

Kategoria zagrożeń	Częstość występowania	Skala skutków	Typowy zasięg
Zagrożenia naturalne (klęski żywiołowe) – np. powodzie, silne wiatry, susze, ekstremalne temperatury, osuwiska, epidemie chorób zakaźnych zwierząt lub ludzi.	Relatywnie wysoka – klęski żywiołowe (zwłaszcza powodzie) występują niemal co roku, częste są też silne burze i wichury sezonowe. Najrzadsze spośród naturalnych są zjawiska typu trzęsienia ziemi.	Zróznicowana – od lokalnych strat materialnych po katastrofalne skutki w skali regionu lub kraju. Np. powodzie mogą powodować wielomiliardowe straty i ofiary śmiertelne.	Przeważnie regionalny – klęski żywiołowe obejmują części kraju (np. dorzecza rzek przy powodzi). Ekstremalne zjawiska mogą jednak dotknąć rozległe obszary (np. upały w całym kraju).
Zagrożenia techniczne (awarie infrastruktury, katastrofy przemysłowe) – np. awarie instalacji chemicznych, pożary przemysłowe, wybuchy, skażenia środowiska, przerwy w dostawie prądu.	Umiarkowana – drobne awarie techniczne zdarzają się często, lecz poważne katastrofy o dużej skali są rzadsze. W skali kraju istotne awarie infrastruktury (np. energetycznej) występują sporadycznie (kilka na dekadę).	Średnia / wysoka – awarie mogą powodować poważne straty lokalnie, najpoważniejsze katastrofy techniczne (np. eksplozja w zakładzie przemysłowym) skutkują ofiarami i długotrwałymi skutkami środowiskowymi.	Na ogół lokalny – konsekwencje ograniczają się do obszaru zakładu lub gminy. W przypadku awarii o charakterze sieciowym (np. blackout) zasięg może objąć kilka województw.

²³³ Federation of European Risk Management Associations (FERMA), A Risk Management Standard, Bruksela, FERMA/AIRMIC/ALARM, 2002.

Kategoria zagrożeń	Częstość występowania	Skala skutków	Typowy zasięg
Zagrożenia społeczne i terrorystyczne – np. zamieszki i niepokoje społeczne, akty terroryzmu, cyberzagrożenia, sytuacje masowej migracji czy konflikty zbrojne w regionie.	Niska – poważne zamachy terrorystyczne czy rozległe zamieszki społeczne są w Polsce bardzo rzadkie. Incydenty cyberataków zdarzają się częściej, lecz rzadko powodują sytuacje kryzysowe na dużą skalę.	Wysoka – jednostkowy akt terroru może spowodować wiele ofiar i silny efekt psychologiczny. Masowe protesty lub zamieszki mogą sparaliżować funkcjonowanie dużych miast. Potencjalne skutki konfliktu zbrojnego lub skoordynowanego cyberataku mogłyby być katastrofalne.	Może być lokalny (np. zamieszki w jednym mieście, atak terrorystyczny w konkretnym miejscu) lub ogólnokrajowy (np. poważne zagrożenie cyberbezpieczeństwa infrastruktury krytycznej, kryzys uchodźczy na granicach państwa).

Źródło: opracowanie własne.

Tabela ilustruje przykładową typologię zagrożeń wraz z oceną ich częstości, skali i zasięgu oddziaływania. W polskich warunkach najbardziej regularnie występują zagrożenia naturalne, zwłaszcza ekstremalne zjawiska pogodowe. Na przykład powodzie pojawiają się niemal co roku w różnych regionach kraju – w ciągu ostatnich dekad wielokrotnie ogłaszano alarmy powodziowe, a dwukrotnie (1997 r., 2010 r.) wprowadzono nawet stan klęski żywiołowej z powodu powodzi na dużą skalę. Powodzie należą jednocześnie do zdarzeń powodujących największe straty ekonomiczne i społecznie w Polsce²³⁴. Według analiz Rządowego Centrum Bezpieczeństwa, wśród zagrożeń naturalnych to właśnie powodzie stanowią największe ryzyko (pod względem skutków finansowych i zagrożenia życia ludzi), kolejne w hierarchii są silne wiatry i nawałnice (w tym sporadyczne trąby powietrzne), a następnie ekstremalne mrozy. Przykładowo, na podstawie danych historycznych wytypowano nawet swoisty „szlak trąb powietrznych” – obszar od Opolszczyzny po Suwalszczyznę, gdzie ryzyko wystąpienia trąby jest największe. Dane statystyczne i historyczne stanowią zatem ważną podstawę identyfikacji zagrożeń naturalnych. Z drugiej strony, zagrożenia wywołane działalnością człowieka (techniczne, komunikacyjne, terrorystyczne) występują rzadziej,

²³⁴ Rządowe Centrum Bezpieczeństwa (RCB), Zagrożenia okresowe występujące w Polsce – aktualizacja, Warszawa, RCB, 2013.

ale mogą mieć poważne konsekwencje, zwłaszcza gdy dotyczą infrastruktury krytycznej lub bezpieczeństwa zbiorowego.

Metody identyfikacji zagrożeń. Skuteczna identyfikacja zagrożeń wymaga zastosowania rozmaitych metod i narzędzi analitycznych, tak, aby niczego nie pominąć. Podstawowym podejściem jest analiza danych historycznych i statystycznych, pozwalająca wyciągać wnioski z przeszłych zdarzeń. Przegląd kronik zdarzeń nadzwyczajnych, raportów służb ratowniczych czy baz danych o katastrofach umożliwia wskazanie, jakie zagrożenia najczęściej dotykały dany obszar oraz z jaką siłą. W Polsce przykładem takiej bazy wiedzy są biuletyny RCB opisujące zagrożenia okresowe – na podstawie wieloletnich obserwacji określono m.in. typowe sezony występowania poszczególnych klęsk żywiołowych czy regiony szczególnie narażone na ich wystąpienie. Identyfikując zagrożenia, analiza historyczna powinna być uzupełniona oceną bieżących trendów i czynników zmian. Jak wskazują wytyczne krajowe, należy brać pod uwagę procesy i trendy społeczne, środowiskowe i technologiczne, które mogą generować nowe zagrożenia – np. starzenie się społeczeństwa (wpływ na zagrożenia epidemiologiczne), zmiany klimatyczne (częstsze zjawiska ekstremalne), rozwój cyfrowy (nowe zagrożenia cyber) itp. Dzięki temu identyfikacji podlegają nie tylko zagrożenia znane z historii, ale i te potencjalne, które jeszcze nie miały miejsca, lecz są przewidywalne w świetle aktualnych zmian otoczenia.

Kolejnym istotnym narzędziem jest analiza scenariuszowa. Metoda scenariuszy polega na tworzeniu hipotetycznych, lecz realistycznych opisów przebiegu zdarzeń kryzysowych, aby zbadać ich możliwe przyczyny i skutki²³⁵. W praktyce oznacza to projektowanie wariantów rozwoju sytuacji dla każdego zidentyfikowanego zagrożenia – od najbardziej prawdopodobnych po skrajnie niebezpieczne scenariusze worst case. Scenariusze tworzy się zwykle we współpracy ekspertów z różnych dziedzin, co umożliwia wieloaspektowe spojrzenie na zagrożenie²³⁶. Rządowe Centrum Bezpieczeństwa zaleca opracowanie dla każdego rodzaju zagrożenia 2-3 scenariuszy zawierających m.in. potencjalne miejsce wystąpienia zdarzenia, możliwe przyczyny

²³⁵ E. Borodzicz, *Risk, Crisis and Security Management*, Chichester, John Wiley & Sons, 2005.

²³⁶ Rządowe Centrum Bezpieczeństwa (RCB), *Ocena ryzyka na potrzeby zarządzania kryzysowego*, Warszawa, RCB, 2013.

(w tym celowe działanie lub awaria) oraz szczegółowy opis przebiegu zdarzeń. Dla każdego scenariusza analizuje się następnie konsekwencje w podziale na kategorie: wpływ na ludzi, na gospodarkę i infrastrukturę oraz na środowisko. Takie podejście pozwala wyobrazić sobie zarówno bezpośrednie skutki (natychmiastowe straty), jak i efekty odroczone (np. długofalowe skutki środowiskowe czy ekonomiczne). Analiza scenariuszowa wspomaga identyfikację zagrożeń, gdyż ujawnia słabe punkty systemu – np. pokazuje, które elementy infrastruktury są wspólne dla wielu scenariuszy (tzw. wąskie gardła bezpieczeństwa) lub jakie nietypowe następstwa może nieść dane zjawisko. W polskim systemie zarządzania kryzysowego scenariusze zagrożeń są podstawą dalszej oceny ryzyka i planowania – na etapie krajowym każdy resort czy województwo przygotowuje własne scenariusze w ramach Raportu o zagrożeniach bezpieczeństwa narodowego²³⁷. Co ważne, proces ten angażuje nie tylko administrację, ale także ekspertów zewnętrznych i podmioty prywatne, np. przy opracowaniu scenariuszy zdarzeń z udziałem infrastruktury krytycznej uczestniczą jej operatorzy oraz służby.

Kolejnym pożytecznym narzędziem są mapy ryzyka. Termin ten, zdefiniowany w ustawie o zarządzaniu kryzysowym, oznacza mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożeń na ludzi, środowisko, mienie i infrastrukturę. Mapa ryzyka może przybrać formę graficzną – na przykład kartograficzne przedstawienie obszarów zagrożonych danym niebezpieczeństwem – lub opisową tabelę zagrożeń wraz z charakterystyką. W Polsce mapy ryzyka sporządzane są m.in. dla zagrożeń powodziowych (zgodnie z wymogami unijnymi opracowano mapy zagrożenia i ryzyka powodziowego pokrywające cały kraj) oraz w ramach wojewódzkich planów zarządzania kryzysowego (gdzie stanowią one załącznik charakteryzujący zagrożenia na danym terenie). Ideą map ryzyka jest syntetyczne ukazanie, gdzie i jakie zagrożenia mogą wystąpić, oraz jak poważne mogą być ich skutki. Narzędzie to ułatwia władzom i służbom skupienie się na obszarach i zagrożeniach o najwyższym poziomie ryzyka. Przykładowo, mapa ryzyka powodziowego wyraźnie pokazuje tereny zalewowe o różnym prawdopodobieństwie zalania, co przekłada się na działania prewencyjne

²³⁷ Rządowe Centrum Bezpieczeństwa (RCB), Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa, RCB, 2013.

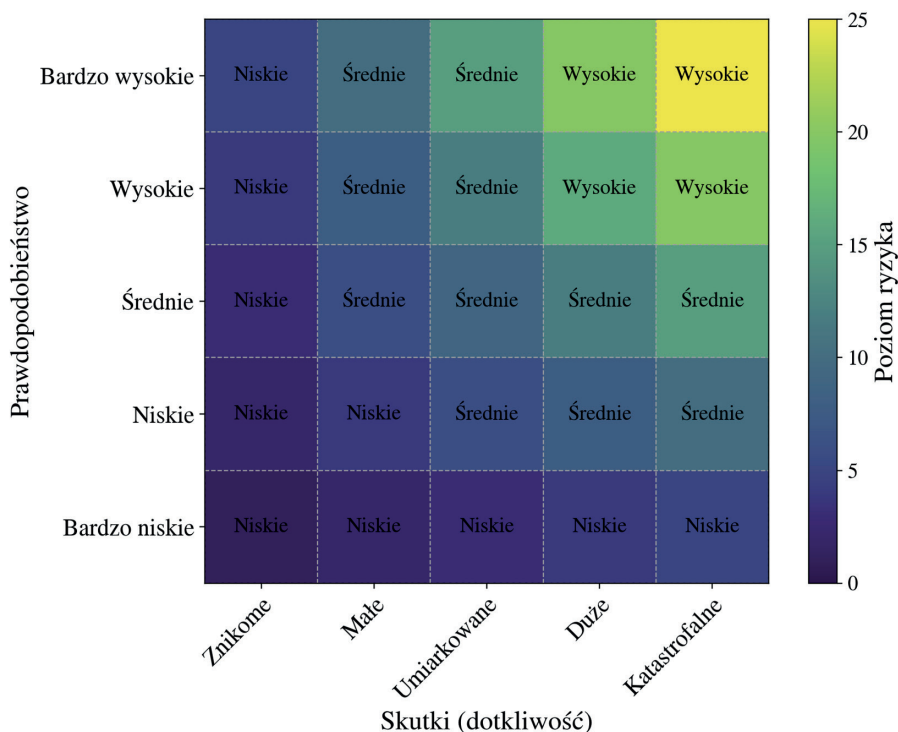
(planowanie przestrzenne, budowa wałów, systemy ostrzegania). Z kolei mapa ryzyka tworzona na poziomie kraju uwzględnia również zagrożenia o charakterze ponadregionalnym – np. skutki konfliktów międzynarodowych czy terroryzmu – choć te trudno zwizualizować geograficznie, więc częściej przybierają one formę opisową²³⁸. Niezależnie od formy, stworzenie mapy ryzyka jest podstawowym rezultatem etapu identyfikacji zagrożeń, wymaganym prawnie jako element planu zarządzania kryzysowego (Ustawa 2007).

Dopełnieniem powyższych metod jest wykorzystanie specjalistycznych baz danych o zdarzeniach niebezpiecznych oraz systemów wczesnego ostrzegania. W skali globalnej istnieją bazy katastrof naturalnych (np. EM-DAT prowadzona przez CRED), zawierające historyczne zapisy dotkliwości i częstotliwości kataklizmów – stanowią one punkt odniesienia przy ocenie ryzyka katastrof w danym kraju. Na poziomie krajowym cennym źródłem informacji są statystyki służb ratunkowych (Państwowej Straży Pożarnej, Policji, pogotowia itp.), rejestry awarii przemysłowych (np. wymagane w zakładach Seveso) czy dane instytucji monitorujących środowisko (IMGW-PIB dla zjawisk meteorologicznych, GIS dla chorób zakaźnych ludzi i zwierząt). Analiza zbiorów danych z tych systemów pozwala identyfikować zarówno trendy częstotliwości (czy dane zagrożenie nasila się czy słabnie z czasem), jak i czynniki sprzyjające wystąpieniu zdarzeń (np. kumulacja opadów poprzedzająca osuwiska). Przykładowo, analiza danych z systemów monitorowania meteorologicznego umożliwia wykrycie oznak nadchodzącej suszy lub powodzi, co jest formą identyfikacji zagrożenia w czasie rzeczywistym. Sumując, efektywna identyfikacja zagrożeń opiera się na wieloźródłowym rozpoznaniu – łączy wiedzę historyczną, prognozy eksperckie, modelowanie (scenariusze, mapy) oraz bieżący monitoring, aby uzyskać możliwie pełną listę potencjalnych zagrożeń.

Techniki oceny ryzyka. Po zidentyfikowaniu katalogu zagrożeń następuje etap ich analizy i szacowania ryzyka. Celem oceny ryzyka jest ustalenie, które zagrożenia stanowią największe prawdopodobieństwo wystąpienia i jednocześnie mogą wywołać najpoważniejsze skutki – czyli mają najwyższy poziom ryzyka. W praktyce najczęściej stosuje się metody

²³⁸ Rządowe Centrum Bezpieczeństwa (RCB), Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa, RCB, 2013.

jakościowe lub pólnościowe, bazujące na eksperckiej ocenie prawdopodobieństwa i skutków każdego zagrożenia. Każdemu zagrożeniu przypisuje się kategorię prawdopodobieństwa (np. bardzo małe, małe, średnie, duże, bardzo duże prawdopodobieństwo w skali kilku lat) oraz kategorię skutków (np. znikome, umiarkowane, poważne, katastrofalne skutki dla zdrowia, mienia, środowiska). Następnie wartości te krzyżuje się na macierzy ryzyka (zwanej też matrycą ryzyka), aby określić poziom ryzyka^{239,240}. Macierz ryzyka przedstawiona została na rysunku 10.



Rysunek 10. Macierz ryzyka wykorzystywana do jakościowej oceny ryzyka na podstawie prawdopodobieństwa (oś pionowa) oraz dotkliwości skutków (oś pozioma) zdarzenia

Źródło: opracowanie własne.

²³⁹ U. Kąkol, M. Marczewski, Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

²⁴⁰ Rządowe Centrum Bezpieczeństwa (RCB), Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa, RCB, 2013.

Kolorami oznaczono poziomy ryzyka. Macierz umożliwia priorytetyzację zagrożeń – np. zdarzenia o bardzo wysokim prawdopodobieństwie i katastrofalnych skutkach lokują się w górnym prawym rogu (ryzyko najwyższe).

Macierz ryzyka jest użytecznym narzędziem wizualnym, które upraszcza ocenę ryzyka poprzez przedstawienie zależności między prawdopodobieństwem a skutkami zagrożeń. Każde zagrożenie można umieścić w odpowiedniej komórce macierzy – przykładowo: powódź stulecia będzie miała bardzo niski poziom prawdopodobieństwa, ale katastrofalne skutki, co daje jej średni poziom ryzyka. Z kolei coroczne podtopienia wiosenne mają wysokie prawdopodobieństwo, lecz zazwyczaj umiarkowane skutki, co również może dawać ryzyko średnie. Najwyższy priorytet otrzymują zagrożenia znajdujące się w żółtych polach macierzy – łączące częste występowanie z dotkliwymi konsekwencjami. W praktyce, jeśli macierz została zdefiniowana liczbowo (np. przypisano punktacje 1-5 dla kategorii prawdopodobieństwa i skutków), to ryzyko można wyrazić liczbowo jako iloczyn lub sumę tych wartości. Jednak nawet ogólna, jakościowa matryca pozwala na kategoryzację ryzyka: zazwyczaj wyróżnia się poziom niski (akceptowalny), umiarkowany (wymagający monitorowania) oraz wysoki (wymagający pilnych działań redukujących ryzyko). W polskich planach zarządzania kryzysowego często stosuje się właśnie macierze 5x5 definiujące te strefy ryzyka kolorami²⁴¹. Po oszacowaniu ryzyka wszystkich zidentyfikowanych zagrożeń sporządza się ich ranking według poziomu ryzyka, czyli dokonuje priorytetyzacji zagrożeń. Technika ta pozwala skoncentrować zasoby i uwagę na tych niebezpieczeństwach, które są najbardziej prawdopodobne lub mogą wywołać najcięższe straty. Zwykle zagrożenia o najwyższym poziomie ryzyka wskazuje się jako nieakceptowalne bez podjęcia działań zaradczych (należy im przeciwdziałać lub przygotować szczegółowe plany reagowania), podczas gdy zagrożenia o niskim poziomie ryzyka mogą zostać zaakceptowane jako część normalnego ryzyka operacyjnego²⁴². W dokumentach krajowych przyjmuje się na przykład cztery kategorie akceptacji

²⁴¹ U. Kąkol, M. Marczewski, Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

²⁴² P. Wilkinson, Crisis Management in Business, London, Kogan Page, 2010.

ryzyka: A – ryzyko akceptowalne (brak dodatkowych działań, wystarczająco bieżące zabezpieczenia), B – ryzyko tolerowane (monitorowanie, działania prewencyjne standardowe), C – ryzyko nietolerowane (konieczne dodatkowe przygotowania i środki), D – ryzyko niedopuszczalne (wymagane natychmiastowe działania lub zakaz podejmowania aktywności narażającej na to ryzyko). Taki podział umożliwia władzom określenie, które scenariusze wymagają opracowania szczegółowych planów operacyjnych, a które jedynie obserwacji. Priorytetyzacja zagrożeń jest także istotna z punktu widzenia edukacji społecznej i alokacji budżetu – najwyższe ryzyka powinny być komunikowane społeczeństwu (np. poprzez kampanie informacyjne o zachowaniu w razie powodzi), a także uwzględniane przy podziale środków na prewencję (największe inwestycje tam, gdzie potencjalne straty są największe).

W polskim systemie zarządzania kryzysowego do oceny ryzyka stosuje się znormalizowane podejście na wszystkich poziomach administracji. Ustawa o zarządzaniu kryzysowym nakłada obowiązek cyklicznej oceny ryzyka i aktualizacji planów zarządzania kryzysowego nie rzadziej niż co 2 lata²⁴³. W praktyce oznacza to, że co najmniej raz na dwa lata organy administracji publicznej dokonują przeglądu zagrożeń oraz aktualizacji ocen prawdopodobieństwa i skutków, uwzględniając nowe dane i okoliczności²⁴⁴. Na poziomie gminy obowiązek ten spoczywa na wójcie/burmistrzu/prezydencie miasta, który jest podmiotem odpowiedzialnym za ocenę ryzyka lokalnie²⁴⁵. Prace wykonuje zwykle gminny zespół zarządzania kryzysowego oraz komórka organizacyjna urzędu gminy ds. zarządzania kryzysowego, które gromadzą informacje o zagrożeniach i opracowują gminny plan zarządzania kryzysowego²⁴⁶. Analogiczne zadania realizują szczeble powiatu i województwa – każdy starosta i wojewoda odpowiada za okresową ocenę ryzyka

²⁴³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 5a, art. 19).

²⁴⁴ U. Kąkol, M. Marczewski, Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

²⁴⁵ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 19, ust. 2).

²⁴⁶ U. Kąkol, M. Marczewski, Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 11(959), 2016, s. 53-69.

na swoim terenie i aktualizację planów²⁴⁷. Co istotne, proces oceny ryzyka ma charakter partycypacyjny – lokalne zespoły kryzysowe zasięgają opinii służb (PSP, Policji, inspekcji sanitarnej itp.), konsultują plany z sąsiednimi samorządami oraz posiłkują się ekspertyzami, np. z ośrodków naukowych²⁴⁸. Dzięki temu ocena nie jest czysto urzędnicza, lecz uwzględnia praktyczną wiedzę różnych podmiotów.

Na szczeblu centralnym funkcjonuje z kolei mechanizm Krajowej Oceny Ryzyka koordynowany przez Rządowe Centrum Bezpieczeństwa. Zgodnie z art. 5a ustawy, co dwa lata RCB opracowuje Raport o zagrożeniach bezpieczeństwa narodowego, który jest przyjmowany uchwałą Rady Ministrów. Do przygotowania tego raportu angażowane są wszystkie kluczowe instytucje państwowe – ministrowie, kierownicy urzędów centralnych oraz wojewodowie, każdy w zakresie swojej właściwości przygotowuje tzw. raport cząstkowy. Raporty cząstkowe zawierają identyfikację najistotniejszych zagrożeń w danym obszarze (np. transport, energetyka, zdrowie publiczne, środowisko), ocenę ryzyka tych zagrożeń oraz wskazanie działań zapobiegawczych i przygotowawczych. RCB zapewnia metodologiczną spójność tych ocen – opracowało jednolitą procedurę i formularze do identyfikacji i analizy zagrożeń, prowadzi także szkolenia dla urzędników różnych resortów w zakresie oceny ryzyka²⁴⁹. Taka centralna koordynacja służy temu, by kryteria oceny ryzyka były jednolite w skali kraju, co umożliwia porównanie i agregację wyników z różnych sektorów. Na podstawie raportów cząstkowych RCB dokonuje analizy porównawczej (cross-impact analysis) i sporządza zbiorczy Raport o zagrożeniach, który następnie trafia do zatwierdzenia przez Rząd.

Rola administracji i podmiotów lokalnych w ocenie zagrożeń jest zatem wielopoziomowa. Administracja publiczna stanowi głównego wykonawcę procesu oceny ryzyka – od poziomu gminy aż po poziom centralny – i ponosi odpowiedzialność za aktualność oraz jakość tych ocen. Istotne jest przy tym, że każda gmina, powiat i województwo uwzględnia lokalną specyfikę zagrożeń. Na przykład nadmorskie gminy muszą oceniać ryzyko

²⁴⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 17, art. 18).

²⁴⁸ Rządowe Centrum Bezpieczeństwa (RCB), Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa, RCB, 2013.

²⁴⁹ Tamże.

sztormów i powodzi sztormowych, podczas gdy gminy górskie – lawin czy osuwisk. Powiaty o rozwiniętym przemyśle chemicznym analizują ryzyko awarii i skażeń toksycznych, a województwa graniczne – zagrożenia związane z migracjami czy handlem ludźmi. Zadaniem władz lokalnych jest więc wykorzystanie wiedzy o uwarunkowaniach lokalnych przy identyfikacji zagrożeń – często odbywa się to poprzez konsultacje ze społecznością i lokalnym biznesem. Na przykład przedsiębiorstwa posiadające instalacje niebezpieczne (zakłady dużego ryzyka) są prawnie zobowiązane do raportowania zagrożeń władzom i współpracy przy planowaniu na wypadek awarii. Z kolei mieszkańcy mogą sygnalizować władzom pojawienie się nowych zagrożeń (np. osuwiska, dzikie wysypiska chemikaliów) – ta oddolna informacja również zasila proces identyfikacji ryzyka. Administracja odgrywa także kluczową rolę w komunikowaniu i dokumentowaniu ryzyka. Wyniki oceny zagrożeń muszą znaleźć odzwierciedlenie w oficjalnych dokumentach planistycznych – wspomnianych planach zarządzania kryzysowego wszystkich szczebli. Plany te zawierają rozdziały poświęcone charakterystyce zagrożeń i analizie ryzyka²⁵⁰. Na poziomie krajowym odpowiednikiem jest Krajowy Plan Zarządzania Kryzysowego, który również zawiera syntezę oceny ryzyka dla całego państwa. Ponadto administracja ma obowiązek udostępniać pewne informacje o zagrożeniach społeczeństwu – np. na stronach Biuletynu Informacji Publicznej często publikowane są tzw. katalogi zagrożeń dla danego regionu. Dzięki temu zarówno służby, jak i obywatele, mogą dowiedzieć się, jakie niebezpieczeństwa uznano za priorytetowe w ich okolicy.

Identyfikacja i ocena zagrożeń to fundament systemu zarządzania kryzysowego, warunkujący skuteczność kolejnych faz cyklu. Rzetelnie zidentyfikowane zagrożenia i oszacowane ryzyko umożliwiają odpowiednie zaplanowanie działań w fazie przygotowania, właściwą reakcję w sytuacji kryzysowej oraz efektywną odbudowę po zdarzeniu. W kontekście Polski proces ten jest sformalizowany prawnie i organizacyjnie – uczestniczą w nim wszystkie szczeble administracji, wspierane przez wiedzę ekspercką, dane historyczne i modele prognostyczne. Tylko dzięki ciągłemu doskonaleniu metod identyfikacji zagrożeń (np. poprzez nowe technologie monitoringu,

²⁵⁰ Rządowe Centrum Bezpieczeństwa, Krajowy Plan Zarządzania Kryzysowego 2025, część A, lipiec 2025.

analizy big data, scenariusze uwzględniające zmieniający się świat) system zarządzania kryzysowego może proaktywnie przygotować się na przyszłe wyzwania bezpieczeństwa. W kolejnych częściach omówione zostaną następne fazy cyklu – od planowania i przygotowania po reagowanie, odbudowę i wyciąganie wniosków – jednak wszystkie one bazują na ustaleniach fazy identyfikacji i oceny zagrożeń przedstawionej powyżej.

3.2. Planowanie i przygotowanie do sytuacji kryzysowych

Planowanie i odpowiednie przygotowanie są kluczowymi elementami zarządzania kryzysowego, stanowiącymi podstawę skutecznego reagowania na zagrożenia. System zarządzania kryzysowego w Polsce ma charakter wielopoziomowy, obejmujący cztery główne szczeble administracyjne: krajowy, wojewódzki, powiatowy i gminny²⁵¹. Na każdym z tych poziomów opracowywane są plany zarządzania kryzysowego. Art. 5 tej ustawy stanowi, że tworzy się Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego, zwane dalej planami zarządzania kryzysowego²⁵². Każdy z tych planów jest dostosowany do specyfiki danego poziomu administracji, ale wszystkie razem powinny tworzyć spójny system planowania cywilnego na wypadek sytuacji kryzysowych. Co istotne, ustawa przewiduje także tworzenie planów zarządzania kryzysowego przez ministrów i kierowników urzędów centralnych dla ich resortów – Krajowy Plan Zarządzania Kryzysowego pełni funkcję matrycy przy opracowywaniu planów resortowych oraz wojewódzkich. Dzięki temu zapewniana jest zasadnicza jednolitość celów i struktur planów na różnych szczeblach.

Krajowy Plan Zarządzania Kryzysowego (KPZK) jest nadrzędnym dokumentem planistycznym na szczeblu centralnym. Opracowuje go Rządowe Centrum Bezpieczeństwa (RCB) we współpracy z ministerstwami,

²⁵¹ D. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021, s. 1-33. <https://doi.org/10.3390/en14248286>

²⁵² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 17, art. 18).

urzędami centralnymi oraz wojewodami. KPZK dotyczy wszystkich faz zarządzania kryzysowego (zapobiegania, przygotowania, reagowania, odbudowy) i zawiera scenariusze najpoważniejszych zagrożeń o charakterze krajowym wraz z procedurami postępowania na wypadek ich wystąpienia. Plan ten jest zatwierdzany przez Premiera/Radę Ministrów i stanowi dokument wyjściowy dla planowania kryzysowego na niższych szczeblach. Obowiązujące przepisy wymagają, by KPZK był aktualizowany nie rzadziej niż co 2 lata. W praktyce oznacza to regularny cykl planistyczny – przykładowo, w sierpniu 2025 r. wprowadzono kolejną (ósmą) aktualizację krajowego planu. Aktualizacje uwzględniają m.in. pojawienie się nowych rodzajów zagrożeń (np. katastrofy ekologiczne, zagrożenia hybrydowe, pandemie) oraz doświadczenia z ostatnich sytuacji kryzysowych. Krajowy plan określa także zadania poszczególnych resortów i instytucji centralnych w sytuacjach kryzysowych, zapewniając ramy do współdziałania między nimi. Dzięki temu pełni on rolę „matrycy” odpowiedzialności – wytycza, które organy są wiodące przy danych zagrożeniach i jakie działania powinny podjąć.

Na szczeblu regionalnym opracowywany jest Wojewódzki Plan Zarządzania Kryzysowego (WPZK) – przygotowuje go wojewoda przy pomocy Wojewódzkiego Zespołu Zarządzania Kryzysowego. Taki plan obowiązuje na obszarze danego województwa i powinien być zgodny z KPZK oraz z wytycznymi Ministra Spraw Wewnętrznych i Administracji. WPZK zawiera m.in. charakterystykę zagrożeń województwa, analizę ryzyka dla regionu, określenie sił i środków dostępnych na terenie województwa oraz procedury reagowania na wypadek różnych sytuacji (np. powódź, skażenie chemiczne, awaria sieci energetycznej). Wojewoda, jako przedstawiciel rządu w terenie, odpowiada za koordynację działań kryzysowych w regionie, stąd plan wojewódzki określa również sposób uruchamiania wsparcia z poziomu centralnego oraz zasady współpracy z sąsiednimi województwami. Zgodnie z ustawą, plany wojewódzkie – podobnie jak krajowy – są aktualizowane co dwa lata i podlegają opiniowaniu przez Rządowe Centrum Bezpieczeństwa oraz zatwierdzeniu przez Wojewódzki Zespół Zarządzania Kryzysowego. Wyniki kontroli Najwyższej Izby Kontroli (NIK) wskazywały w przeszłości, że proces tworzenia spójnego systemu planowania na wszystkich szczeblach przebiegał opieszale – w 2011 r. stwierdzono opóźnienia na poziomie gmin, powiatów i województw w dostosowaniu planów do nowych wymogów

oraz występowanie braków w treści części planów. Przykładowo, Narodowy Plan Zarządzania Kryzysowego przez pewien czas w ogóle nie istniał (mimo ustawowego obowiązku jego opracowania od 2010 r.), co powodowało lukę w systemie planowania. Ponadto NIK zwróciła uwagę, że niektóre gminne i powiatowe plany były niekompatybilne z planami wyższego szczebla, co utrudniało koordynację – jaskrawym przykładem była niespójność planów ochrony przeciwpowodziowej. Te zastrzeżenia stały się impulsem do poprawy integracji planów różnych szczebli w kolejnych latach.

Powiatowy Plan Zarządzania Kryzysowego opracowuje starosta powiatu we współpracy z Powiatowym Zespołem Zarządzania Kryzysowego. Plan powiatowy precyzuje zadania władz powiatu (starosty i służb powiatowych, np. komendy powiatowej PSP, policji, inspektora sanitarnego itp.) w sytuacjach kryzysowych dotyczących obszaru powiatu. Elementem planu powiatowego – podobnie jak innych planów – jest ocena zagrożeń lokalnych i mapa ryzyka dla powiatu. Zawiera on także procedury reagowania na wypadek najbardziej prawdopodobnych kryzysów (np. duży wypadek komunikacyjny, epidemia choroby zakaźnej zwierząt, awaria przemysłowa w zakładzie na terenie powiatu). Plan powiatowy powinien być spójny z planem wojewódzkim oraz gminnymi planami gmin należących do powiatu. Badania wykazują jednak, że spójność planów bywa problematyczna – analiza 40 powiatowych planów zarządzania kryzysowego z lat 2013-2015 wykazała znaczne rozbieżności w zawartości i szczegółowości tych dokumentów²⁵³. Według Wiśniewskiego zawartość powiatowych planów różniła się średnio w niemal 50% w stosunku do ustalonego wzorca, a poziom ich uszczegółowienia był mniejszy o ok. 49% w porównaniu z oczekiwaniami. Różnice dotyczyły zarówno formy prezentacji danych, jak i kompletności informacji, co utrudniało agregację danych na poziomie krajowym i dokonywanie rzetelnej oceny ryzyka w skali kraju. Przyczyną takiego stanu rzeczy jest m.in. brak jednolitych standardów wykonawczych oraz niedostateczny nadzór merytoryczny nad jakością planów na poziomie lokalnym (pomimo istnienia ogólnych wytycznych). W konsekwencji Rządowe Centrum Bezpieczeństwa oraz wojewodowie podejmują działania w celu ujednolicenia

²⁵³ M. Wiśniewski, Analysis of the integrity of district crisis management plans in Poland, *International Journal of Disaster Risk Reduction*, 67, 102650, 2022, <https://doi.org/10.1016/j.ijdr.2021.102650>

formatów i zawartości planów – np. poprzez wzorcowe szablony i wytyczne do planów powiatowych oraz szkolenia dla osób je sporządzających.

Gminny Plan Zarządzania Kryzysowego sporządza wójt, burmistrz lub prezydent miasta dla danej gminy, przy udziale Gminnego Zespołu Zarządzania Kryzysowego. Jest to dokument operacyjny najniższego szczebla w strukturze administracyjnej, obejmujący działania na terenie gminy. Plan gminny zawiera charakterystykę lokalnych zagrożeń, np. listę miejsc o podwyższonym ryzyku (zakłady przemysłowe z niebezpiecznymi substancjami, tereny zalewowe, osuwiskowe itp.), oraz procedury reagowania na incydenty lokalne – takie jak pożary, lokalne podtopienia, skażenie wody pitnej, przerwy w dostawie mediów, epidemie na ograniczoną skalę czy sytuacje kryzysowe w infrastrukturze komunalnej. W planie określa się również lokalne siły i środki do wykorzystania (gminne jednostki Ochotniczej Straży Pożarnej (OSP), lokalne służby komunalne, potencjał lokalnych firm do wsparcia itp.), a także organizację kierowania akcją kryzysową na poziomie gminy (role wójta/burmistrza, komendanta gminnego OSP, kierowników jednostek organizacyjnych gminy). Dla gmin, podobnie jak wyżej, obowiązuje cykliczna aktualizacja planu (co 2 lata). Niestety, poziom przygotowania wielu gmin do sytuacji kryzysowych pozostaje wyzwaniem. NIK w swoim raporcie z 2019 r. podkreśliła, że na poziomie gmin występują szczególnie duże braki kadrowe i kompetencyjne w obszarze zarządzania kryzysowego. Często samo sporządzenie planu przez gminę bywa traktowane jako wypełnienie formalnego obowiązku, bez zapewnienia realnej funkcjonalności dokumentu (np. plany są ogólne, nie zawierają konkretnych procedur czy aktualnych danych kontaktowych)²⁵⁴. Taki formalistyczny charakter planów znacząco obniża ich przydatność praktyczną. Należy jednak zaznaczyć, że istnieją też gminy dobrze przygotowane – NIK w 2011 r. odnotowała dobre praktyki w niektórych urzędach wojewódzkich, które przekładały się na skuteczniejsze działania na niższym szczeblu. Niemniej standaryzacja i realne wdrożenie planów gminnych wciąż wymaga uwagi – stąd postulaty, by plany te były okresowo testowane w praktyce i konsultowane ze społecznością lokalną, która jest ich bezpośrednim beneficjentem.

²⁵⁴ Najwyższa Izba Kontroli, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej (Informacja o wynikach kontroli), nr ewidencyjny: P/17/039 (KPB.430.009.2017; Nr ewid. 147/2018/P/17/039/KPB), Warszawa, NIK, 2019.

Poza planami terytorialnymi, istotną rolę odgrywają plany zarządzania kryzysowego instytucji i podmiotów kluczowych. Ustawa o zarządzaniu kryzysowym nakłada obowiązki planistyczne również na ministrów i centralne organy administracji rządowej (tzw. plany resortowe), co zapewnia, że np. Minister Zdrowia posiada plan na wypadek kryzysu epidemiologicznego, Minister Klimatu – plan reagowania na kryzys zaopatrzenia w energię czy paliwa, itp. Ponadto, przepisy zobowiązują operatorów infrastruktury krytycznej (np. dużych przedsiębiorstw z sektorów energetyki, transportu, telekomunikacji, zaopatrzenia w wodę, finansów) do opracowania planów ochrony infrastruktury krytycznej oraz procedur ciągłości działania swoich systemów. Plany instytucjonalne przygotowują również inne podmioty publiczne: np. szkoły i uczelnie opracowują plany ewakuacji i procedury na wypadek zagrożeń na terenie placówki, szpitale mają plany działań na wypadek zdarzeń masowych i katastrof (tzw. plany awaryjne szpitala, regulowane odrębnymi przepisami resortu zdrowia), zakłady przemysłowe o zwiększonym ryzyku (objęte Dyrektywą Seveso) muszą posiadać wewnętrzne plany operacyjno-ratownicze, a władze lokalne – zewnętrzne plany operacyjne na wypadek awarii chemicznej w takim zakładzie. Celem tych planów instytucjonalnych jest zapewnienie, że każda jednostka lub obiekt mają przygotowaną własną procedurę reagowania zanim wsparcie z zewnątrz (np. służb ratunkowych czy zespołów kryzysowych) dotrze na miejsce.

Szczególnym rodzajem planowania na poziomie organizacji (zarówno firm prywatnych, jak i urzędów) są plany ciągłości działania (Business Continuity Plans, BCP). Tego typu plany koncentrują się na utrzymaniu kluczowych funkcji danej organizacji w sytuacji zakłóceń, takich jak awarie systemów IT, przerwy w dostawie mediów, niedostępność obiektów lub personelu, cyberataki czy inne zdarzenia kryzysowe, które niekoniecznie mają charakter szerokiej klęski żywiołowej, ale bezpośrednio zagrażają ciągłości operacyjnej danej instytucji. Plan ciągłości działania jest udokumentowanym przewodnikiem opisującym sposób reakcji organizacji na zakłócenie oraz kroki niezbędne do przywrócenia krytycznych procesów w akceptowalnym czasie. W odróżnieniu od typowego „planu zarządzania kryzysowego” skupionego na ochronie życia i mienia podczas sytuacji nadzwyczajnych, BCP kładzie nacisk na minimalizację przerw w działalności i szybkie wznowienie usług na określonym minimalnym poziomie. W praktyce jednak oba

podejścia się uzupełniają – organizacja dobrze przygotowana powinna zadbać zarówno o bezpieczeństwo ludzi (plany kryzysowe), jak i o ciągłość kluczowych usług (BCP). W Polsce standardy dotyczące ciągłości działania czerpią z norm międzynarodowych, takich jak ISO 22301:2019, która definiuje wymagania dla systemów zarządzania ciągłością działania (Business Continuity Management System). Zgodnie z tym standardem skuteczne utrzymanie ciągłości obejmuje m.in.: ustanowienie polityki ciągłości działania, wyznaczenie kompetentnych osób odpowiedzialnych, identyfikację kluczowych procesów i zasobów, ocenę ryzyka zakłóceń, przygotowanie procedur awaryjnych, a następnie regularne testowanie i doskonalenie planów. W ostatnich latach, zwłaszcza w wyniku doświadczeń pandemii COVID-19, wzrosła świadomość znaczenia BCP zarówno w sektorze prywatnym, jak i publicznym. Administracja publiczna zaczęła w szerszym zakresie wdrażać plany ciągłości świadczenia usług publicznych – na co zwracają uwagę m.in. raporty Najwyższej Izby Kontroli i wytyczne RCB. Przykładem może być opracowanie w 2024 r. przez Ministerstwo Cyfryzacji metodologii audytu planów ciągłości działania usług publicznych²⁵⁵. Oznacza to, że ciągłość działania staje się integralnym elementem ogólnego systemu bezpieczeństwa państwa, uzupełniając tradycyjne planowanie kryzysowe o perspektywę zarządzania ryzykiem operacyjnym i odpornością instytucjonalną na zakłócenia. Struktura dokumentów planistycznych w zarządzaniu kryzysowym w Polsce jest rozbudowana i obejmuje wiele szczebli oraz typów planów. W teorii gwarantuje to kompleksowe przygotowanie – od poziomu centralnego aż po poszczególne instytucje i przedsiębiorstwa. Wyzwanie stanowi jednak zapewnienie spójności i realnej skuteczności tych planów, tak by nie były one jedynie formalnością, lecz praktycznym narzędziem gotowym do użycia w momencie kryzysu. Jak zauważa Wiśniewski²⁵⁶, brak ujednolicenia formatu i zawartości planów utrudnia ocenę ryzyka i zarządzanie informacją na poziomie krajowym. Z kolei analizy NIK wskazują, że niedociągnięcia w jakości planów i kwalifikacjach osób je sporządzających przekładają się na błędy podczas faktycznych zdarzeń kryzysowych. Dlatego kolejne lata

²⁵⁵ OECD, Wsparcie realizacji audytu planów ciągłości świadczenia usług publicznych w Polsce (wytyczne/metodyka audytu), OECD, 2024.

²⁵⁶ M. Wiśniewski, Analysis of the integrity of district crisis management plans in Poland, *International Journal of Disaster Risk Reduction*, 67, 102650, 2022. <https://doi.org/10.1016/j.ijdr.2021.102650>

przynoszą działania naprawcze: standaryzację, szkolenia specjalistyczne, a także wdrażanie kultury ciągłego doskonalenia planów poprzez ich testowanie i aktualizację.

Skuteczność planu zarządzania kryzysowego zależy w dużej mierze od jego zawartości merytorycznej oraz od tego, czy został opracowany z uwzględnieniem realnych zagrożeń i uwarunkowań. Dobry plan kryzysowy powinien zawierać pewne kluczowe elementy, które zapewnią jego użyteczność w praktyce. Do najważniejszych z nich należą: scenariusze zdarzeń kryzysowych, macierz odpowiedzialności (przydział zadań), zasoby i ich alokacja oraz procedury decyzyjne i operacyjne na czas kryzysu.

Scenariusze – Plan musi opierać się na solidnej analizie ryzyka i przewidywać różne możliwe scenariusze rozwoju sytuacji kryzysowych. Scenariusz w planowaniu kryzysowym to opis hipotetycznego zdarzenia (np. powodzi stuletniej, ataku terrorystycznego w centrum miasta, blackoutu energetycznego trwającego powyżej 72 h, pandemii grypy itd.) wraz z założeniami co do jego przebiegu, skutków i potrzeb interwencyjnych. Opracowanie scenariuszy pozwala dostosować działania do specyfiki danego zagrożenia – inaczej przebiega reagowanie na powódź, a inaczej na skażenie chemiczne. Procedury budowy scenariuszy stały się nawet przedmiotem badań naukowych, które mają ułatwić tworzenie realistycznych i przydatnych scenariuszy. Przykładowo, Wiśniewski zaproponował także metodykę konstruowania scenariuszy zdarzeń niekorzystnych w procesie planowania cywilnego, przetestowaną na danych z planów wojewódzkich²⁵⁷. Istotne jest, by scenariusze w planach były zróżnicowane pod względem skali i rodzaju zagrożeń – obejmowały zarówno scenariusze najbardziej prawdopodobne (wysokiego ryzyka), jak i scenariusze skrajne o niskim prawdopodobieństwie, ale potencjalnie katastrofalnych skutkach. Każdy scenariusz powinien zawierać opis fazy prewencyjnej (jakie działania podjąć zawczasu, by zmniejszyć ryzyko), fazy przygotowania (jakie sygnały ostrzegawcze i działania natychmiastowe przewidzieć), fazy reagowania (jak przebiega akcja ratunkowa/kryzysowa) oraz fazy odbudowy (jak likwidować skutki i odtwarzać normalne warunki). Brak scenariuszy lub ich ogólnikowe potraktowanie

²⁵⁷ M. Wiśniewski, Procedury budowy scenariuszy zdarzeń niekorzystnych w strukturze procesu planowania cywilnego, Zeszyty Naukowe Politechniki Śląskiej, seria: Organizacja i Zarządzanie, (128), 2018, s. 451-473.

sprawia, że plan staje się dokumentem mało konkretnym. Niestety, wcześniejsze kontrole ujawniały przypadki planów (zwłaszcza na szczeblu lokalnym), które nie zawierały istotnych elementów, jakie powinny się w nich znaleźć – można przypuszczać, że chodziło m.in. o brak jasno opisanych scenariuszy czy wariantów rozwoju sytuacji. Dobre praktyki sugerują, że do planu warto włączyć scenariusze alternatywne i wskaźniki progowe (trigger points), po osiągnięciu których uruchamiane są kolejne etapy reagowania lub dodatkowe siły. Przykładowo, scenariusz powodzi może zawierać progi stanów wód, przy których ogłasza się alarm przeciwpowodziowy, zarządza ewakuację zagrożonych osiedli itd. Scenariusze powinny być przygotowane we współpracy z ekspertami od danego rodzaju zagrożeń (np. hydrologami, sejsmologami, epidemiologami) oraz uzgadniane z podmiotami, które będą według nich działać.

Matryce odpowiedzialności – Kolejnym kluczowym elementem planu jest jasne przypisanie ról i zadań wszystkim uczestnikom działań kryzysowych. Często przybiera to formę tabeli lub macierzy, w której w kolumnach wymienia się główne zadania/obszary działań (np. ewakuacja, medyczne ratownictwo, logistyka zaopatrzenia, informacja publiczna, ochrona porządku) a w wierszach – instytucje lub służby. Na przecięciu wskazuje się, kto jest odpowiedzialny za dane zadanie, kto wspiera, ewentualnie kto koordynuje. Taka macierz odpowiedzialności (nierzadko nazywana RACI – od ang. Responsible, Accountable, Consulted, Informed) zapobiega częstemu problemowi w kryzysie: rozmyciu odpowiedzialności lub dublowaniu działań. W sytuacji kryzysowej wszyscy powinni wiedzieć, kto konkretnie odpowiada za dane działanie – np. kto dowodzi ewakuacją ludności, kto organizuje komunikację zastępczą, kto prowadzi komunikaty medialne. Dobrze skonstruowany plan będzie zawierał schemat organizacyjny sztabu kryzysowego oraz listę osób funkcyjnych (z podaniem stanowiska, kompetencji oraz kontaktu). Ważne jest również wyznaczenie zastępstw – plan musi przewidywać, kto przejmie zadania, jeśli osoba przewidziana do roli lidera akcji jest niedostępna. W praktyce, zestawienie ról i zadań bywa prezentowane zarówno tekstowo, jak i graficznie (np. diagramem zależności). Krajowy Plan Zarządzania Kryzysowego pełni wspomnianą rolę matrycy na poziomie krajowym, wyznaczając wiodące podmioty dla poszczególnych zagrożeń. Analogiczne podejście zaleca się w planach wojewódzkich i lokalnych – tam

również powinny znaleźć się czytelne tabele odpowiedzialności, aby np. powiatowy inspektor sanitarny, komendant PSP, wójtowie gmin i inne podmioty wiedzieli, jakie mają obowiązki w ramach powiatowego czy gminnego planu. Niestety, zdarzało się, że na poziomie gmin nie ustalono wyraźnych kompetencji w zarządzaniu kryzysowym – np. brak przypisania konkretnego pracownika urzędu do obsługi zadań zarządzania kryzysowego lub łączenie tej funkcji z innymi obowiązkami bez odpowiedniego przeszkolenia. Taka sytuacja rodzi ryzyko chaosu decyzyjnego. Stąd w ostatnich latach coraz mocniej podkreśla się profesjonalizację kadr – nie tylko rządowych, ale i samorządowych – odpowiedzialnych za ten obszar (o czym szerzej w dalszej części). Plan musi zatem jasno odpowiadać na pytanie: kto, co robi i z kim współpracuje, gdy wydarzy się X.

Zasoby – Nawet najlepszy plan nie zadziała, jeśli braknie zasobów do jego realizacji. Dlatego nieodłącznym elementem planowania kryzysowego jest inwentaryzacja zasobów i opracowanie planów ich użycia. W planach zarządzania kryzysowego zazwyczaj znajduje się wykaz dostępnych sił i środków na danym terenie lub w dyspozycji danej instytucji. Obejmuje to zarówno zasoby ludzkie (jednostki straży pożarnej, policji, wojska, służb medycznych, zespoły ratownictwa chemicznego, energetycznego itp.), jak też sprzęt (np. liczba i rodzaje pojazdów specjalistycznych, pomp wysokiej wydajności, agregatów prądotwórczych, namiotów, łodzi, środków transportu, zapór przeciwpowodziowych, rezerwowe systemy łączności). Plan powinien wskazywać lokalizacje ważnych zasobów (magazyny przeciwpowodziowe, rezerwy żywności i wody, szpitale i miejsca do ewakuacji poszkodowanych, bazy sprzętu ciężkiego) oraz procedury ich uruchomienia. Ważnym elementem jest też plan logistyczny: w jaki sposób dostarczyć zasoby tam, gdzie będą potrzebne, kto jest odpowiedzialny za ich dysponowanie i jak uzupełniać zużyte materiały (np. zaopatrzenie w paliwo dla pojazdów ratowniczych podczas długotrwałej akcji). Macierz zasobów może również przybrać formę tabelaryczną – np. które jednostki posiadają dany typ sprzętu i w jakiej ilości. Planując wykorzystanie zasobów, należy także określić limity i priorytety – np. przy ograniczonej liczbie śmigłowców ratowniczych, w którym scenariuszu zostaną one użyte w pierwszej kolejności. Dobrze skonstruowany plan zawiera procedury alokacji zasobów – kto podejmuje decyzje o skierowaniu dodatkowych sił do gminy dotkniętej kryzysem, jak

występować o wsparcie z sąsiednich regionów lub z poziomu centralnego, jak uruchomić rezerwy strategiczne. Brak tych ustaleń może prowadzić do opóźnień i improwizacji w trakcie realnej akcji. Przykładem problemu z zasobami może być długotrwała przerwa w dostawie prądu – plan wojewódzki czy krajowy powinien wówczas wskazywać dostępne agregaty prądotwórcze, plan ich transportu i instalacji w priorytetowych miejscach (szpitale, stacje ujęcia wody, węzły telekomunikacyjne). Jak wykazały badania²⁵⁸, rozległa awaria zasilania typu blackout stanowi poważny test dla systemu – analizy tego rodzaju zagrożenia pokazały, że wiele krajów (w tym Polska) nie było w pełni przygotowanych na długotrwały brak prądu, co skłoniło do opracowania szczegółowych planów awaryjnego zasilania infrastruktury krytycznej. To pokazuje, że plan musi iść w parze z realnymi inwestycjami w zasoby i ich dyspozycyjność.

Procedury decyzyjne – W sytuacji kryzysowej czas ma kluczowe znaczenie, a chaos informacyjny może prowadzić do paraliżu decyzyjnego. Dlatego plan kryzysowy powinien zawierać jasno zdefiniowane procedury podejmowania decyzji i uruchamiania działań. Chodzi tu m.in. o zasady alarmowania i zwoływania sztabu kryzysowego, tryb wprowadzania stanu nadzwyczajnego (jeśli to konieczne) lub alarmowego na danym terenie, procedury przekazywania władzy dowodzenia (np. z gminy do powiatu, z powiatu do województwa, jeśli skala kryzysu rośnie). Istotne są tzw. procedury reagowania kryzysowego – często tworzone w formie odrębnych kart lub instrukcji wchodzących w skład planu (w KPZK są to np. procedury wykonawcze w częściach B). Procedura opisuje krok po kroku, jakie decyzje powinny zapaść po wystąpieniu zdarzenia: kto ocenia sytuację, komu należy zgłosić informację, jakie działania podjąć natychmiast (np. ewakuacja, ostrzeżenie ludności), jakie służby uruchomić, kiedy i jak wnioskować o pomoc zewnętrzną (np. wojska, wsparcie międzynarodowe). Decyzyjność w kryzysie często wymaga odejścia od hierarchicznych, czasochłonnych procedur biurokratycznych – stąd w dobrym planie zawarte są zapisy dające kierującemu akcją odpowiednie uprawnienia do działania w warunkach nagłych. Przykładowo, plan może przewidywać, że wójt ma prawo natychmiast zarządzić

²⁵⁸ M. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021. <https://doi.org/10.3390/en14248286>

ewakuację na swoim terenie w sytuacji bezpośredniego zagrożenia życia, informując jedynie przełożonych *post factum*, zamiast czekać na ich zgodę. Innym aspektem jest ustanowienie struktur dowodzenia: np. model ICS (Incident Command System) lub analogiczne struktury, które wyznaczają jednoosobowego kierownika akcji i podporządkowanie mu wszystkich działających służb według wspólnego planu działania. W polskich warunkach elementy ICS wprowadzono np. dla dużych akcji ratowniczych pod egidą PSP. W planie warto również określić tryb pracy sztabu kryzysowego – czy działa on w trybie ciągłym (24/7) w czasie kryzysu, jak często odbywają się narady operacyjne, jak wygląda obieg informacji i dokumentowanie decyzji (np. prowadzenie dziennika działań). NIK stwierdziła, że brak wiedzy i kompetencji osób zaangażowanych w zarządzanie kryzysowe na poziomie lokalnym prowadził do niewłaściwych decyzji. Opisano przypadek, gdzie w ćwiczebnej sytuacji skażenia chemicznego ewakuowano ludność do strefy skażonej, co w realnym działaniu skończyłoby się tragicznie²⁵⁹. Powodem był brak elementarnej wiedzy osób decydujących. Odpowiednie procedury decyzyjne w planie (oraz przeszkolenie ludzi z ich stosowania) mają właśnie zapobiegać tego rodzaju błędom – decyzje muszą opierać się na wcześniej uzgodnionych zasadach nauczonych podczas ćwiczeń, a nie być podejmowane *ad hoc* w stresie. Kompleksowy plan zarządzania kryzysowego powinien być konkretny, praktyczny i dostosowany do realiów. Powinien zawierać scenariusze zagrożeń (co się może stać), przydział ról (kto co robi), plan wykorzystania zasobów (czym dysponujemy i jak to użyjemy) oraz procedury działania (jak będziemy podejmować decyzje i prowadzić akcję). Dodatkowo ważnymi elementami są: aktualne dane kontaktowe do wszystkich zaangażowanych podmiotów, plan komunikacji (zarówno wewnętrznej – między służbami, jak i zewnętrznej – z mediami i społeczeństwem), a także aneksy z mapami, schematami organizacyjnymi, listami kontrolnymi itp. Plan musi być dokumentem żywym – regularnie aktualizowanym, ćwiczoną i korygowaną na podstawie doświadczeń oraz zmieniających się uwarunkowań (np. nowych inwestycji, zmiany sieci dróg, pojawienia się nowych zagrożeń). Tylko wtedy spełni swoją rolę podczas faktycznego

²⁵⁹ J. Ostrowski, D. Krzysztofik, Człowiek największym wyzwaniem systemu ochrony ludności, Wspólnota (Pismo Samorządu Terytorialnego), 2024.

kryzysu. Samo posiadanie nawet najlepszego planu nie gwarantuje powodzenia działań kryzysowych, jeśli ludzie odpowiedzialni za jego realizację nie są odpowiednio przeszkoleni i przygotowani. Szkolenia i ćwiczenia stanowią integralną część fazy przygotowania do sytuacji kryzysowych²⁶⁰. Ich celem jest upewnienie się, że wszystkie osoby i instytucje wiedzą, jakie mają zadania w kryzysie, potrafią skutecznie współdziałać i podejmować decyzje pod presją czasu i niepewności.

Szkolenia teoretyczne – Pierwszym poziomem przygotowania jest przekazanie wiedzy na temat planów, procedur i ogólnych zasad reagowania. Obejmuje to np. szkolenia dla członków gminnych zespołów zarządzania kryzysowego z zakresu przepisów prawa, obowiązków podczas poszczególnych zagrożeń, zasad alarmowania i łączności, itp. Takie szkolenia często mają formę seminariów, wykładów czy warsztatów. Ważne jest, by uczestniczyły w nich osoby na co dzień pełniące różne funkcje – urzędnicy, przedstawiciele służb, ale też np. administratorzy infrastruktury krytycznej czy dyrektorzy kluczowych instytucji. Dzięki temu wszyscy zdobywają wspólny język i zrozumienie planu. Niestety, w Polsce bywało z tym różnie – NIK w 2019 r. wykazała, że wielu pracowników odpowiedzialnych za zarządzanie kryzysowe na poziomie lokalnym nie miało odpowiednich kwalifikacji i nie przeszło specjalistycznych szkoleń. Co więcej, do 2019 r. nie istniały formalne wymagania co do wykształcenia i doświadczenia osób zatrudnianych na stanowiskach ds. zarządzania kryzysowego w samorządach. To powodowało, że nierzadko funkcje te pełniły przypadkowe osoby, dla których była to poboczna część obowiązków. W odpowiedzi na te problemy, podjęto działania zmierzające do profesjonalizacji kadr – m.in. uruchomiono studia podyplomowe z zarządzania kryzysowego, certyfikowane kursy (np. przez RCB czy szkoły PSP) oraz zaczęto wymagać od koordynatorów kryzysowych określonych szkoleń podstawowych. W roku 2020 i kolejnych, w wielu gminach i powiatach przeprowadzono dodatkowe szkolenia z obsługi nowych narzędzi (np. aplikacji do ostrzegania, systemów łączności kryzysowej) w związku z wprowadzeniem krajowego systemu ostrzegania SMS (Alert RCB) i innych rozwiązań technicznych.

²⁶⁰ W. Skomra, Edukacja jako element zarządzania kryzysowego, Wiadomości Ubezpieczeniowe (wydanie specjalne: Powódź – Infrastruktura – Finansowanie), Polska Izba Ubezpieczeń, 2012, s. 13-18.

Ćwiczenia praktyczne – Kluczowym sprawdzianem przygotowania są ćwiczenia, podczas których uczestnicy w warunkach symulowanych odtwarzają swoje role i działania tak, jakby doszło do prawdziwego kryzysu. Ćwiczenia mogą mieć różny charakter i skalę: od ćwiczeń sztabowych (table-top exercises), poprzez gry decyzyjne, aż po pełnoskalowe ćwiczenia poligonowe z udziałem służb. Gry decyzyjne to symulacje prowadzone zazwyczaj w sali – uczestnicy (np. członkowie sztabu kryzysowego) otrzymują scenariusz sytuacji i muszą podejmować decyzje na podstawie napływających „meldunków” i informacji. Tego typu gry są bardzo użytecznym narzędziem dydaktycznym – pozwalają trenować proces decyzyjny pod presją czasu, koordynację między różnymi podmiotami oraz komunikację²⁶¹. Jak wskazują specjaliści, gry decyzyjne wyzwalały emocje zbliżone do realnych i zmuszają uczestników do myślenia w warunkach niepełnych danych, co świetnie przygotowuje na rzeczywistość kryzysu. Przykładem gry decyzyjnej może być symulacja ataku terrorystycznego w mieście: zespół uczestników (władze miasta, policja, straż, pogotowie) musi wspólnie zdecydować o ewakuacji, zamknięciu przestrzeni publicznych, informowaniu mieszkańców, podczas gdy moderator (zespół kontrolny ćwiczenia) dostarcza kolejne informacje o rozwoju sytuacji. Ćwiczenia sztabowe są podobne, choć często bardziej formalne – odtwarza się pracę sztabu kryzysowego według procedur, np. przez kilka godzin symuluje się przebieg powodzi od ostrzeżenia hydrologicznego aż po przerwanie wału i konieczność ewakuacji dzielnic. W trakcie ćwiczeń sztabowych uczestnicy uczą się współpracy i komunikacji – np. kto komu przekazuje informacje, jak często odbywają się odprawy, jak formułować polecenia i raporty. Najbardziej rozbudowaną formą są ćwiczenia praktyczne z pozoracją – angażują one realne siły ratownicze, wolontariuszy odgrywających rolę poszkodowanych, używany jest sprzęt i pojazdy. Przykładem może być cykliczne ogólnopolskie ćwiczenie RENEGADE/SAREX (organizowane we współpracy z wojskiem i NATO) symulujące katastrofę lotniczą i incydent terrorystyczny z użyciem statku powietrznego – w ćwiczeniu tym udział biorą wojsko, policja, straż pożarna, ratownicy medyczni i inne służby, a sztaby na różnych szczeblach trenują wspólne

²⁶¹ J. Falecki, Organizacja gier decyzyjnych w zarządzaniu kryzysowym, Sosnowiec, Oficyna Wydawnicza Humanitas, 2016.

działania. Innym przykładem były ćwiczenia LIBERO z 2018 r., symulujące długotrwały blackout energetyczny w dużej części kraju – scenariusz zakładał brak zasilania przez kilkadziesiąt godzin i sprawdzał gotowość systemu energetycznego, samorządów i służb do radzenia sobie z konsekwencjami (brak ogrzewania, łączności, zaopatrzenia itp.). Takie ćwiczenia ujawniają praktyczne problemy, które trudno przewidzieć „na papierze” – np. podczas testów blackoutu okazało się, że wiele gmin nie ma awaryjnych źródeł energii dla zapewnienia ciągłości pracy infrastruktury wodno-kanalizacyjnej, co stało się impulsem do zmian w planach zarządzania kryzysowego i inwestycji w agregaty²⁶². Ćwiczenia polowe organizuje się również na poziomie regionalnym – np. wojewodowie co pewien czas zarządzają wojewódzkie ćwiczenia obronne lub kryzysowe z udziałem służb i samorządów (scenariusze obejmują np. powódź, skażenie chemiczne, migracje ludności na dużą skalę itp.).

Testowanie planów – Każde ćwiczenie pełni jednocześnie rolę testu dla obowiązujących planów. Pozwala zweryfikować, czy procedury zapisane w dokumentach faktycznie działają w praktyce. Często bezpośrednio po ćwiczeniu przeprowadza się szczegółowe omówienie (tzw. debriefing), podczas którego analizowane są działania uczestników i ich zgodność z planem. Na tej podstawie formułuje się wnioski i rekomendacje – np. konieczność doprecyzowania pewnych procedur, dodania brakujących danych kontaktowych, usprawnienia łączności między konkretnymi podmiotami itp. Dobrym zwyczajem jest sporządzenie raportu z ćwiczenia, który zawiera listę zaobserwowanych nieprawidłowości czy trudności i zalecenia ich rozwiązania. Następnie raport taki przekłada się na aktualizację planów oraz plan kolejnych szkoleń. W ten sposób zamyka się pętlę ciągłego doskonalenia: plan – szkolenie – ćwiczenie – korekta planu. W literaturze przedmiotu podkreśla się, że planowanie kryzysowe jest procesem ciągłym, a nie jednorazowym aktem – organizacje powinny stale uczyć się na doświadczeniach (ang. *lessons learned*), zarówno własnych, jak i innych (np. analizując cudze sytuacje kryzysowe i wdrażając u siebie wnioski z tych analiz). W Polsce pewnym problemem pozostawało długo ograniczone wykorzystanie ćwiczeń na

²⁶² M. Majchrzak, K. Michalski, J. Reginia-Zacharski, Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021. <https://doi.org/10.3390/en14248286>

najniższych szczeblach – o ile służby ratownicze (PSP, Policja, PRM) regularnie ćwiczą procedury, o tyle sztaby kryzysowe gmin czy powiatów zbierały się rzadko, często tylko „na papierze”. NIK w raportach wskazywała, że zaniedbania w szkoleniu kadr kryzysowych na poziomie samorządowym skutkują niską gotowością. W ostatnich latach dostrzeżono tę lukę – np. RCB we współpracy ze Związkiem Powiatów Polskich organizowało warsztaty i treningi decyzyjne dla samorządowców, symulując różne scenariusze (np. kryzys migracyjny na granicy w 2021 r., masowe zachorowania COVID-19 w 2020 r.). Ponadto duży kryzys realny – pandemia koronawirusa w latach 2020-21 – niejako zmusił wszystkie szczeble do działania w warunkach kryzysowych, co ujawniło liczne mankamenty, ale też zwiększyło doświadczenie praktyczne kadr. Wiele samorządów po tej lekcji zaktualizowało swoje plany i procedury, a także przećwiczyło (już w rzeczywistości) elementy takie jak rozdysponowanie środków ochrony osobistej, organizacja zdalnego działania urzędu czy masowe informowanie mieszkańców o restrykcjach.

Jak można zauważyć, przygotowanie do kryzysu nie kończy się na napisaniu planu – wymaga ciężkiej pracy nad praktycznym opanowaniem tego planu przez ludzi, którzy będą go realizować. Regularne szkolenia specjalistyczne budują kompetencje i wiedzę teoretyczną, natomiast ćwiczenia terenowe i symulacyjne kształtują umiejętności praktyczne, pozwalając zagrać współdziałanie różnych podmiotów. Dzięki temu w sytuacji prawdziwego zagrożenia mniej rzeczy „zaskoczy” decydentów i służby – będą oni działać według przećwiczonych schematów, co zwiększa szansę na sprawne opanowanie kryzysu i zmniejszenie jego skutków.

Istotną częścią przygotowania na sytuacje kryzysowe jest system wczesnego ostrzegania i alarmowania ludności o zagrożeniach. Nawet najlepszy plan i gotowe zasoby nie spełnią swojej roli, jeśli osoby zagrożone nie zostaną na czas poinformowane o niebezpieczeństwie i nie podejmą właściwych działań ochronnych. Dlatego budowa efektywnego systemu ostrzegania stanowi ważny aspekt fazy przygotowania – umożliwia skrócenie czasu reakcji społeczeństwa oraz służb, a tym samym zmniejszenie potencjalnych strat. Tradycyjnie w Polsce funkcjonował system alarmowania oparty na syrenach (obrony cywilnej) – wciąż wykorzystywany do ogłaszania alarmów (ciągły dźwięk syreny oznacza alarm, modulowany – odwołanie alarmu). Jednak zasięg i skuteczność syren są ograniczone (nie wszędzie je słychać,

a ludzie nie zawsze znają znaczenie sygnałów). W ostatnich latach postawiono zatem na unowocześnienie sposobów ostrzegania, zwłaszcza z wykorzystaniem telefonii komórkowej. System Alert RCB, uruchomiony w 2018 r., stał się centralnym elementem ostrzegania ludności przed nagłymi zagrożeniami. Jest to system komunikatów SMS wysyłanych do wszystkich telefonów komórkowych znajdujących się na obszarze przewidywanego zagrożenia. Implementacja Alertu RCB była odpowiedzią na potrzebę szybkiego i masowego przekazywania ostrzeżeń, z pominięciem tradycyjnych mediów (radia, TV). Działa on w oparciu o technologię Cell Broadcast, co oznacza, że wiadomość dociera do każdego telefonu zarejestrowanego w stacjach bazowych na danym terenie – niezależnie od tego, czy jest to mieszkaniec, czy osoba przebywająca przejazdem. Wiadomość taka ma standaryzowaną formę – zazwyczaj zawiera rodzaj zagrożenia, lokalizację, czas ważności ostrzeżenia oraz zalecenia dla ludności. Przykładowo: „Uwaga! 08/09.07 prognozowane intensywne opady deszczu. Możliwe podtopienia. Nie zbliżaj się do wezbranych rzek. Słuchaj poleceń służb.” – taki komunikat ostrzega przed nawałnicą i daje konkretne wskazówki. Alert RCB jest uruchamiany przez Rządowe Centrum Bezpieczeństwa w porozumieniu z właściwymi służbami (np. IMGW przy zagrożeniach meteorologicznych) i za zgodą MSWiA. Podstawa prawna do wysyłania takich alertów została wprowadzona w ustawie o zarządzaniu kryzysowym – organy administracji publicznej uzyskały uprawnienie do przekazywania w ten sposób informacji w razie zagrożenia życia, zdrowia, mienia lub środowiska, a operatorzy komórkowi są zobowiązani do niezwłocznej dystrybucji tych komunikatów. Od momentu uruchomienia systemu (styczeń 2018 r.) do chwili obecnej Alert RCB był używany wielokrotnie przy różnego rodzaju zdarzeniach. Początkowo dotyczył głównie ekstremalnych zjawisk pogodowych – silnych burz, huraganowych wiatrów, intensywnych opadów powodujących powódzie błyskawiczne. Z czasem zastosowanie rozszerzono: ostrzegano przed falami upałów (szczególnie groźnymi dla osób starszych), przed skażeniami wody (np. po awarii kolektora w Warszawie), przed zdarzeniami chemicznymi (jak pożar składowiska toksycznych odpadów), a także wykorzystywano system do pilnych komunikatów w trakcie pandemii COVID-19 (np. o wprowadzanych obostrzeniach na danym obszarze). Badania opinii publicznej pokazują, że system ten szybko stał się powszechnie rozpoznawalny – według ankiety

z końca 2019 r., 81% Polaków otrzymało przynajmniej raz SMS z Alertem RCB²⁶³. Większość oceniała tę formę ostrzeżeń jako przydatną i zwiększającą poczucie bezpieczeństwa. Dzięki bezpośredniemu dotarciu do obywateli system pozwala na wcześniejsze przygotowanie się – np. zabezpieczenie dobytku przed nadciągającą burzą czy też szybkie opuszczenie zagrożonego obszaru. W ocenie RCB, Alert RCB znacząco poprawił skuteczność ostrzegania ludności i stał się ważnym uzupełnieniem dotychczasowych metod. Oczywiście, system ostrzegania to nie tylko Alert RCB. Nadal funkcjonują tradycyjne kanały jak komunikaty radiowe i telewizyjne – w sytuacjach kryzysowych uruchamia się tzw. komunikaty alarmowe nadawane w radio/TV (warto, aby plany zarządzania kryzysowego zawierały gotowe wzory takich komunikatów do szybkiego użycia). Ponadto od 2015 r. działa Regionalny System Ostrzegania (RSO) – jest to usługa pozwalająca na przekazywanie ostrzeżeń poprzez telewizję (napisy DVB na ekranie TV) oraz aplikację mobilną. RSO docelowo służy przekazywaniu komunikatów wojewodów o lokalnych zagrożeniach, integruje się z nim też Alert RCB. Wreszcie, ważnym ogniwem są syreny alarmowe – w wielu gminach przeprowadzono modernizację i rozbudowę sieci syren, aby w razie np. skażenia chemicznego czy ataku z powietrza móc natychmiast zaalarmować mieszkańców. Syreny te coraz częściej sterowane są zdalnie (radiowo) i mogą być uruchamiane przez wojewodów lub RCB centralnie, co poprawia ich użyteczność. Nowoczesne systemy alarmowe pozwalają też na nadawanie komunikatów głosowych przez syreny (tzw. systemy miejskiego ostrzegania i alarmowania z głośnikami), choć to rozwiązanie jest nierównomiernie wdrożone – głównie w większych miastach.

System ostrzegania ludności należy traktować jako nierozzerwalną część przygotowania kryzysowego. Plan zarządzania kryzysowego powinien zawierać procedury uruchamiania alarmowania – kto podejmuje decyzję o nadaniu komunikatu (np. wójt w porozumieniu z PSP przy lokalnym pożarze chemicznym), jakiej treści mają być komunikaty i jakimi kanałami dystrybuowane. Ważne jest również edukowanie społeczeństwa, jak reagować na ostrzeżenia. Ten element jest często niedoceniany – ludzie muszą

²⁶³ P. Majcher, Alert RCB – dotychczasowe doświadczenia, Biuletyn kwartalny Rządowego Centrum Bezpieczeństwa (Biuro Analiz i Reagowania), nr 29 (październik-grudzień 2019), 2020.

wiedzieć, co oznacza dany sygnał lub SMS i jakie działania powinni podjąć (np. pozostanie w domu, przygotowanie zapasów, ewakuacja). Rządowe Centrum Bezpieczeństwa prowadzi kampanie informacyjne na ten temat, a alarmy syren są okresowo testowane (np. w rocznicę Powstania Warszawskiego odbywa się ogólnopolski test syren, co przy okazji przypomina znaczenie tych sygnałów). System ostrzegania stale jest doskonalony – trwają prace nad wykorzystaniem nowych technologii, jak Cell Broadcast w standardzie 5G, powiadomienia geolokalizacyjne w aplikacjach, integracja z systemami samochodowymi itp. Pojawiają się też głosy krytyczne, aby unikać nadużywania Alertu RCB do komunikatów o charakterze informacyjnym niezwiązanym z bezpośrednim zagrożeniem (co zdarzało się np. na początku pandemii, gdy SMS-y dotyczyły zasad wyborów korespondencyjnych czy kontroli granicznych). Ekspertki wskazują, że dla zachowania skuteczności systemu ostrzeżeń, ludzie powinni otrzymywać alerty tylko w sytuacjach rzeczywistego niebezpieczeństwa, tak, aby zawsze traktowali je poważnie. Reasumując, system wczesnego ostrzegania jest ważnym „technicznym” filarem przygotowań kryzysowych. Umożliwia on przekazanie społeczeństwu cennego czasu na reakcję – czy to schronienie się, ewakuację, czy podjęcie innych środków ostrożności. Zintegrowanie nowoczesnych narzędzi (jak Alert RCB) z tradycyjnymi metodami alarmowania zwiększa odporność kraju na zagrożenia poprzez redukcję potencjalnych ofiar i szkód. W połączeniu z dobrze przygotowanymi planami i przeszkolonym personelem, efektywny system ostrzegania stanowi gwarancję, że gdy kryzys nadejdzie, społeczeństwo nie będzie całkowicie zaskoczone, lecz otrzyma jasne wskazówki, jak się ratować. Jest to zatem nieodzowna część kompleksowego podejścia do bezpieczeństwa, które obejmuje zarówno planowanie, trening, jak i informowanie obywateli.

3.3. Reagowanie i zarządzanie w czasie kryzysu

System zarządzania kryzysowego opiera się na zhierarchizowanej strukturze organów na różnych szczeblach administracji, z wyraźnym podziałem kompetencji między poziom krajowy, wojewódzki, powiatowy i gminny. Na każdym z tych poziomów funkcjonuje organ kierujący

(jednoosobowy decydent, np. wójt, starosta, wojewoda, premier), wspierany przez zespół zarządzania kryzysowego (organ doradczo-opiniotwórczy) oraz centrum zarządzania kryzysowego (całodobowe centrum operacyjne). Taka architektura zapewnia sprawne podejmowanie decyzji, koordynację służb i spójne wdrażanie planów reagowania, a także realizuje zasadę jednoosobowego kierownictwa, gwarantując, że na każdym obszarze działania jest wyznaczony jeden odpowiedzialny dowódca mogący szybko wydawać polecenia. Zasada prymatu jednoosobowego kierownictwa polega na powierzeniu kompetencji decyzyjnych jednoosobowym organom władzy właściwym dla danego szczebla – np. burmistrzowi, staroście, wojewodzie – co skraca ścieżki decyzyjne i usprawnia kierowanie akcją²⁶⁴. Jednocześnie obowiązuje zasada układu terytorialnego, zgodnie z którą reakcja następuje jak najbliżej miejsca zagrożenia, a wyższe szczeble włączają się w miarę potrzeb, zapewniając wsparcie lokalnym siłom.

W praktyce oznacza to, że na poziomie centralnym Rada Ministrów z Premierem na czele odpowiada za zarządzanie kryzysowe w skali kraju, korzystając z Rządowego Zespołu Zarządzania Kryzysowego (RZZK) jako ciała doradczego oraz z Rządowego Centrum Bezpieczeństwa (RCB) jako krajowego centrum operacyjnego. Na poziomie województwa to Wojewoda kieruje działaniami, przy pomocy Wojewódzkiego Zespołu Zarządzania Kryzysowego i Wojewódzkiego Centrum Zarządzania Kryzysowego, analogicznie na szczeblu powiatu rolę tę pełni Starosta ze swoim zespołem i centrum, a na szczeblu gminy – Wójt/Burmistrz/Prezydent miasta ze sztabem gminnym i lokalnym centrum operacyjnym²⁶⁵. Wszystkie te organy współpracują ze sobą i utrzymują łączność zarówno pionowo (między szczeblami), jak i poziomo (między służbami), wymieniając informacje o zagrożeniach i potrzebach. Dzięki istnieniu centrów zarządzania kryzysowego zapewniony jest całodobowy przepływ informacji i monitorowanie sytuacji na każdym poziomie (np. powiatowe centra pełnią dyżury 24/7 na potrzeby ostrzegania i koordynacji)²⁶⁶. W sytuacji kryzysowej organ kierujący działaniami (np. sta-

²⁶⁴ J. Gryz, W. Kitler (red.), System reagowania kryzysowego, Toruń, Wydawnictwo Adam Marszałek, 2007.

²⁶⁵ P. Idrian, Zarządzanie kryzysowe a system bezpieczeństwa narodowego. Obronność, *Zeszyty Naukowe*, 3(15), 2015, s. 18.

²⁶⁶ W. Otwinowski, Podstawy zarządzania kryzysowego i systemu obronnego, Poznań, Wydawnictwo Naukowe Wyższej Szkoły Handlu i Usług, 2015.

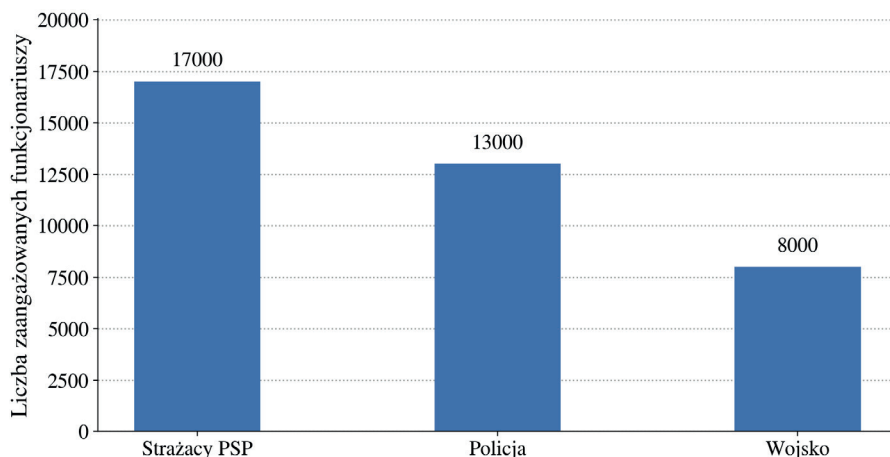
rosta na terenie powiatu) korzysta ze wsparcia swojego sztabu kryzysowego, który analizuje rozwój zdarzeń, proponuje użycie niezbędnych sił i środków oraz doradza w koordynacji działań różnych służb. Centra zarządzania kryzysowego zapewniają natomiast infrastrukturę do zarządzania operacyjnego – zbierają i przekazują meldunki, utrzymują łączność między podmiotami ratowniczymi, uruchamiają procedury alarmowania, a w razie potrzeby przekazują sprawę na wyższy szczebel. Ważnym elementem systemu są również punkty kierowania działaniami bezpośrednio na miejscu zdarzenia – np. wyznaczony posterunek dowodzenia akcją ratunkową – skład dowódca akcji (zazwyczaj oficer Państwowej Straży Pożarnej przy zdarzeniach ratowniczo-gaśniczych) kieruje bezpośrednio pracą podległych sił na terenie operacji. Zapewnienie jednoosobowego dowodzenia na miejscu akcji (np. Kierownika Działów Ratowniczych) jest kluczowe dla unikania chaosu i sprzecznych poleceń w dynamicznym środowisku kryzysowym²⁶⁷. Jednocześnie obowiązuje zasada współdziałania – wszystkie służby, inspekcje i straże zaangażowane w reagowanie (Straż Pożarna, Policja, Pogotowie, Wojsko, itd.) są podporządkowane wspólnemu celowi ochrony życia i mienia, a ich działania powinny być skoordynowane przez ustanowiony sztab kryzysowy²⁶⁸.

Faza reagowania rozpoczyna się natychmiast po wystąpieniu sytuacji kryzysowej (katastrofy, klęski żywiołowej, poważnego wypadku etc.) i polega na podejmowaniu działań w celu udzielenia pomocy poszkodowanym, zahamowania rozwoju zagrożeń oraz ograniczenia strat i zniszczeń. W praktyce można wyróżnić szereg typowych czynności realizowanych przez służby ratownicze i organy władzy w tej fazie. Do najważniejszych należą: ewakuacja ludności z obszarów zagrożonych, działania ratownicze (poszukiwawcze, medyczne, gaśnicze itp.), ochrona mienia oraz zabezpieczenie infrastruktury krytycznej i utrzymanie porządku publicznego na dotkniętym kryzysem terenie. Ewakuacja jest jednym z pierwszych i podstawowych działań ochronnych – polega na zorganizowanym przemieszczaniu ludzi (oraz niekiedy zwierząt i cennego mienia) z rejonów niebezpiecznych

²⁶⁷ I. Sterczewska, Wybrane elementy zarządzania kryzysowego, *Bezpieczeństwo. Teoria i Praktyka*, 4, 2016, s. 81-95.

²⁶⁸ W. Lidwa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach zagrożeń niemilitarnych*, Warszawa, Akademia Obrony Narodowej, 2010.

do rejonów bezpiecznych²⁶⁹. Dobrze przeprowadzona ewakuacja potrafi uratować życie wielu osobom i minimalizuje liczbę ofiar katastrofy. Przykładowo podczas powodzi w Polsce w maju-czerwcu 2010 r. służby ewakuowały prewencyjnie około 30 tysięcy osób z terenów zalanych. Było to największe przemieszczenie ludności w sytuacji kryzysowej w Polsce od dekad – akcję zabezpieczały siły Państwowej Straży Pożarnej, Policji oraz Wojska Polskiego, działając wspólnie pod kierownictwem władz lokalnych i centralnych. Udział służb w reagowaniu na powódź 2010 r. w Polsce – liczba funkcjonariuszy zaangażowanych w działania ratunkowe (Straż Pożarna, Policja, Wojsko) przedstawiony został na rysunku 11.



Rysunek 11. Udział służb w reagowaniu na powódź 2010 r. w Polsce – liczba funkcjonariuszy zaangażowanych w działania ratunkowe (Straż Pożarna, Policja, Wojsko)

Źródło: opracowanie własne.

W akcjach przeciwpowodziowych w 2010 r. uczestniczyło łącznie ponad 17 tysięcy strażaków PSP, 13 tysięcy policjantów oraz 8 tysięcy żołnierzy, co obrazuje znaczenie współdziałania różnych formacji w reagowaniu na duży kryzys²⁷⁰. Ewakuacja może mieć charakter doraźny (natychmiastowy,

²⁶⁹ Z. Świątek (red.), Mały słownik języka polskiego: Obrona cywilna i zarządzanie kryzysowe, Warszawa, Wydawnictwo Ministerstwa Obrony Narodowej, 2012.

²⁷⁰ W. Leśniakiewicz, Strażacy o powodzi: 19 ofiar, 30 tys. ewakuowanych (wypowiedź Komendanta Głównego PSP; dane o zaangażowaniu: 17 tys. strażaków, 13 tys. policjantów, 8 tys. żołnierzy), depesza PAP, 17.06.2010, 2010.

w sytuacji nagłego zagrożenia, np. zarządzanie opuszczenia budynku po wykryciu pożaru) lub planowy (przygotowany zawczasu na wypadek przewidywalnych zagrożeń, np. ewakuacja powodziowa czy przed operacjami bojowymi). Istotne jest zapewnienie ewakuowanym niezbędnej opieki – w tym tymczasowych schronień, wyżywienia, opieki medycznej i psychologicznej. Dlatego reagowanie kryzysowe obejmuje również organizację punktów recepcyjnych i miejsc pobytu dla ewakuowanych oraz uruchomienie pomocy humanitarnej²⁷¹. Równolegle do działań organizacyjnych realizowane są właściwe czynności ratownicze, ukierunkowane na ochronę życia i zdrowia ludzi oraz ograniczanie strat materialnych wywołanych zdarzeniem. W zależności od charakteru sytuacji kryzysowej wiodącą rolę w działaniach operacyjnych przypisuje się różnym podmiotom: Państwowej Straży Pożarnej w przypadku pożarów, katastrof budowlanych oraz klęsk żywiołowych, Policji w zdarzeniach związanych z zagrożeniami bezpieczeństwa publicznego (w tym aktami terrorystycznymi lub masowymi zakłóceniami porządku), Państwowemu Ratownictwu Medycznemu w sytuacjach wieloosobowych zdarzeń medycznych oraz kryzysów zdrowotnych, a także Siłom Zbrojnym RP w sytuacjach przekraczających możliwości służb cywilnych, w szczególności gdy konieczne jest wykorzystanie specjalistycznych zdolności (np. komponentów inżynierskich do działań przeciwpowodziowych lub zdolności CBRN do działań związanych ze skażeniami). W praktyce działania ratownicze mają najczęściej charakter wielopodmiotowy, w ramach którego równocześnie prowadzone są zadania o odmiennym profilu, np. uwalnianie osób poszkodowanych, udzielanie medycznych czynności ratunkowych, zabezpieczenie terenu i organizacja ruchu, a także uruchomienie wsparcia technicznego właściwych służb branżowych. Koordynacja działań zapewniana jest poprzez wyznaczanie wspólnych priorytetów operacyjnych, w tym nadrzędności ochrony życia i zdrowia nad ochroną mienia, oraz poprzez bieżącą wymianę informacji między kierującymi poszczególnymi odcinkami działań. Istotnym elementem fazy reagowania pozostaje ochrona mienia i infrastruktury. Po ograniczeniu bezpośredniego zagrożenia dla życia podejmowane są działania zmierzające do zabezpieczenia mienia ludności oraz

²⁷¹ Rozporządzenie Rady Ministrów z dnia 30 maja 2025 r. w sprawie ewakuacji ludności oraz zabezpieczenia mienia (Dz.U. z 2025 r. poz. 765, § 18).

ochrony kluczowych obiektów i instalacji przed dalszymi stratami. W tym kontekście realizowane bywa patrolowanie obszarów poddanych ewakuacji w celu przeciwdziałania przestępczości przeciwko mieniu oraz ograniczania ryzyka aktów dewastacji. Równolegle podejmowane są przedsięwzięcia zabezpieczające uszkodzoną infrastrukturę, obejmujące m.in. doraźne naprawy i wzmacnianie elementów zabezpieczeń przeciwpowodziowych, stabilizowanie konstrukcji naruszonych w wyniku zdarzeń technicznych, a także odłączanie zasilania elektrycznego i gazu w uszkodzonych instalacjach w celu ograniczenia ryzyka zdarzeń wtórnych, takich jak pożary lub eksplozje²⁷². Utrzymanie porządku publicznego w strefie działań uznawane jest za warunek skuteczności reagowania, dlatego wprowadzane mogą być strefy zamknięte, ograniczenia dostępu oraz czasowe regulacje porządkowe, w tym zakazy przebywania na określonym obszarze, w celu zapewnienia bezpieczeństwa osobom postronnym oraz usprawnienia pracy służb. Zadania te realizowane są zasadniczo przez Policję oraz formacje wspierające, a w uzasadnionych przypadkach również przy współdziałaniu Żandarmerii Wojskowej, zwłaszcza w warunkach reżimów prawnych właściwych stanom nadzwyczajnym. W ramach reagowania istotne znaczenie przypisuje się także zapewnieniu ciągłości funkcjonowania usług kluczowych. Ochrona i podtrzymanie pracy infrastruktury krytycznej, w szczególności w obszarze dostaw energii, wody, łączności, paliw oraz systemów teleinformatycznych, stanowią część działań ukierunkowanych na stabilizację sytuacji oraz ograniczenie skutków wtórnych kryzysu. Służby techniczne i operatorzy infrastruktury realizują wówczas prace odtworzeniowe w warunkach wysokiej presji czasowej, dążąc do przywrócenia podstawowych usług lub zapewnienia rozwiązań zastępczych, takich jak zasilanie awaryjne czy alternatywne źródła zaopatrzenia w wodę. Priorytety działań odtworzeniowych określone są w trybie zarządczym, z uwzględnieniem krytycznych potrzeb ludności i funkcjonowania instytucji kluczowych, w tym placówek ochrony zdrowia oraz obiektów infrastruktury publicznej²⁷³. Należy podkreślić, że faza reagowania charakteryzuje się szczególnie wysoką intensywnością czasową oraz

²⁷² A. Bednarski, Rola Policji w zabezpieczeniu mienia w sytuacjach kryzysowych, w: Wyzwania bezpieczeństwa wewnętrznego, K. Dobek (red.), Warszawa, Wyższa Szkoła Policji w Szczytnie, 2018.

²⁷³ D. Alexander, *Principles of Emergency Planning and Management*, New York, Oxford University Press, 2002.

prowadzeniem działań w warunkach presji decyzyjnej i niepewności informacyjnej. W dalszej części przedstawiona zostanie specyfika podejmowania decyzji w takich uwarunkowaniach oraz znaczenie sprawnego zarządzania informacją.

Kolejne ważne zagadnienie to decyzje pod presją czasu, niepewności i stresu, tj. zarządzanie informacją i ryzykiem. Zarządzanie kryzysowe to szczególnie rodzaj działalności kierowniczej, który odbywa się pod ekstremalną presją czasu i w warunkach niepełnej informacji. Decydenci często muszą działać szybko, na podstawie niepełnych lub przeciwnie – nadmiernych, chaotycznych informacji, przy świadomości wysokiej niepewności co do skutków swoich decyzji oraz stresu związanego z powagą sytuacji. Jak ujął to Otwinowski, typowe cechy decyzji kryzysowych to m.in. ograniczony czas na reakcję, działanie pod presją, brak pełnych danych, niepewność rezultatów oraz skrócony proces decyzyjny²⁷⁴. W takich warunkach łatwo o błędy wynikające z pośpiechu, przeciążenia informacją lub paniki. Dlatego kluczowe jest wdrożenie zasad zarządzania informacją i zarządzania ryzykiem, które pomogą ograniczyć dowolność i chaos w podejmowaniu decyzji. Zarządzanie informacją w kryzysie polega na szybkim zbieraniu, weryfikowaniu i rozpowszechnianiu istotnych danych o sytuacji. Konieczna jest dyscyplina informacyjna – ustanowienie jednoznacznych kanałów przepływu wiadomości i procedur raportowania (np. regularne meldunki sytuacyjne w określonych godzinach). Pozwala to uniknąć zarówno dezinformacji, jak i informacyjnej pustki, która rodzi plotki. W pierwszych chwilach kryzysu często panuje chaos informacyjny – spływają sprzeczne meldunki o liczbie ofiar, zasięgu zniszczeń itp. Zadaniem sztabu kryzysowego jest szybkie rozpoznanie sytuacji i prognozowanie jej rozwoju na podstawie dostępnych danych. Stosuje się przy tym narzędzia takie jak mapy sytuacyjne, wizualizacje danych (np. zaznaczanie na mapie obszaru zalanego), a także techniki analizy ryzyka. Zarządzanie ryzykiem w fazie reagowania polega na ciągłej ocenie, jakie zagrożenia wciąż występują i jakie działania przyniosą najlepszy skutek, minimalizując potencjalne straty²⁷⁵. Decydenci muszą

²⁷⁴ W. Otwinowski, *Podstawy zarządzania kryzysowego i systemu obronnego*, Poznań, Wydawnictwo Naukowe Wyższej Szkoły Handlu i Usług, 2015.

²⁷⁵ K. Chrużik, Zarządzanie ryzykiem w sytuacjach kryzysowych, *Journal of KONBiN*, 49(4), 2019, s. 261-273. <https://doi.org/10.2478/jok-2019-0085>

priorytetyzować zadania – np. ewakuować najpierw obszary najbardziej zagrożone życia lub zdrowia, nawet jeśli oznacza to pozostawienie mniej istotnych aktywów bez ochrony. W praktyce wykorzystuje się proste metody oceny ryzyka, jak matryce ryzyka (szacowanie prawdopodobieństwa i skutków danego zdarzenia) czy scenariusze rozwoju sytuacji (optymistyczny, pesymistyczny). Na ich podstawie zespół kryzysowy opracowuje warianty działań i przedstawia kierującemu rekomendacje. Niezbędne jest też przygotowanie planów awaryjnych na wypadek, gdy sytuacja rozwinie się inaczej niż zakładano. Na przykład, jeśli istnieje ryzyko przerwania wału przeciwpowodziowego, już zawczasu planuje się trasy ewakuacji i rozmieszczenie służb ratowniczych po ewentualnym zalaniu kolejnych terenów. Podejmowanie decyzji w warunkach stresu wymaga od liderów odporności psychicznej i pewnego przygotowania. Dlatego tak ważne są szkolenia i ćwiczenia symulacyjne, podczas których osoby odpowiedzialne za zarządzanie kryzysowe mogą przećwiczyć scenariusze podejmowania decyzji pod presją²⁷⁶. Treningi sztabowe odzwierciedlające warunki kryzysu – np. szybki napływ informacji, konieczność natychmiastowej reakcji na zmieniające się okoliczności – pomagają wypracować odpowiednie nawyki decyzyjne. Badania wskazują, że zespoły, które regularnie ćwiczą reagowanie, lepiej radzą sobie z presją czasu i niepewnością w realnym zdarzeniu²⁷⁷. Jedną z technik decyzyjnych stosowanych w takich sytuacjach jest model rozpoznania i reagowania (ang. recognition-primed decision model) Gary’ego Kleina – polega on na szybkim rozpoznaniu wzorców sytuacyjnych przez doświadczonego dowódcę i natychmiastowym wyborze możliwie najlepszego działania na podstawie intuicji opartej o doświadczenie, zamiast czasochłonnego porównywania wszystkich opcji²⁷⁸. Choć model ten nie zastąpi pełnej analizy, w kryzysie bywa praktyczny, gdyż czas na decyzję jest drastycznie skrócony. Niezależnie od techniki, każda decyzja podjęta w kryzysie wiąże się z ryzykiem. Ważne jest, by to ryzyko było świadomie akceptowane – dlatego dokumentuje się tok rozumowania, dowody, na których oparto decyzję,

²⁷⁶ M. Fenigstein, Doskonalenie procesu decyzyjnego w sytuacjach kryzysowych poprzez gry decyzyjne, *Zeszyty Naukowe Akademii Obrony Narodowej*, 2(119), 2020, s. 45-59.

²⁷⁷ E. B. Hsu, Community Empowerment Strategies for Disaster Resilience, *Journal of Homeland Security and Emergency Management*, 13(3), 2016, s. 347-367.

²⁷⁸ G. Klein, *Sources of Power: How People Make Decisions*, Cambridge, MA, MIT Press, 1998.

oraz założenia. Pozwala to później wyciągnąć wnioski (tzw. lessons learned) i ewentualnie rozliczyć błędy, ale też bronić poprawnych decyzji podjętych na podstawie informacji dostępnych w danym momencie. Otwartość na korygowanie decyzji również jest istotna – gdy pojawiają się nowe informacje, sztab musi być gotów zmienić wcześniejsze ustalenia (np. odwołać ewakuację, jeśli zagrożenie minęło, lub przeciwnie – rozszerzyć ją). Krótko mówiąc, efektywne reagowanie kryzysowe wymaga elastyczności decyzyjnej połączonej z dyscypliną wykonawczą: podejmowania szybkich decyzji, ale zarazem ścisłego kierowania się procedurami i planami, o ile pasują do sytuacji, lub ich modyfikacji w razie potrzeby.

Integralnym komponentem reagowania jest komunikacja kryzysowa skierowana do społeczeństwa. Choć może wydawać się ona „miękkim” aspektem w porównaniu z działaniami ratowniczymi, w rzeczywistości skuteczna komunikacja z ludnością bywa decydująca dla powodzenia całej akcji. Informowanie społeczeństwa o zagrożeniu, instrukcjach postępowania i podjętych działaniach pozwala zapobiec panice, zmobilizować do współpracy oraz utrzymać zaufanie obywateli do instytucji publicznych²⁷⁹. Jak wskazują eksperci Rządowego Centrum Bezpieczeństwa, w sytuacji kryzysowej tylko otwarta i uczciwa komunikacja ze społeczeństwem może zniwelować lub osłabić skutki kryzysu²⁸⁰. Natomiast brak komunikacji lub jej błędne prowadzenie grozi rozprzestrzenieniem się dezinformacji, pogłoskami i utratą wiarygodności władz. Dlatego każda instytucja zaangażowana w reagowanie kryzysowe powinna mieć przygotowany plan komunikacji – określający, kto i w jaki sposób przekazuje informacje opinii publicznej. Z reguły wyznacza się rzecznika prasowego lub głównego komunikatora kryzysowego, który regularnie informuje media o rozwoju wydarzeń (np. organizując briefingi prasowe o ustalonych porach). Dobra komunikacja kryzysowa charakteryzuje się kilkoma zasadami: szybkość, prawdziwość i empatia. Informacje powinny być przekazywane możliwie szybko po zaistnieniu zdarzenia – tak, aby ludność usłyszała oficjalny komunikat wcześniej niż plotki. Treść komunikatów musi być wiarygodna i oparta na faktach,

²⁷⁹ B. Reynolds, M. Seeger, Crisis and Emergency Risk Communication as an Integrative Model, *Journal of Health Communication*, 10(1), 2005, s. 43-55. <https://doi.org/10.1080/10810730590904571>

²⁸⁰ Rządowe Centrum Bezpieczeństwa, *Księga Komunikacji Kryzysowej* – 2017, RCB, Warszawa, 2017.

nawet jeśli są to złe wiadomości – ukrywanie prawdy niemal zawsze obraca się przeciw komunikatorom (zasada “mów wszystko, co możesz, ale nigdy nie kłam”). Ważny jest też ton komunikacji: powinien być opanowany, lecz współczujący – ludzie dotknięci kryzysem muszą czuć, że władze rozumieją ich cierpienie i robią wszystko, by pomóc. W praktyce często stosuje się podejście modelu CERC (Crisis and Emergency Risk Communication), który zaleca m.in. wyrażanie empatii, wyjaśnianie sytuacji, przedstawienie planu działań i wskazówek dla publiczności²⁸¹. W warunkach sytuacji kryzysowej kluczowe znaczenie ma koordynacja przekazu informacyjnego, tak, aby wszystkie podmioty zaangażowane w reagowanie przekazywały spójne, jednolite komunikaty. Informacje sprzeczne, nieaktualne lub dublujące się prowadzą do dezorientacji odbiorców i obniżają skuteczność oddziaływań ochronnych. W tym celu ustanawiane jest centrum prasowe lub wspólna platforma informacyjna, w ramach której uzgadniana jest treść komunikatów kierowanych do ludności. W przypadku zdarzeń o większej skali Rządowe Centrum Bezpieczeństwa uruchamia portal informacyjny kryzys.gov.pl oraz wykorzystuje system Alert RCB do przekazywania ostrzeżeń i zaleceń w formie wiadomości SMS do osób przebywających na obszarze zagrożenia. Równolegle komunikaty dystrybuowane są za pośrednictwem mediów tradycyjnych (telewizja, radio) oraz kanałów cyfrowych, w tym mediów społecznościowych. Skuteczność komunikacji zwiększa wielokanałowa dystrybucja przekazu, uwzględniająca potrzeby odbiorców wymagających dostępności, w szczególności poprzez zapewnienie alternatywnych form komunikatu (np. tłumaczenia na polski język migowy) oraz wersji językowych dla cudzoziemców. Komunikacja kryzysowa stanowi element działań o znaczeniu porównywalnym z przedsięwzięciami operacyjnymi, ponieważ informowanie społeczeństwa o zagrożeniach, zalecanych zachowaniach oraz przebiegu działań wpływa na poziom odporności społecznej na kryzys. Odbiorcy dysponujący rzetelną informacją częściej podejmują zachowania zgodne z zaleceniami służb i organów administracji, w tym wykonują polecenia ewakuacji lub stosują środki samoochrony, co ogranicza ryzyko paniki i sprzyja racjonalnym reakcjom. W warunkach deficytu informacji oficjalnej

²⁸¹ B. Reynolds, M. Seeger, Crisis and Emergency Risk Communication as an Integrative Model, *Journal of Health Communication*, 10(1), 2005, s. 43-55. <https://doi.org/10.1080/10810730590904571>

wzrasta podatność na dezinformację, pogłoski i narracje spiskowe, co może prowadzić do zakłóceń porządku publicznego oraz obniżyć skuteczność działań ochronnych. Z tego względu w zarządzaniu kryzysowym komunikacja z ludnością traktowana jest jako komponent niezbędny na każdym etapie reagowania, a jej rzetelność, przejrzystość i terminowość pozostają czynnikami sprzyjającymi utrzymaniu zaufania społecznego i efektywności przedsięwzięć realizowanych w celu przezwyciężenia sytuacji kryzysowej²⁸². Po ustabilizowaniu sytuacji i zakończeniu działań ratunkowych system przechodzi do fazy odbudowy, w której priorytetem staje się przywrócenie usług i warunków życia oraz redukcja podatności na przyszłe zdarzenia.

3.4. Odbudowa i odtwarzanie po kryzysie

Odbudowa – zwana też fazą recovery – to końcowy etap zarządzania kryzysowego, obejmujący działania podejmowane po ustaniu fazy reagowania, w celu przywrócenia normalnego funkcjonowania społeczności dotkniętej kryzysem (katastrofą) do stanu sprzed zdarzenia lub nawet lepszego niż przed kryzysem. Innymi słowy, proces odbudowy trwa aż do momentu, gdy wszystkie kluczowe systemy i usługi zostaną odtworzone – albo do stanu poprzedniego, albo do stanu bardziej odpornego na przyszłe zagrożenia. W praktyce wyróżnia się odbudowę krótkoterminową oraz długoterminową²⁸³. Pierwsza koncentruje się na pilnych działaniach zabezpieczających i przywróceniu podstawowych usług do minimalnych standardów operacyjnych, tworząc warunki do dalszej odbudowy. Druga obejmuje wieloletnie, kompleksowe odtwarzanie całego dotkniętego obszaru, wraz z wzmocnieniem odbudowanych systemów, tak, aby społeczność stała się mniej wrażliwa na kolejne kryzysy. Proces ten jest złożony, długotrwały i wymaga skoordynowanego wysiłku wszystkich sektorów – od infrastruktury fizycznej, przez gospodarkę, po sferę społeczną i psychospołeczną. Co istotne, fazy odbudowy nakładają się czasowo z fazą reagowania oraz między sobą – działania naprawcze podejmowane są już w trakcie akcji ratunkowej, a odbudowa

²⁸² Rządowe Centrum Bezpieczeństwa, Księga Komunikacji Kryzysowej – 2017, Warszawa, RCB, 2017.

²⁸³ A. Leszczyńska, Wybrane uwarunkowania odbudowy organizacji po wystąpieniu klęsk, Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie, 2018, s. 273-285.

krótkoterminowa płynnie przechodzi w działania długofalowe. Ciągłość odbudowy – fazy i harmonogram przedstawione zostały na rysunku 12.



Rysunek 12. Schemat ciągłości procesu odbudowy po katastrofie – zakres zadań i nakładanie się faz krótkoterminowej, pośredniej i długoterminowej

Źródło: opracowanie własne na podstawie: Federal Emergency Management Agency, National Disaster Recovery Framework, 2011, <https://www.fema.gov/pdf/recoveryframework/ndrf.pdf#page=1&zoom=auto,-263,552>, [dostęp: 22.09.2025].

W ostatnich dekadach znaczenie skutecznej odbudowy po kryzysach wzrasta ze względu na rosnącą częstotliwość i skalę klęsk dotykających społeczności na całym świecie. Dla zobrazowania: w roku 2020 zanotowano globalnie 389 poważnych klęsk naturalnych, które spowodowały śmierć ponad 15 tys. osób, dotknęły niemal 100 mln ludzi i przyniosły straty ekonomiczne szacowane na 171 mld USD²⁸⁴. Wiele współczesnych katastrof osiąga rozmiary katastrof kompleksowych lub katastrof o charakterze chronicznym, których skutki humanitarne i ekonomiczne utrzymują się latami. Dlatego proces odbudowy nie sprowadza się jedynie do doraźnej naprawy szkód – jest to wieloletni wysiłek rozwojowy, warunkujący powrót społeczności do normalności oraz jej przyszłą odporność. Szacuje się, że dla wielu społeczności dotkniętych poważną katastrofą powrót do względnej normalności zajmuje od 5 do 7 lat, choć w przypadku najcięższych kryzysów odbudowa może trwać nawet dekadę lub dłużej. Poniżej omówiono kluczowe aspekty krótkoterminowej i długoterminowej odbudowy po kryzysie, a także

²⁸⁴ Centre for Research on the Epidemiology of Disasters (CRED), Cred Crunch, Issue no. 62: Disaster Year in Review 2020, Brussels, EM-DAT/CRED – UCLouvain, 2021.

konceptję „build back better” i budowania odporności, jako nowoczesnego podejścia do procesu recovery.

Odbudowa krótkoterminowa rozpoczyna się bezpośrednio po opanowaniu najpilniejszych działań ratunkowych. Jej horyzont czasowy to zwykle pierwsze dni, tygodnie i miesiące po zdarzeniu kryzysowym. Głównym celem jest jak najszybsze przywrócenie funkcjonowania podstawowych usług i infrastruktury krytycznej, niezbędnych do zabezpieczenia życia i zdrowia ludności²⁸⁵. Mowa tu o osiągnięciu minimalnych standardów operacyjnych sieci zaopatrzenia w wodę pitną, energię elektryczną, gaz i paliwo, o odtworzeniu łączności telekomunikacyjnej oraz podstawowej przepustowości sieci transportowych. Równolegle zapewnione musi być funkcjonowanie służb medycznych (uruchomienie szpitali polowych, zabezpieczenie dostaw leków) oraz porządku publicznego (działanie policji, straży itp.) – tak, aby chronić ocalałą ludność przed dalszymi zagrożeniami. Integralną częścią krótkoterminowej odbudowy jest pomoc humanitarna i wsparcie społeczne dla poszkodowanych. Obejmuje to dystrybucję żywności, wody, odzieży i innych artykułów pierwszej potrzeby, zapewnienie tymczasowego schronienia dla osób, które utraciły domy (np. w postaci namiotów, kontenerów mieszkalnych lub zakwaterowania w szkołach, halach sportowych) oraz organizację punktów wydawania pomocy. Ważnym elementem jest też opieka nad grupami wrażliwymi – dziećmi, seniorami, osobami chorymi i niepełnosprawnymi – poprzez tworzenie bezpiecznych przestrzeni (np. tymczasowe szkoły, świetlice) i skierowanie do nich odpowiednich służb (opieka medyczna, psychologiczna, wyżywienie). Zapewnienie wsparcia psychospołecznego rozpoczyna się już na tym etapie – przykładowo poprzez psychologiczną pomoc pierwszej potrzeby (tzw. psychological first aid) dla ofiar w szoku, organizowanie grup wsparcia czy udzielanie informacji o zaginionych bliskich (co pomaga w łączeniu rodzin). Jak podkreślają badacze, wczesna interwencja psychospołeczna po katastrofie – choć skupiona głównie na zabezpieczeniu podstawowych potrzeb – może zmniejszyć długofalowe negatywne skutki psychiczne i ułatwić proces zdrowienia społeczności²⁸⁶.

²⁸⁵ A. Leszczyńska, Wybrane uwarunkowania odbudowy organizacji po wystąpieniu klęsk, *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, 2018, s. 273-285.

²⁸⁶ M. F. Mooney, D. Paton, I. de Terte, S. Johal, A. N. Karanci, Psychosocial Recovery from Disasters: a Framework Informed by Evidence, *New Zealand Journal of Psychology*, 40(4), 2011, s. 26-38.

Na etapie krótkoterminowej odbudowy kluczowe jest także uprzątnięcie zniszczeń i zabezpieczenie terenu. Usuwanie gruzu, powalonych drzew i wraków z dróg umożliwia przywrócenie przejezdności oraz dostęp ekip naprawczych do uszkodzonych obiektów. Często tworzone są tymczasowe rozwiązania infrastrukturalne, np. zastępcze mosty pontonowe, generatory prądu, mobilne stacje uzdatniania wody czy szpitale polowe, aby chociaż częściowo wznowić działanie kluczowych systemów. Prowizoryczne naprawy (tzw. quick fixes) – takie jak łatanie uszkodzonych dachów plandekami, zabezpieczanie pękniętych okien, wzmacnianie naruszonych konstrukcji podporami – zapobiegają dalszym zniszczeniom mienia i umożliwiają wykorzystanie budynków w ograniczonym zakresie. Bardzo ważne jest równoczesne prowadzenie oceny szkód i potrzeb, która posłuży do zaplanowania kolejnych faz odbudowy. Już w pierwszych dniach kryzysu specjaliści dokonują wstępnej oceny strat: liczby zniszczonych domów, infrastruktury, szacunkowych kosztów oraz oceny liczby osób wymagających długoterminowej pomocy. Te informacje stanowią bazę do opracowania planu odbudowy długofalowej. Odbudowa krótkoterminowa bywa określana mianem fazy stabilizacji lub odbudowy pomostowej, ponieważ łączy etap reagowania z fazą rekonstrukcji długoterminowej. W praktyce wiele działań humanitarnych i ratunkowych płynnie przechodzi w działania naprawcze. Przykładowo, masowe schronienie tymczasowe najpierw ma charakter ratunkowy (chroni życie ofiar bez dachu nad głową), ale z czasem przekształca się w rozwiązanie tymczasowe na tygodnie czy miesiące, dopóki nie zostaną wybudowane domy stałe. Podobnie polowe systemy zaopatrzenia w wodę i energię działają do momentu odbudowania sieci komunalnych. Na tym etapie kładzie się również nacisk na koordynację pomocy – ważne jest utworzenie centrów zarządzania kryzysowego i punktów informacji dla ludności, aby przepływ informacji i zasobów był płynny²⁸⁷. Im sprawniej przebiegnie faza krótkoterminowa, tym lepsze fundamenty zostaną położone pod pomyslną odbudowę długoterminową.

Odbudowa długoterminowa obejmuje wszystkie przedsięwzięcia podejmowane w miesiącach i latach po katastrofie, zmierzające do pełnej

²⁸⁷ A. Leszczyńska, Wybrane uwarunkowania odbudowy organizacji po wystąpieniu klęsk, Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 2018, s. 273-285.

odbudowy zniszczeń oraz przywrócenia normalnych warunków życia i rozwoju w danej społeczności. Ten etap jest z reguły najbardziej czasochłonny i kosztochłonny, a jego realizacja może trwać wiele lat – w zależności od skali kryzysu nawet dekadę lub dłużej. Przykładowo, po trzęsieniu ziemi i tsunami w Japonii w 2011 r. (najkosztowniejszej katastrofie naturalnej w historii, z szacowanymi stratami rzędu 235 mld USD) pełna odbudowa infrastruktury i społeczności została rozłożona na co najmniej 5-10 lat. Z kolei po znacznie mniej zamożnym Haiti, gdzie w 2010 r. trzęsienie ziemi zniszczyło stołeczne miasto Port-au-Prince, nawet dekadę później dziesiątki tysięcy ludzi wciąż mieszkali w tymczasowych schronieniach, a wysiłki rekonstrukcyjne pozostawały niesfinalizowane. Długoterminową odbudowę cechuje zatem złożoność – obejmuje ona równoległe działania w sferze fizycznej (infrastrukturalnej), gospodarczej oraz społecznej. Poniżej omówiono trzy kluczowe wymiary odbudowy długofalowej.

Infrastruktura – rozumiana jako budynki, budowle i sieci techniczne – zwykle doznaje największych zniszczeń w wyniku katastrof i kryzysów. Jej odbudowa jest więc centralnym zadaniem fazy długoterminowej. Obejmuje to zarówno infrastrukturę publiczną (drogi, mosty, linie kolejowe, lotniska, sieci energetyczne, wodociągi, kanalizacja, szkoły, szpitale, urzędy), jak i prywatną (domy mieszkalne, budynki usługowe, zakłady przemysłowe, gospodarstwa rolne). Celem jest nie tylko naprawa uszkodzonych obiektów, ale często ich całkowita rekonstrukcja – w wielu przypadkach bardziej opłaca się zburzyć poważnie zniszczony budynek i wybudować go od nowa, niż łątać uszkodzenia. Proces odbudowy infrastruktury przebiega etapami. W pierwszej kolejności zapewnia się infrastrukturę zastępczą – np. stawia się tymczasowe mosty, jeśli stałe przeprawy runęły, czy buduje się osiedla tymczasowych domów modułowych dla mieszkańców pozbawionych lokum. Równoległe trwają prace planistyczne nad odbudową docelową: ocena stanu technicznego ocalałych konstrukcji, decyzje które obiekty i gdzie odbudować, przygotowanie planów urbanistycznych odbudowy zniszczonych dzielnic itp. Następnie następuje faza realizacji inwestycji – odbudowy lub remontu tysięcy jednostkowych obiektów. Wyzwania w odbudowie infrastruktury są ogromne. Przede wszystkim wymaga to ogromnych nakładów finansowych – często przewyższających możliwości lokalnych samorządów czy nawet budżetu państwa. Przykładowo, rząd japoński utworzył specjalną

Agencję Odbudowy i fundusz na odbudowę Tohoku po 2011 r., z budżetem sięgającym 25 bln jenów (ok. 250 mld USD) rozłożonym na 10 lat²⁸⁸. W krajach rozwijających się niezbędne jest zaangażowanie środków międzynarodowych (pomoc ONZ, Banku Światowego, międzynarodowe fundusze pomocowe) – np. po trzęsieniu ziemi na Haiti w 2010 r. większość inwestycji odbudowujących szkoły, szpitale i systemy wodne została sfinansowana ze źródeł zagranicznych²⁸⁹.

Kolejną kwestią jest czasochłonność: od przygotowania projektów budowlanych, poprzez procedury przetargowe, po samą budowę – odbudowa tysięcy domów czy setek kilometrów dróg nie może odbyć się natychmiast. Zwykle szczególnie długo trwa odtworzenie infrastruktury krytycznej o wysokim stopniu skomplikowania technologicznego, takiej jak systemy energetyczne (elektrownie, sieci przesyłowe) czy infrastruktura ochronna (np. wały przeciwpowodziowe, systemy melioracyjne). Dla przykładu, po huraganie Katrina (USA, 2005 r.) odbudowa przerwanych wałów przeciwpowodziowych oraz usprawnienie systemu pomp w Nowym Orleanie zajęła kilka lat i pochłonęła miliardy dolarów, ale była warunkiem bezpiecznego funkcjonowania miasta w przyszłości. Podobnie odbudowa budynków użyteczności publicznej (szkół, szpitali) często jest realizowana w dalszej kolejności – najpierw uruchamia się prowizoryczne obiekty (np. szkoły w barakach, szpitale polowe), a dopiero po zapewnieniu mieszkań ludności i podstawowej infrastruktury przystępuje do inwestycji w stałe gmachy.

Ważnym trendem we współczesnej odbudowie infrastruktury jest zasada, by „odbudowywać lepiej” (build back better), o czym szerzej mowa będzie w dalszej części rozdziału. W kontekście infrastruktury oznacza to, że rekonstrukcja nie powinna mechanicznie odtwarzać wcześniejszego stanu, ale raczej poprawiać charakterystyki obiektów i sieci pod kątem bezpieczeństwa i odporności. Przykładowo, przy odbudowie zniszczonych budynków wprowadza się ulepszone kodeksy budowlane – np. w obszarach sejsmicznych wymaga się stosowania projektów odporniejszych na trzęsienia ziemi

²⁸⁸ Reconstruction Agency, After the Great East Japan Earthquake (informacja o 10-letnim horyzoncie odbudowy i alokacji 25 bln JPY na okres intensywnej odbudowy), Reconstruction Agency, 2021.

²⁸⁹ The World Bank (Trustee), Haiti Reconstruction Fund Trust Fund Financial Summary as of December 31, 2018 (zestawienie finansowania projektów m.in. w sektorach Education oraz Water and Sanitation), The World Bank Group, 2018.

(wzmocnione zbrojenia, elastyczne fundamenty itp.), na terenach zalewowych – budowania budynków na podwyższeniach lub nasypach, a w strefach huraganowych – montażu okien i dachów odpornych na wiatr. Także odtwarzając sieci infrastruktury technicznej, często zmienia się ich przebieg lub parametry, by zmniejszyć ryzyko przyszłych awarii – np. linie energetyczne mogą zostać poprowadzone pod ziemią zamiast napowietrznie, by uchronić je przed zerwaniem przez wichury, a wały przeciwpowodziowe buduje się wyższe i z lepszych materiałów niż przed powodzią. Choć takie podejście podnosi koszty i wydłuża czas odbudowy, przynosi korzyść w postaci zwiększenia bezpieczeństwa na przyszłość.

Odbudowa gospodarcza to kolejny kluczowy wymiar recovery. Katastrofy mogą zadać lokalnej ekonomii potężny cios – zniszczeniu lub przerwaniu ulega działalność przedsiębiorstw, łańcuchy dostaw, rynki zbytu, spada zatrudnienie i dochody ludności, kurczy się baza podatkowa samorządów. Długoterminowe ożywienie gospodarki lokalnej wymaga więc szeregu interwencji mających przywrócić warunki do prowadzenia działalności gospodarczej i ponownego generowania miejsc pracy. Pierwszym krokiem jest często wsparcie dla przedsiębiorców, zwłaszcza drobnych firm (sklepy, warsztaty, usługi), które często najbardziej cierpią w wyniku klęski. Statystyki są alarmujące – szacuje się, że ok. 40% małych i średnich firm nie wznowia działalności po poważnej katastrofie, a wiele kolejnych upada w ciągu następnego roku. Główne przyczyny to straty finansowe, brak rezerw i ubezpieczeń, utrata majątku oraz przerwanie rynku zbytu. Dlatego w ramach odbudowy gospodarczej stosuje się instrumenty takie jak: preferencyjne pożyczki i granty na wznowienie działalności, ulgi podatkowe i dopłaty dla firm utrzymujących zatrudnienie, programy „cash-for-work” (płacenie lokalnym mieszkańcom za udział w pracach porządkowych i odbudowie, co jednocześnie napędza lokalną konsumpcję) oraz fundusze gwarancyjne zachęcające banki do kredytowania odbudowy biznesu. Często tworzone są specjalne strefy ekonomiczne lub targowiska tymczasowe, by umożliwić handel i świadczenie usług mimo zniszczeń infrastruktury handlowej. Ważną rolę odgrywają organizacje pozarządowe i agencje pomocowe, które szkolą przedsiębiorców, doradzają przy tworzeniu planów odbudowy biznesu i dostarczają mikrokredytów – przykładowo po katastrofach prowadzonych jest wiele programów mikrofinansowania pomagających rolnikom zakupić

nasiona i sprzęt, a drobnym handlarzom wznović zaopatrzenie. Na poziomie makro, reaktywacja lokalnej gospodarki wymaga inwestycji w odbudovę kluczowych sektorov. Jeśli region był rolniczy – konieczne jest wsparcie rolnikov (np. odbudova systemov irygacyjnych, dostarczenie inwentarza żywego w miejsce utraconego, odtworzenie zasiewov). Jeśli opierał się na turystyce – odbudova atrakcji turystycznych i bazy hotelowej staje się priorytetem, połączona z kampanią promocyjną po zakończeniu odbudovy, by na nowo przyciągnąć turystov. W regionach przemysłowych – wysiłki koncentrują się na reaktywacji zakładov przemysłowych, naprawie lub odbudowie fabryk, magazynov, oraz na przywróceniu funkcjonowania centrów logistycznych. Rząd centralny często stymuluje ożywienie dotkniętego regionu poprzez specjalne programy inwestycyjne – np. budovę nowych zakładov publicznych (typu warsztaty szkolne, drobne manufaktury) czy lokowanie w regionie nowych instytucji (np. jednostek wojskowych, uczelni), co tworzy miejsca pracy i popyt.

Niezwykle ważnym aspektem jest przywrócenie zaufania inwestorov i uczestnikov rynku do dotkniętej kryzysem społeczności. Jeżeli odbudova infrastruktury i porządku publicznego postępuje sprawnie, a władze lokalne prezentują jasny plan rozwoju po katastrofie, rośnie szansa, że prywatny kapitał nie wycofa się trwale z regionu. W przeciwnym razie może dojść do długotrwałej stagnacji – przedsiębiorcy przeniosą się gdzie indziej, ludność zdolna do pracy wyemigruje w poszukiwaniu dochodov, co tworzy sprzężenie zwrotne pogłębiające kryzys ekonomiczny. Dlatego odbudova gospodarcza często jest sprzężona z działaniami rewitalizacyjnymi – wykorzystuje się moment odbudovy, by dokonać pewnych przekształceń strukturalnych w gospodarce lokalnej. Na przykład, po katastrofie można zaplanować dywersyfikację gospodarki (aby nie opierała się na jednym podatnym na kryzys sektorze), przyciągnąć inwestorov z nowych branż poprzez ulgi i kampanie promocyjne, a także poprawić otoczenie biznesu (np. uprościć procedury administracyjne, unowocześnić infrastrukturę techniczną dla biznesu). Takie podejście wpisuje się w filozofię „lepszego odbudovy”, starając się wyeliminować nie tylko skutki, ale i przyczyny podatności lokalnej gospodarki na kryzysy. Długoterminowa odbudova gospodarcza zakłada zarówno przywrócenie, jak i przekroczenie poprzedniego poziomu aktywności ekonomicznej. Sukcesem będzie sytuacja, gdy po kilku latach region

nie tylko odrobi straty, ale również rozwinie nowe gałęzie działalności, zapewniając mieszkańcom trwałe dochody. Warunkiem jest jednak skoordynowane wsparcie finansowe, instytucjonalne i planistyczne – od poziomu lokalnego aż po centralny i międzynarodowy – by przezwyciężyć inicjalny impas ekonomiczny po katastrofie. Psychospołeczne aspekty odbudowy są często mniej namacalne niż infrastruktura czy ekonomia, ale nie mniej ważne dla pełnego wyjścia społeczności z kryzysu. Katastrofy powodują zbiorowe traumy, żalobę po ofiarach śmiertelnych, poczucie utraty bezpieczeństwa i przewidywalności życia, a także mogą prowadzić do rozpadu więzi społecznych (przynajmniej czasowo, wskutek przesiedleń i chaosu). Długoterminowe zdrowie psychiczne i odporność społeczna mieszkańców dotkniętych kryzysem stają się zatem kluczowym polem działań w procesie recovery. Pierwszym elementem jest zapewnienie długofalowego wsparcia psychologicznego i psychiatrycznego dla osób dotkniętych traumą. Badania epidemiologiczne pokazują, że po poważnych katastrofach znaczna część populacji cierpi na zaburzenia stresowe (w tym PTSD, zaburzenia lękowe, depresję) – według metaanaliz nawet 10-20% bezpośrednich ocalałych może doświadczać przedłużających się objawów stresu pourazowego. Dlatego w ramach odbudowy tworzy się programy wsparcia zdrowia psychicznego: poradnie i linie telefoniczne dla ofiar, terapie indywidualne i grupowe, szkolenia dla lokalnych lekarzy pierwszego kontaktu z zakresu rozpoznawania i leczenia zaburzeń potraumatycznych, a także kampanie edukacyjne destygmatyzujące korzystanie z pomocy psychologicznej. Szczególną troską otacza się dzieci i młodzież – dla nich przewiduje się obecność psychologów w szkołach, specjalne programy przywracania poczucia bezpieczeństwa (np. poprzez zabawę, rytuały szkolne, wsparcie rówieśnicze), a w razie potrzeby terapię traumy dostosowaną do wieku. Ważne jest również udzielenie pomocy personelowi ratownicznemu i opiekunom (np. strażakom, ratownikom, pielęgniarcom) – oni także często doświadczają wypalenia i stresu pourazowego po intensywnej akcji ratunkowej.

Drugim komponentem jest odbudowa kapitału społecznego i więzi społecznych. Paradoksalnie, doświadczenie katastrofy może zarówno rozbić więzi (poprzez migracje, konflikty o zasoby), jak i je wzmocnić, gdy ludzie jednoczą się we wzajemnej pomocy. Dlatego świadome działania ukierunkowane na integrację społeczności są istotne. Na etapie odbudowy

organizuje się różnego rodzaju spotkania społeczności, konsultacje publiczne na temat planów odbudowy (co daje mieszkańcom poczucie wpływu na przyszłość ich otoczenia), a także inicjatywy oddolne – od upamiętnienia ofiar (np. wspólne obchody rocznic katastrofy, budowa pomników pamięci), po wspólne projekty odbudowy (np. wolontariat przy odbudowie domów sąsiadów, organizowanie szkół i opieki dziecięcej przez społeczność). Jak wykazano w analizach przypadków, aktywny udział ocalałych w procesie odbudowy sprzyja ich zdrowieniu psychicznemu – daje poczucie sprawczości, sensu i kontroli nad sytuacją²⁹⁰. Władze lokalne i organizacje pomocowe starają się więc angażować społeczność w planowanie i realizację projektów – np. poprzez komitety odbudowy z udziałem mieszkańców, konsultacje społeczne nowych rozwiązań urbanistycznych, czy wspieranie lokalnych liderów (np. duchownych, nauczycieli) w roli przewodników społeczności w trudnym okresie.

Istotnym elementem jest również przywrócenie funkcjonowania instytucji życia społecznego – szkół, miejsc kultu religijnego, ośrodków kultury, organizacji społecznych. Zapewniają one ramy dla odbudowy rutyny i poczucia normalności. Szybkie otwarcie szkół (choćby w tymczasowych warunkach) daje dzieciom i młodzieży nie tylko możliwość kontynuacji edukacji, ale też strukturę dnia i wsparcie rówieśnicze oraz dorosłych, co łagodzi stres. Podobnie wznowienie praktyk religijnych i spotkań społecznych (np. lokalnych festynów) pomaga społeczności przepracować wspólnie żałobę i odbudować nadzieję.

W ujęciu psychospołecznym, pełna odbudowa po kryzysie oznacza, że społeczność nie tylko odbudowała domy i miejsca pracy, ale też odzyskała poczucie bezpieczeństwa, tożsamości i wspólnoty. Trudniej to zmierzyć, lecz kluczowe wskaźniki to np. powrót lub zatrzymanie odpływu ludności (czy mieszkańcy, którzy wyjechali po katastrofie, wracają i czy nowi chcą się osiedlać), poziom zaufania społecznego i zaangażowania obywatelskiego, oraz stabilizacja wskaźników zdrowia psychicznego na poziomie sprzed kryzysu. Badania wskazują, że społeczności o silniejszych więziach i bogatszym kapitale społecznym lepiej radzą sobie z długofalową odbudową

²⁹⁰ M. F. Mooney, D. Paton, I. de Terte, S. Johal, A. N. Karanci, Psychosocial Recovery from Disasters: A Framework Informed by Evidence, *New Zealand Journal of Psychology*, 40(4), 2011, s. 26-38.

– szybciej rozwiązują lokalne problemy i wspierają nawzajem swoich członków²⁹¹. Dlatego inwestycje w „społeczną infrastrukturę” – relacje, zaufanie, organizacje lokalne – są równie ważne jak te w infrastrukturę fizyczną.

W toku doświadczeń z wieloma katastrofami na świecie narodziła się idea, że odbudowa powinna być traktowana nie tylko jako okazja do odtworzenia stanu sprzed kryzysu, ale także jako szansa na wzmocnienie społeczności i zmniejszenie jej podatności na przyszłe zagrożenia. Koncepcja ta znana jest pod hasłem „Build Back Better” (BBB), co tłumaczy się dosłownie jako „odbudować lepiej”. Znalazła ona szerokie uznanie – została m.in. włączona jako jeden z czterech priorytetów w ramach międzynarodowej Ram Sendai na lata 2015-2030 (Priority 4: „Enhancing disaster preparedness for effective response and Build Back Better in recovery, rehabilitation and reconstruction”). Istotą podejścia BBB jest redukcja przyszłego ryzyka poprzez działania odbudowy. Według definicji Globalnej Fundacji na rzecz Redukcji Ryzyka i Odbudowy, Build Back Better to podejście do odbudowy po katastrofie, które zmniejsza wrażliwość społeczności na przyszłe zagrożenia oraz buduje odporność przez uwzględnienie i korektę słabych punktów fizycznych, społecznych, środowiskowych i ekonomicznych ujawnionych przez katastrofę. Innymi słowy, chodzi o to, by wykorzystać proces rekonstrukcji do zbudowania bezpieczniejszych i bardziej zrównoważonych społeczności niż te, które istniały przed kryzysem. Praktyczne zastosowanie BBB przejawia się na wielu polach. Po pierwsze – jak już wspomniano przy odbudowie infrastruktury – oznacza wdrożenie ulepszonych standardów i norm przy rekonstrukcji fizycznej. Wprowadzenie lub zaostrzenie kodeksów budowlanych podnoszących odporność na zagrożenia (trzęsienia ziemi, wiatr, powódź itp.) to typowy przykład. Kolejnym jest lepsze planowanie przestrzenne: np. nie należy odbudowywać osiedli na terenach, o których wiadomo, że są szczególnie narażone (strefy zalewowe rzek, linia brzegowa podatna na tsunami, obszary osuwiskowe). Zamiast tego można przeznaczyć te tereny na funkcje niezamieszkałe (parki, tereny zalewowe kontrolowane), a budownictwo przenieść na obszary bezpieczniejsze. Często po katastrofie następuje rewizja planów zagospodarowania – co bywa trudne społecznie

²⁹¹ D. P. Aldrich, *Building Resilience: Social Capital in Post-Disaster Recovery*, Chicago, University of Chicago Press, 2012. <https://doi.org/10.7208/chicago/9780226012896.001.0001>

(bo może wymagać przesiedleń), ale długofalowo zwiększa odporność. BBB dotyczy też odbudowy usług i systemów społecznych. Przykładowo, jeśli katastrofa obnażyła słabość systemu ochrony zdrowia (jak stało się to podczas pandemii czy podczas katastrof masowych z dużą liczbą rannych), to w fazie odbudowy inwestuje się w wzmocnienie systemu opieki zdrowotnej – np. budowę nowoczesnego szpitala zamiast dwóch starych zniszczonych, stworzenie zapasów sprzętu medycznego, szkolenia personelu w zarządzaniu sytuacjami kryzysowymi. Jeśli zawiodła komunikacja kryzysowa – odbudowa powinna objąć utworzenie bardziej niezawodnego systemu łączności (np. sieci satelitarnej na wypadek zniszczenia wież telekomunikacyjnych). Jeżeli zaś kryzys pokazał niedostatki w strukturze gospodarczej (np. region zbyt uzależniony od jednego przemysłu uległ załamaniu, gdy ten przemysł stanął) – plan odbudowy może zakładać dywersyfikację ekonomiczną i programy przebranżowienia pracowników, by w przyszłości uderzenie w jeden sektor nie pogrążyło całej lokalnej gospodarki. Koncept „build back better” ściśle wiąże się z ideą odporności (resilience). Odporność społeczności można zdefiniować jako zdolność do przewidywania zagrożeń, przygotowania się na nie, zaabsorbowania uderzenia, a następnie szybkiego odbudowania się i adaptacji po zdarzeniu kryzysowym. Odbudowa prowadzona według zasad BBB zwiększa odporność, bo sprawia, że skutki następnej potencjalnej katastrofy będą mniejsze, a zdolność reagowania – większa. Przykładowo, odbudowanie sieci energetycznej w wersji rozproszonej (mikrosieci ze źródłami odnawialnymi w każdej dzielnicy) zamiast scentralizowanej sprawi, że awaria lub zniszczenie części sieci nie pozbawi zasilania całego regionu – to czyni społeczność bardziej odporną. Podobnie przeszkolenie mieszkańców w pierwszej pomocy czy wyznaczenie lokalnych liderów kryzysowych (np. w każdej wsi) zwiększa kapitał odpornościowy – w razie kolejnego kryzysu reakcja będzie szybsza i bardziej zorganizowana. Włączenie zasady BBB do planowania odbudowy wymaga świadomego podejścia ze strony władz i społeczności. Istnieją już opracowane wytyczne i ramy ułatwiające to zadanie – np. narodowe ramy odbudowy po katastrofie (Disaster Recovery Frameworks), które rządy mogą stworzyć jeszcze przed wystąpieniem kryzysu. Taki dokument określa role i odpowiedzialności instytucji w procesie recovery, priorytety odbudowy i właśnie elementy budowania odporności. W fazie planowania odbudowy po konkretnym zdarzeniu

kluczowe jest, aby w proces zaangażować ekspertów od redukcji ryzyka oraz samą społeczność – tak by identyfikować, co można zrobić lepiej niż było. Dzięki temu odbudowa nie ograniczy się do odbicia lustrzanego strat, ale stanie się procesem rozwojowym. Skala i złożoność procesów odbudowy sprawia, że powodzenie zależy w dużej mierze od zapewnienia odpowiednich instrumentów finansowych oraz rozwiązań prawno-instytucjonalnych. Nawet najlepiej zaplanowana odbudowa nie dojdzie do skutku bez funduszy – a te muszą pochodzić z różnych źródeł: budżetów publicznych, mechanizmów ubezpieczeniowych, pomocy międzynarodowej oraz wkładu sektora prywatnego. Rządy dotkniętych krajów często tworzą specjalne fundusze odbudowy, sięgają po nadzwyczajne alokacje budżetowe, emitują obligacje (np. tzw. obligacje odbudowy), czy też korzystają ze wsparcia międzynarodowego (kredyty i granty Banku Światowego, fundusze ONZ, pomoc dwustronna od innych państw). Na szczeblu międzynarodowym istnieją też mechanizmy finansowe uruchamiane w razie katastrof – przykładowo Fundusz Solidarności UE pomagający państwom unijnym w odbudowie po klęskach żywiołowych, czy globalne fundusze celowe na duże kryzysy humanitarne. Innym źródłem są wypłaty ubezpieczeń – odszkodowania z polis mienia, upraw czy zdrowia, które zasilają prywatne budżety odbudowy poszkodowanych (w krajach o wysokiej penetracji ubezpieczeniowej może to być znaczący zastrzyk środków). Niestety, tam gdzie społeczeństwo było słabo ubezpieczone, luki finansowe są największe – jak wskazuje UNDRR, niedostateczne ubezpieczenie i brak dostępu do finansowania należą do głównych przyczyn, dla których wiele firm (i rodzin) nie podnosi się po katastrofach. Dlatego częścią budowania odporności (jeszcze przed kryzysem) jest rozwój systemów ubezpieczeń i rezerw finansowych. W trakcie odbudowy natomiast, władze często wprowadzają pakiety pomocowe – np. dopłaty do odbudowy domów dla mieszkańców (pokrywające różnicę między kosztem odbudowy a odszkodowaniem), bezzwrotne zasiłki celowe dla poszkodowanych rodzin, czy preferencyjne kredyty dla samorządów na odbudowę infrastruktury. Równie istotne są ramy prawne i instytucjonalne zarządzania odbudową. W sytuacjach kryzysowych często stosuje się specjalne rozwiązania prawne, które upraszczają i przyspieszają procedury inwestycyjne oraz administracyjne. Przykładowo, po dużym trzęsieniu ziemi rząd może wprowadzić tzw. „specustawę” odbudowową, znoszącą na pewien czas niektóre

wymogi (jak długotrwałe procedury uzyskiwania pozwoleń na budowę, ocen oddziaływania na środowisko itp.) – tak, aby rekonstrukcja kluczowych obiektów mogła ruszyć bez zbędnej zwłoki. Ważne jest jednak zachowanie równowagi: uproszczenia prawne nie mogą np. prowadzić do obniżenia standardów bezpieczeństwa (np. nie można znosić wymogów sejsmicznych w budownictwie „dla szybkości”). Często powoływane są też specjalne jednostki organizacyjne do koordynacji odbudowy – np. rządowe pełnomocnictwo lub agencja ds. odbudowy, która skupia kompetencje rozproszone normalnie między różne resorty (budownictwa, finansów, spraw wewnętrznych itd.). Taka instytucja może nadawać spójny kierunek działaniom wielu aktorów, monitorować postępy i rozliczać wykorzystanie funduszy. Na poziomie lokalnym, samorządy często tworzą lokalne komitety odbudowy z udziałem władz, ekspertów i przedstawicieli społeczności, aby zapewnić partycypację i koordynację projektów na miejscu. Międzynarodowe wytyczne (np. ONZ) zalecają, by kraje jeszcze przed wystąpieniem katastrofy opracowały narodowe plany lub ramy odbudowy – analogicznie jak plany reagowania – tak, aby w momencie kryzysu móc szybciej uruchomić odpowiednie mechanizmy. Ramy te określają źródła finansowania awaryjnego, role instytucji rządowych i samorządowych, procedury współpracy z organizacjami międzynarodowymi oraz priorytety strategiczne (np. że odbudowa ma być prowadzona zgodnie z zasadą BBB). W Polsce kwestie zarządzania kryzysowego – w tym etap odbudowy – reguluje m.in. Ustawa o zarządzaniu kryzysowym oraz Ustawa o stanie klęski żywiołowej. Choć ustawy te koncentrują się głównie na fazie reagowania, przewidują także mechanizmy pomocy i odbudowy (np. zasiłki dla poszkodowanych, możliwość wprowadzenia uproszczeń administracyjnych w stanie klęski). Dodatkowo, po każdej większej katastrofie rząd zwykle przyjmuje specjalne programy odbudowy – np. po powodzi w 2010 r. w Polsce uruchomiono program odbudowy infrastruktury komunalnej finansowany z budżetu państwa i funduszy UE.

Odbudowa i odtwarzanie po kryzysie to proces wielowymiarowy, obejmujący szybkie działania ratunkowo-naprawcze, długofalową rekonstrukcję materialną i gospodarczą oraz uzdrawianie tkanki społecznej. Jego powodzenie wymaga nie tylko technicznej realizacji inwestycji, ale też umiejętnego zarządzania zasobami finansowymi, wsparcia prawnoinstytucjonalnego i włączania społeczności w proces decyzyjny. Coraz częściej

kładzie się nacisk, aby odbudowa była mądrzejsza i bardziej odporna – tak by z każdego kryzysu wyciągać wnioski, przekuwając tragedię w impuls do zbudowania bezpieczniejszych warunków życia na przyszłość. Tylko w ten sposób społeczności mogą przerwać cykl niszczycielskich strat i wejść na ścieżkę zrównoważonego rozwoju pomimo doświadczonych kryzysów. Odbudowa ujawnia mocne i słabe strony systemu, dlatego jej integralnym elementem powinno być zebranie doświadczeń i ich implementacja w procedurach, planach i szkoleniach – co stanowi przedmiot kolejnego podrozdziału.

3.5. Doskonalenie systemu i zarządzanie wiedzą po zdarzeniu

Po zakończeniu działań ratowniczych i opanowaniu sytuacji kryzysowej kluczowe jest wyciągnięcie wniosków z przebiegu zdarzenia oraz wprowadzenie ulepszeń do systemu zarządzania kryzysowego. Etap ten obejmuje po pierwsze analizę po zdarzeniu, odpowiednie gromadzenie i udostępnianie wiedzy o przebiegu i skutkach sytuacji, a następnie wdrożenie wniosków do praktyki poprzez aktualizację planów, zmiany organizacyjne czy nawet inicjowanie zmian prawnych. Taki proces zapewnia ciągle doskonalenie systemu i tworzy pętlę uczenia się. Główne elementy tego etapu to analiza po zdarzeniu: wyciąganie wniosków (lessons learned) i After Action Review. Analiza po zdarzeniu polega na systematycznym zebraniu informacji o przebiegu sytuacji kryzysowej oraz działaniach podjętych w trakcie reagowania, a następnie na ocenie, co zadziałało skutecznie, a co wymaga poprawy. Często stosowaną metodą jest After Action Review (AAR) – ustrukturyzowany proces debriefingu uczestników akcji ratunkowej, wywodzący się z praktyk wojskowych, obecnie powszechnie używany także w zarządzaniu kryzysowym. Podczas sesji AAR wszystkie zaangażowane służby i podmioty omawiają kolejno: co miało miejsce (faktyczny przebieg wydarzeń), co planowano (założenia planu reagowania), co się udało, a co nie (ocena działań), oraz czego się nauczyliśmy – czyli jakie wnioski i rekomendacje na przyszłość wynikają z porównania planów z rzeczywistością. Tego rodzaju pouczające podsumowanie pozwala zespołom ratowniczym szczerze przeanalizować błędy i dobre praktyki w atmosferze pozbawionej

wzajemnego obwiniania. Rezultatem AAR jest zazwyczaj lista konkretnych wniosków (tzw. *lessons identified*), które po zatwierdzeniu stają się *lessons learned* – oficjalnie przyjętymi doświadczeniami do wykorzystania. W polskiej praktyce zarządzania kryzysowego analiza po zdarzeniu również stanowi standardowy element zakończenia działań. Przykładowo, w Państwowej Straży Pożarnej ostatnim etapem każdej akcji ratowniczej jest sporządzenie dokumentacji i ocena przebiegu akcji, czyli właśnie omówienie po działaniu. Na podstawie tej analizy formułowane są rekomendacje mające poprawić skuteczność przyszłych działań ratowniczych – np. ulepszenia procedur taktycznych, dodatkowe szkolenia czy doposażenie jednostek. Raporty z akcji zawierające opis zdarzenia, podjęte działania i wnioski trafiają następnie do przełożonych oraz do baz wiedzy danej służby. Oprócz wewnętrznych analiz typu AAR przeprowadzanych przez same zespoły reagowania, istotną rolę odgrywają raporty pokontrolne przygotowywane przez organy nadzorujące i audytujące działanie systemu. Takie raporty – sporządzane np. przez Najwyższą Izbę Kontroli (NIK) lub specjalne komisje powołane po katastrofach – zawierają niezależną ocenę przebiegu zdarzenia i działań administracji wraz z zaleceniami naprawczymi. Raporty pokontrolne formułują oficjalne wnioski i zalecenia usunięcia stwierdzonych nieprawidłowości, często z wyznaczonym terminem ich realizacji. Przykładowo, po tragicznej w skutkach nawałnicy z sierpnia 2017 r. NIK w swoim raporcie wskazała szereg zaniedbań na różnych szczeblach administracji, konkludując, że “w Polsce nie funkcjonuje skuteczny system ochrony ludności”²⁹². Wśród rekomendacji pokontrolnych znalazły się m.in. postulaty pilnego stworzenia spójnego systemu obrony cywilnej oraz usprawnienia procedur ostrzegania ludności. Tak zdecydowane wnioski stały się impulsem do przygotowania nowych rozwiązań systemowych – kilka lat później opracowano projekt ustawy o ochronie ludności i obronie cywilnej, uwzględniający zalecenia pokontrolne NIK. Aby pojedyncze *lessons learned* nie pozostały tylko na papierze, konieczne jest stworzenie mechanizmów gromadzenia i udostępniania wiedzy o przebytych sytuacjach kryzysowych. W praktyce oznacza to prowadzenie baz danych, raportów i studiów przypadku dostępnych dla podmiotów systemu

²⁹² Najwyższa Izba Kontroli, Informacja o wynikach kontroli: Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, Nr P/17/039, Warszawa, NIK, 2019.

zarządzania kryzysowego, tak by mogły one czerpać z doświadczeń swoich oraz innych jednostek. Ważnym narzędziem są bazy case studies opisujące przebieg rozmaitych incydentów, ich przyczyny i konsekwencje, a przede wszystkim – zawierające lessons learned, czyli wnioski i rekomendacje dla przyszłości. Tego typu wiedza gromadzona jest zarówno na poziomie krajowym, jak i międzynarodowym. Na szczęblu Unii Europejskiej funkcjonuje np. baza poważnych awarii przemysłowych eMARS, w której gromadzi się opisy i ustalenia ze zdarzeń obejmujących zagrożenia chemiczne. Z bazy tej korzysta Wspólne Centrum Badawcze (JRC) przy tworzeniu specjalnych biuletynów Lessons Learned. Przykładowo, Biuro ds. Zagrożeń Poważnymi Awariami (MAHB) przeanalizowało 85 awarii w sektorze gospodarowania odpadami niebezpiecznymi z lat 1989-2022, identyfikując najczęstsze błędy i środki zaradcze. Wyniki tej analizy udostępniono w formie raportu zawierającego 6 studiów przypadków wraz z omówieniem „nauki płynącej z ich wystąpienia” – czyli konkretnych lekcji dla operatorów i służb. Takie publikacje (Lessons Learned Bulletin) pełnią funkcję praktycznych poradników: wskazują, jakie działania prewencyjne wdrożyć, by uniknąć powtórzenia podobnych zdarzeń, oraz jakie procedury reagowania warto usprawnić. Również inne kraje tworzą własne repozytoria wiedzy – np. we Francji działa baza ARIA dokumentująca przypadki awarii przemysłowych, a NATO dysponuje systemem wymiany doświadczeń z ćwiczeń i misji (tzw. NATO Lessons Learned Database). Na poziomie krajowym instytucje odpowiedzialne za bezpieczeństwo również starają się systematyzować wiedzę z incydentów. Rządowe Centrum Bezpieczeństwa (RCB) publikuje okresowe Raporty o zagrożeniach bezpieczeństwa oraz prowadzi analizy poważnych zdarzeń, których konkluzje następnie przekłada na zalecenia dla administracji. Ponadto, wyniki audytów (np. wspomniane raporty NIK) są upubliczniane – dzięki czemu zarówno jednostki samorządowe, jak i służby ratownicze mogą zapoznać się z rekomendacjami i dobrymi praktykami czy też z błędami do niepowtarzania. Wiedza ta bywa rozpowszechniana poprzez wytyczne i instrukcje wydawane przez organy centralne. Przykładowo, po doświadczeniach pandemii COVID-19 Ministerstwo Zdrowia i Rządowe Centrum Bezpieczeństwa opracowały zaktualizowane wytyczne dotyczące postępowania w sytuacji epidemii, uwzględniające wnioski z lat 2020-2021 (MZ, RCB 2021). Z kolei Komenda Główna PSP cyklicznie wydaje opracowania

analityczne po dużych akcjach (np. po pożarach kompleksów leśnych czy skutkach silnych wichur), zawierające zalecenia taktyczne dla jednostek terenowych. Dzięki temu wiedza o rzadkich, lecz istotnych zdarzeniach nie pozostaje rozproszona – jest dokumentowana i przekazywana w formie zaleceń, standardów postępowania czy materiałów szkoleniowych.

Warto podkreślić, że kultura dzielenia się wiedzą jest niezbędna do doskonalenia całego systemu. Organizacje zaangażowane w reagowanie kryzysowe muszą mieć zapewnione platformy wymiany informacji o wnioskach z przeprowadzonych działań²⁹³. Istotne jest również uczenie się od innych – zarówno na poziomie międzynarodowym, jak i między poszczególnymi regionami kraju. Jak zauważa Zakrzewska²⁹⁴, ważnym źródłem doskonalenia systemu zarządzania kryzysowego jest korzystanie z doświadczeń państw, które już takie systemy zbudowały i używają – stąd analiza zagranicznych best practices może wskazać kierunki usprawnień. Przykładowo, Niemcy po powodzi z 2002 r. i wcześniejszych atakach terrorystycznych z 2001 r. opracowały Nową strategię ochrony ludności, integrującą istniejące podsystemy i kładącą nacisk na lepszą koordynację służb²⁹⁵. Polska również korzysta z międzynarodowych inicjatyw wiedzy – jest członkiem platform wymiany doświadczeń w ramach UE (np. w sieci centrów kryzysowych) oraz uczestniczy w projektach badawczych dotyczących doskonalenia reagowania. Wszystkie te działania służą temu, by cenne doświadczenia nie zostały zapomniane, lecz przekute w konkretne wskazówki i standardy na przyszłość. Sama identyfikacja wniosków to dopiero początek – kluczowym etapem jest wcielenie ich w życie. Efekty procesu lessons learned powinny znaleźć odzwierciedlenie w aktualizacji planów zarządzania kryzysowego, w modyfikacji procedur i struktury organizacyjnej, a niekiedy wręcz w zmianach legislacyjnych. Bez tego pętla uczenia się nie domknie, a te same błędy mogą powtarzać się w kolejnych sytuacjach. Niestety, badania wskazują, że często istnieje luka między sformułowaniem wniosków a ich implementacją – brak skutecznego mechanizmu wdrażania powoduje, że organizacje nie

²⁹³ K. Sienkiewicz-Małyjurek, *Skuteczne zarządzanie kryzysowe*, Warszawa, Difin, 2015.

²⁹⁴ S. Zakrzewska, Kierunki doskonalenia systemu zarządzania kryzysowego w kontekście ochrony ludności i ratownictwa, *Doctrina. Studia Społeczno-Polityczne*, 18, 2021, s. 225-239. <https://doi.org/10.34739/doc.2021.18.14>

²⁹⁵ B. Kaczmarczyk, B. (red.), *Zarządzanie kryzysowe w Polsce i w państwach sąsiednich*, Wrocław, Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki, 2017.

uczają się dostatecznie na błędach²⁹⁶. Dlatego też nowoczesne podejście do zarządzania kryzysowego kładzie nacisk na ustanowienie formalnych procedur włączania wniosków do systemu.

Kolejny etap po zakończeniu działań ratowniczych i opanowaniu sytuacji kryzysowej to aktualizacja planów i procedur. Plany zarządzania kryzysowego na wszystkich szczeblach administracji powinny być dokumentami żywymi, okresowo przeglądаныmi i korygowanymi w oparciu o najnowsze doświadczenia. Polskie przepisy zobowiązują do aktualizacji planów co najmniej raz na 2 lata, a także po każdym większym zdarzeniu, jeśli ujawniło ono potrzebę korekt lub uzupełnień. Przykładem może być Krajowy Plan Zarządzania Kryzysowego (KPZK), który po katastrofalnej w skutkach powodzi na Odrze w 2022 r. został znowelizowany o nowe zagrożenie „zanieczyszczenie wód” – wcześniej nieuwzględnione w dokumentach planistycznych. W procesie najnowszej aktualizacji KPZK (2024) uwzględniono także listę wniosków z Raportu o zagrożeniach Bezpieczeństwa Narodowego przyjętego przez rząd – m.in. rekomendacje dotyczące skutków zmian klimatu. Na tej podstawie dodano do planu nowe scenariusze oraz doprecyzowano zadania poszczególnych instytucji na wypadek zagrożeń, które wcześniej były pomijane. Podobnie dzieje się na poziomie lokalnym: powiatowe i gminne plany zarządzania kryzysowego są korygowane po realnych zdarzeniach oraz ćwiczeniach – na przykład, jeśli w trakcie powodzi okaże się, że brakuje procedury ewakuacji określonego typu obiektu, plan zostaje uzupełniony o taki aneks na przyszłość.

Następny etap po działaniach ratowniczych i opanowaniu sytuacji kryzysowych to wprowadzenie zmian organizacyjnych i szkoleniowych. Wnioski z analiz po zdarzeniu mogą wskazywać na potrzebę zmian w strukturze organizacyjnej systemu lub sposobie działania służb. Często rekomenduje się ulepszenie koordynacji między podmiotami – np. stworzenie stałych zespołów koordynujących określone zagrożenia, lepsze powiązanie centrów zarządzania kryzysowego różnych resortów, czy ustanowienie punktów kontaktowych. Po poważnych kryzysach dokonuje się przeglądu obsad personalnych i kompetencji: bywa, że powoływane są nowe komórki organizacyjne

²⁹⁶ A. Rostis, Make no Mistake: The Effectiveness of the Lessons-Learned Approach to Emergency Management in Canada, *International Journal of Emergency Management*, 4(2), 2007, s. 250-259. <https://doi.org/10.1504/IJEM.2007.013990>

(np. centra operacyjne, zespoły analiz), lub redefiniowane są zakresy odpowiedzialności istniejących jednostek. Przykładowo, po fali cyberataków włączono ekspertów od bezpieczeństwa teleinformatycznego do sztabów kryzysowych, a po nawałnicy 2017 r. zarekomendowano włączenie Prezesa Urzędu Transportu Kolejowego w skład zespołu zarządzania kryzysowego na kolei. Istotnym elementem jest także doskonalenie kadr – lessons learned często prowadzą do modyfikacji programów szkoleniowych i ćwiczeń. Jeśli analiza ujawniła braki w wyszkoleniu (np. problemy z łącznością radiową między służbami), organizuje się dodatkowe treningi i doposaża systemy komunikacji. Po wystąpieniu nowych typów zagrożeń (np. epidemii) wprowadza się tematy tych zagrożeń do regularnych ćwiczeń, aby przygotować personel na podobne sytuacje. Krótko mówiąc, organizacja uczy się i adaptuje, wzmacniając swoje słabe punkty ujawnione podczas kryzysu.

Następnie należy wprowadzić zmiany prawne. Najpoważniejsze kryzysy często obnażają luki prawne lub niespójności w systemie, co może skutkować inicjatywą ustawodawczą. Wnioski sformułowane w raportach pokryzysowych nierzadko trafiają do agendy rządu i parlamentu. Jak wspomniano, NIK już w 2019 r. alarmowała o braku skutecznego systemu ochrony ludności – w odpowiedzi na te zarzuty podejmowano kolejne próby legislacyjne (projekty ustaw w 2019 i 2022 r.), aby w końcu doprowadzić do uchwalenia nowej ustawy o ochronie ludności (wejście w życie przewidziane na 2024/2025). Ustawa ta kompleksowo reformuje obronę cywilną i zarządzanie kryzysowe w Polsce, wykorzystując dotychczasowe analizy, wnioski z kontroli i doświadczenia z ostatnich lat. Przykładowo, wprowadza centralny rejestr zasobów ratowniczych „SI Omnibus”, lepiej precyzuje obowiązki poszczególnych organów oraz ustanawia fundusz wsparcia dla samorządów – są to rozwiązania wprost odpowiedzią na problemy zidentyfikowane podczas poprzednich kryzysów. Innym przykładem zmian prawnych będących efektem wyciągniętych wniosków jest nowelizacja ustawy Prawo wodne po powodzi 2010 r., która uszczelniła system zarządzania gospodarką wodną i zarządzania ryzykiem powodziowym (m.in. wdrażając unijną Dyrektywę Powodziową). Również doświadczenia walki z pandemią COVID-19 zaowocowały zmianami legislacyjnymi – znowelizowano ustawę o zarządzaniu kryzysowym i ustawy sanitarne, dodając tryby działania na wypadek epidemii i stanu zagrożenia zdrowia publicznego. Wszystkie te

korekty prawne spinają klamrą proces uczenia się: państwo dokonuje korekt ram prawnych, aby w przyszłości reagować szybciej i skuteczniej.

Na koniec warto zaznaczyć, że proces doskonalenia systemu nigdy się nie kończy. Każdy kryzys niesie nowe doświadczenia – zarówno błędy, które więcej nie powinny się powtórzyć, jak i innowacyjne rozwiązania warte stałego wdrożenia. Organizacja ucząca się to taka, która potrafi te doświadczenia wychwycić i przekuć w realne zmiany. Tylko wtedy można mówić o prawdziwej odporności i ciągłym podnoszeniu bezpieczeństwa. Jak ujął to jeden z raportów: „lessons learned” nie mogą pozostać sloganem – muszą przełożyć się na znaczące zmiany organizacyjne, inaczej system nie posuwa się naprzód. Dlatego zarządzanie wiedzą po zdarzeniu jest integralną częścią efektywnego zarządzania kryzysowego, zapewniającą, że ofiara danego kryzysu nie pójdzie na marne, lecz przyczyni się do lepszego przygotowania na przyszłe zagrożenia.

Rozdział IV.

Instrumenty i narzędzia zarządzania kryzysowego

4.1. Systemy informatyczne i bazy danych w zarządzaniu kryzysowym

Współczesne zarządzanie kryzysowe jest ściśle powiązane z wykorzystaniem systemów informatycznych oraz baz danych, które stanowią podstawę gromadzenia i przetwarzania informacji niezbędnych do skutecznego reagowania na zagrożenia. Zaawansowane technologie informacyjne wspierają cały cykl zarządzania kryzysowego – od monitorowania potencjalnych zagrożeń, poprzez planowanie działań i podejmowanie decyzji w sytuacjach kryzysowych, aż po analizę zdarzeń po zakończeniu akcji²⁹⁷. W literaturze przedmiotu systemy te określane są często mianem Emergency Management Information Systems (EMIS), czyli informatycznych systemów zarządzania kryzysowego, integrujących ludzi, procedury i technologie w celu dostarczenia decydentom właściwych informacji we właściwym czasie. Poniżej omówiono główne rodzaje systemów informatycznych wykorzystywanych w zarządzaniu kryzysowym, zagadnienie integracji danych między tymi systemami, a także wyzwania związane z ich bezpieczeństwem.

Jednym z filarów zarządzania kryzysowego są systemy informatyczne służące do ciągłego monitorowania i wczesnego wykrywania zagrożeń. Należą do nich rozmaite wyspecjalizowane platformy obserwacyjne, zbierające

²⁹⁷ J. Ristvej, A. Zagorecki, Information Systems for Crisis Management – Current Applications and Future Directions, Communications – Scientific Letters of the University of Žilina, 13(2), 2011, s. 59-63. <https://doi.org/10.26552/com.C.2011.2.59-63>

dane z sieci czujników i instytucji branżowych. Przykładowo, w zakresie zagrożeń meteorologicznych i hydrologicznych w Polsce funkcjonuje system Monitor IMGW-PIB, który prezentuje w czasie rzeczywistym dane o niebezpiecznych zjawiskach pogodowych i stanach wód na potrzeby służb kryzysowych. System ten integruje dane z automatycznych stacji pomiarowych IMGW, umożliwiając wizualizację sytuacji hydrologiczno-meteorologicznej na mapach cyfrowych, co stanowi podstawę ostrzegania przed powodzią, silnymi wiatrami czy innymi ekstremalnymi zjawiskami. W obszarze zagrożeń geologicznych (np. trzęsienia ziemi, osuwiska) rozwijane są systemy takie jak Centrum Zarządzania Geozagrożeniami Państwowego Instytutu Geologicznego, pełniące rolę centralnej bazy informacji o zdarzeniach sejsmicznych i geologicznych. Z kolei zagrożenia epidemiologiczne i sanitarne monitorowane są poprzez systemy inspekcji sanitarnych – przykładem jest tworzony w ostatnich latach Rejestr Ognisk Epidemiologicznych Narodowego Instytutu Zdrowia Publicznego PZH, gromadzący dane o pojawiających się chorobach zakaźnych. Systemy monitorowania funkcjonują również w innych domenach: Główny Inspektorat Ochrony Środowiska śledzi skażenia środowiskowe, Instytut Oceanologii monitoruje poziom morza i zagrożenia sztormowe, a Państwowa Agencja Atomistyki utrzymuje systemy detekcji skażeń promieniotwórczych. Cechą wspólną tych rozwiązań jest automatyzacja zbierania danych i generowanie wczesnych alertów – dzięki nim centra zarządzania kryzysowego otrzymują szybko informację o pojawiających się zagrożeniach, co umożliwia podjęcie działań prewencyjnych lub przygotowanie odpowiedzi.

Oprócz systemów bieżącego monitoringu, istotną rolę odgrywają bazy danych historycznych dotyczących sytuacji kryzysowych, klęsk żywiołowych i innych incydentów. Dane historyczne pozwalają na analizę trendów, wyciąganie wniosków i planowanie lepszych strategii na przyszłość. Na poziomie globalnym podstawowym źródłem informacji o katastrofach jest baza EM-DAT (Emergency Events Database), prowadzona od 1988 r. przez Centrum Badań nad Epidemiologią Katastrof CRED w Brukseli. EM-DAT zawiera ustandaryzowane informacje o ponad 17 000 katastrof (naturalnych i technologicznych) od 1900 r. do dziś, w tym dane o lokalizacji zdarzeń,

liczbie ofiar, osobach poszkodowanych oraz stratach ekonomicznych²⁹⁸. Stanowi to obiektywną podstawę do oceny ryzyka i podejmowania racjonalnych decyzji – np. pozwala decydentom zidentyfikować, jakie rodzaje klęsk najczęściej dotyczą dany kraj i jakie skutki powodowały historycznie. Profile krajowe generowane z EM-DAT są pomocne przy opracowywaniu planów zarządzania kryzysowego i redukcji ryzyka. W Europie i na świecie istnieją także inne bazy tego typu, jak choćby DesInventar gromadzący szczegółowe dane o klęskach na poziomie lokalnym, czy branżowe rejestry prowadzone przez agencje ONZ. W Polsce brak jest jednolitej publicznej bazy danych o wszystkich sytuacjach kryzysowych, jednak poszczególne służby i instytucje prowadzą własne rejestry zdarzeń. Państwowa Straż Pożarna od lat ewidencjonuje wszystkie interwencje ratowniczo-gaśnicze w elektronicznym Systemie Wspomagania Decyzji (SWD PSP). Dane te są następnie agregowane i publikowane w formie rocznych statystyk – na przykład w 2022 r. odnotowano w SWD PSP ponad 608 tysięcy interwencji strażaków, co było najwyższą liczbą zdarzeń w 30-letniej historii PSP. Tak ogromny zbiór danych obejmuje zarówno pożary, miejscowe zagrożenia (wichury, powodzie, wypadki itp.), jak i alarmy fałszywe, dostarczając cennych informacji o częstotliwości i charakterze zagrożeń na terenie kraju. Podobnie Policja, ratownictwo medyczne i inne służby gromadzą informacje o swoich działaniach w odpowiednich bazach danych. Coraz większego znaczenia nabiera też zbieranie danych o stratach (ludzkich i materialnych) bezpośrednio po katastrofach – wymóg taki stawia m.in. Ramka Sendai 2015-2030 dotycząca redukcji ryzyka katastrof, zobowiązując państwa do raportowania szkód spowodowanych zdarzeniami kryzysowymi. Dane te zasilają krajowe i międzynarodowe raporty, wspierając analizy kosztów katastrof oraz efektywności podejmowanych środków zaradczych.

Trzecim kluczowym rodzajem narzędzi informatycznych są systemy wspomagania decyzji, które integrują różnorodne informacje i modele celem ułatwienia pracy sztabów kryzysowych podczas planowania i reagowania. Zarządzanie kryzysowe wiąże się z koniecznością podejmowania szybkich decyzji w warunkach niepewności, presji czasu i brakujących danych

²⁹⁸ Centre for Research on the Epidemiology of Disasters (CRED), EM-DAT: międzynarodowa baza danych o katastrofach, Opis w portalu Climate-ADAPT, European Environment Agency, 2022.

– dlatego dedykowane systemy informatyczne starają się odciążyć decydentów, przetwarzając dane i proponując możliwe rozwiązania²⁹⁹. Systemy te przybierają rozmaite formy, w zależności od etapu cyklu kryzysowego. Na etapie przygotowania i zapobiegania mogą to być narzędzia do modelowania scenariuszy i oceny ryzyka (np. symulacje powodzi, rozprzestrzeniania skażeń czy przebiegu epidemii). Przykładowo, systemy GIS (geograficzne systemy informacyjne) pozwalają tworzyć mapy zagrożeń i analizować, które obszary i społeczności są najbardziej narażone – wykorzystuje się tu dane historyczne z baz zdarzeń oraz aktualne dane środowiskowe. W fazie reagowania coraz powszechniej stosuje się platformy dowodzenia i koordynacji akcji ratunkowych, które zapewniają wspólny obraz sytuacji dla wszystkich zaangażowanych służb. Przykładem może być rozwijany w Polsce zintegrowany System Zarządzania Kryzysowego JAŚMIN, który pozwala na bieżąco agregować i wizualizować dane o sytuacji (tworząc cyfrowy obraz operacyjny), zarządzać zasobami sił i środków, planować zadania dla poszczególnych jednostek oraz prowadzić komunikację między służbami w terenie a centrami decyzyjnymi³⁰⁰. System JAŚMIN, dzięki modułowej budowie, może wspierać zarówno działania stacjonarne (w centrach kryzysowych), jak i mobilne poprzez terminale i aplikacje terenowe, zapewniając m.in. funkcje monitoringu GPS jednostek w terenie, odbiór obrazu z dronów i kamer czy też symulowanie rozwoju sytuacji. Ważnym elementem systemów tego typu jest optymalizacja decyzji – poprzez wbudowane mechanizmy analityczne i symulacyjne mogą one proponować np. najkorzystniejsze rozmieszczenie sił ratowniczych, wyznaczanie stref ewakuacji w oparciu o prognozy pogody itp. Do klasy systemów wspomagania decyzji zaliczają się także rozwiązania eksperckie wykorzystujące sztuczną inteligencję i modele wiedzy do oceny sytuacji. Przykładowo, algorytmy uczenia maszynowego mogą pomagać prognozować rozwój pożaru na podstawie warunków atmosferycznych i danych o terenie, sugerując dowódcy optymalną strategię gaszenia.

²⁹⁹ J. Ristvej, A. Zagorecki, *Information Systems for Crisis Management – Current Applications and Future Directions*, Communications – Scientific Letters of the University of Žilina, 13(2), 2011, s. 59-63. <https://doi.org/10.26552/com.C.2011.2.59-63>

³⁰⁰ J. Sabak, *System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych*, Serwis Defence24.pl, 2021, <https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych>, [dostęp: 22.09.2025].

W zarządzaniu kryzysowym stosowane są również systemy typu Command & Control zaadaptowane z wojska, służące koordynacji działań i komunikacji. Niezależnie od implementacji, wspólnym celem systemów wspomagania decyzji jest dostarczenie decydentom aktualnej informacji oraz narzędzi analitycznych, aby decyzje podejmowane pod presją czasu były trafniejsze i oparte na danych, a nie wyłącznie na intuicji. Badania wskazują, że wykorzystanie takich systemów podnosi skuteczność i spójność działań ratunkowych, zwłaszcza gdy w akcję zaangażowanych jest wiele podmiotów³⁰¹.

Różnorodność opisanych wyżej systemów – tworzonych przez odmienne służby i instytucje, wyspecjalizowanych pod kątem określonych zagrożeń lub działań – rodzi wyzwanie skutecznej wymiany informacji między nimi. Interoperacyjność systemów informatycznych w zarządzaniu kryzysowym oznacza zdolność różnych platform i baz danych do współpracy, tak, aby uczestnicy działań kryzysowych mieli jednolity, wspólny obraz sytuacji i mogli sprawnie się komunikować³⁰². W praktyce osiągnięcie tego jest trudne z uwagi na silosowe struktury – np. straż pożarna, policja, pogotowie, wojsko, administracja lokalna czy służby hydrologiczne tradycyjnie posiadały własne, odrębnie rozwijane systemy informacyjne, często nieprzystosowane do automatycznego udostępniania danych na zewnątrz. Brak interoperacyjności skutkowało opóźnieniami w przepływie danych (np. konieczność przekazywania informacji telefonicznie lub ręcznego wprowadzania do innych systemów) oraz ryzykiem niejednoznaczności informacji. W odpowiedzi na te problemy podejmuje się działania na rzecz integracji danych – zarówno na poziomie organizacyjnym (zawieranie porozumień o współpracy i wymianie informacji między instytucjami), jak i technicznym (tworzenie wspólnych platform lub translatorów danych).

We współczesnych systemach zarządzania kryzysowego coraz częściej wdraża się otwarte standardy wymiany danych, co ułatwia łączenie różnych rozwiązań. Przykładem uznanych międzynarodowo standardów są: Common Alerting Protocol (CAP) – ujednolicony format komunikatu alarmowego i ostrzeżenia, oraz rodzina standardów Emergency Data Exchange

³⁰¹ M. Kuziemski, G. Misuraca, AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings, *Telecommunications Policy*, 44(6), 101976, 2020, <https://doi.org/10.1016/j.telpol.2020.101976>

³⁰² S. J. Rysz, Integracja informatyczna w obszarze zarządzania kryzysowego, *Modern Management Review*, 22(2), 2017, s. 117-130. <https://doi.org/10.7862/rz.2017.mmr.20>

Language (EDXL), definiująca schematy XML dla różnych rodzajów komunikatów kryzysowych (np. raporty sytuacyjne, zapotrzebowanie na zasoby, informacje o poszkodowanych itp.). Zastosowanie standardu CAP pozwala np. Instytutowi Meteorologii i Gospodarki Wodnej wysłać ostrzeżenie o gwałtownej burzy w formacie zrozumiałym automatycznie dla systemów wykorzystywanych przez Rządowe Centrum Bezpieczeństwa, media czy aplikacje alarmowe – ten sam komunikat może być jednocześnie wykorzystany do powiadomienia ludności (np. poprzez SMS) i do aktualizacji danych w systemach sztabowych. Z kolei standardy z rodziny EDXL (opracowane przez organizację OASIS) obejmują m.in. EDXL-DE (Distribution Element) do opisu pakietów danych dystrybuowanych między systemami, EDXL-RM (Resource Messaging) do zgłaszania zapotrzebowania na siły i środki czy EDXL-SitRep do przesyłania ustandaryzowanych raportów sytuacyjnych. W praktyce wdrożenie tych standardów umożliwia, by różne służby wymieniały między sobą zrozumiałe informacje nawet wtedy, gdy używają odmiennych aplikacji – translacja odbywa się do wspólnego, neutralnego formatu³⁰³. Przykładowo, jeśli policja posługuje się innym systemem niż straż pożarna, ale oba wspierają EDXL, wówczas dane o zdarzeniu (jak lokalizacja, typ zagrożenia, wymagane zasoby) mogą przepływać automatycznie między tymi służbami. Standardy obejmują zarówno interoperacyjność syntaktyczną (wspólny format danych), jak i interoperacyjność semantyczną – poprzez zdefiniowane taksonomie zagrożeń, zasobów i działań zapewnia się jednakowe rozumienie pojęć w różnych instytucjach. Innymi słowy, systemy korzystające ze standardów nie muszą być ręcznie dostosowywane do siebie nawzajem, a mimo to mogą wymieniać dane.

W Polsce dążenie do integracji systemów informacji kryzysowej również jest dostrzegalne. Ustawa o zarządzaniu kryzysowym zobowiązuje Rządowe Centrum Bezpieczeństwa (RCB) do monitorowania, analizowania i wymiany informacji o zagrożeniach z innymi podmiotami systemu zarządzania kryzysowego³⁰⁴. RCB pełni rolę koordynatora – utrzymuje całodobowe centrum operacyjne, które korzysta z danych dostarczanych m.in. przez

³⁰³ DRIVER+, Common Information Space (CIS) – narzędzie wymiany danych w zarządzaniu kryzysowym, 2025, <https://tgm.ercis.org/pl/metody-i-narzedzia/common-information-space>, [dostęp: 22.09.2025].

³⁰⁴ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 11 ust. 2).

IMGW, PIG, GIS, PAA i inne instytucje branżowe. W praktyce współpraca ta realizowana jest poprzez uzgodnione kanały komunikacji i narzędzia. Przykładowo, Platforma Informatyczna RCB umożliwia wojewódzkim centrom zarządzania kryzysowego raportowanie zdarzeń do poziomu centralnego oraz pobieranie ostrzeżeń i zaleceń. Z kolei w ramach projektów unijnych tworzono prototypy zintegrowanych systemów – jak ISP (Informatyczny System Osłony Kraju) przed nadzwyczajnymi zagrożeniami, który miał scalać informacje meteorologiczne, hydrologiczne i geologiczne dla administracji publicznej. We wspomnianym już systemie JAŚMIN szczególny nacisk położono na interoperacyjność z innymi systemami resortów – zaimplementowano tam kilkanaście standardów wymiany danych (m.in. wojskowe standardy NATO, a także cywilne standardy GIS jak usługi WMS) gwarantujących zdolność do współpracy z systemami zarówno krajowej administracji, jak i sieci sojuszniczych. Można stwierdzić, że techniczna możliwość integracji jest już obecna – wyzwaniem pozostaje często uzgodnienie kwestii organizacyjnych i prawnych, takich jak zakres udostępnianych informacji, procedury bezpieczeństwa przy wymianie danych, czy zapewnienie kompatybilności wersji oprogramowania w różnych instytucjach. Niemniej trend zmierza ku tworzeniu wspólnej przestrzeni informacyjnej dla podmiotów zarządzania kryzysowego, gdzie dane z różnych źródeł zasilają jeden spójny obraz sytuacji (tzw. Common Operational Picture). Dzięki temu np. dyżurny w centrum kryzysowym może na jednym ekranie śledzić jednocześnie obraz radarowy opadów, poziomy rzek, lokalizacje wypadków drogowych i położenie pojazdów ratowniczych – choć informacje te pochodzą z różnych systemów, są zintegrowane na jednej platformie.

Dynamiczny rozwój systemów teleinformatycznych w zarządzaniu kryzysowym pociąga za sobą również nowe wyzwania, zwłaszcza w obszarze bezpieczeństwa informacji. Po pierwsze, systemy te gromadzą ogromne wolumeny danych, w tym dane wrażliwe (np. dane osobowe poszkodowanych, informacje o infrastrukturze krytycznej, szczegóły operacji służb), co wymaga zapewnienia odpowiedniej ochrony przed nieuprawnionym dostępem. Bezpieczeństwo informacji musi być uwzględniane już na etapie projektowania i wdrażania systemów – obejmuje to szyfrowanie transmisji danych, uwierzytelnianie użytkowników, zarządzanie rolami i uprawnieniami dostępu, regularne tworzenie kopii zapasowych baz danych oraz fizyczne

zabezpieczenie centrów przetwarzania. Wysokie wymagania dotyczą zwłaszcza tych elementów systemu, które muszą działać nawet w warunkach kryzysowych – np. kiedy infrastruktura telekomunikacyjna jest uszkodzona lub przeciążona. Niezawodność i redundancja systemów informatycznych staje się kluczowa: centra zapasowe, alternatywne łącza komunikacyjne i generatory awaryjne zasilania to standard w krytycznych węzłach systemu, takich jak centra zarządzania kryzysowego szczebla krajowego i wojewódzkiego.

Równocześnie coraz większym zagrożeniem są cyberataki wymierzone w infrastrukturę teleinformatyczną wykorzystywaną do zarządzania kryzysowego. Paradoksalnie, systemy tworzone po to, by radzić sobie z tradycyjnymi sytuacjami kryzysowymi, same mogą stać się celem ataku i wywołać sytuację kryzysową nowego typu. Przykładowo, atak hakerski na systemy łączności służb ratunkowych mógłby sparaliżować koordynację akcji, a manipulacja danymi (np. fałszywe alarmy lub zmiana odczytów sensorów) – wprowadzić chaos decyzyjny. Odnotowano przypadki, gdy cyberprzestępcy uruchamiali syreny alarmowe w miastach (jak incydent masowego włączenia syren w Dallas w 2017 r.), czy też ataki ransomware unieruchamiające całe sieci informatyczne szpitali i urzędów. Dlatego też cyberbezpieczeństwo stało się integralną częścią zarządzania kryzysowego. Samorządy i służby lokalne, które jeszcze do niedawna koncentrowały się głównie na zagrożeniach fizycznych, obecnie muszą inwestować w ochronę swoich systemów IT – stosować zapory sieciowe, systemy wykrywania włamań (IDS/IPS), aktualizować oprogramowanie oraz szkolić personel z zasad bezpieczeństwa³⁰⁵. Konieczne jest opracowanie procedur reagowania na cyberincydenty w ramach struktur kryzysowych – np. przygotowanie planów awaryjnych na wypadek utraty kluczowych systemów (procedury pracy manualnej, przełączenia na zapasowe kanały komunikacji). W Polsce za reagowanie na incydenty komputerowe odpowiada m.in. zespół CERT Polska, a na szczeblu administracji publicznej – CSIRT GOV przy ABW, ich współpraca z centrami kryzysowymi jest coraz ściślejsza, zwłaszcza w obliczu narastających globalnych napięć i ataków hybrydowych. Wysokie standardy bezpieczeństwa są też wbudowywane w nowe systemy – przykładowo SZK JAŚMIN zapewnia wielopoziomowe

³⁰⁵ J. Staśkiewicz, Budowanie odporności na zagrożenia – rola samorządów w zarządzaniu kryzysowym, OpenSecurity.pl, 2024, <https://opensecurity.pl/budowanie-odpornosci-na-zagrozenia-rola-samorzadow-w-zarzadzaniu-kryzysowym/>, [dostęp: 22.09.2025].

zabezpieczenia, umożliwiając nawet przetwarzanie informacji niejawnych dzięki mechanizmom klasyfikacji, szyfrowania end-to-end i kontroli dostępu zgodnym z wymaganiami NATO³⁰⁶.

Systemy informatyczne i bazy danych stały się nieodzownym narzędziem we współczesnym zarządzaniu kryzysowym, radykalnie zwiększając możliwości monitorowania zagrożeń, szybkiej wymiany informacji i podejmowania decyzji w trudnych sytuacjach. Jednocześnie wymagają one ciągłego doskonalenia pod względem integracji i bezpieczeństwa. Kolejne rozdziały niniejszej pracy poświęcone będą specyficznym technologiom (takim jak GIS, drony, analityka danych) oraz aspektom komunikacji i cyberbezpieczeństwa, uzupełniając obraz roli, jaką odgrywa informatyka w zapewnianiu bezpieczeństwa w obliczu kryzysów.

4.2. Centra zarządzania kryzysowego i systemy ostrzegania ludności

W efektywnym systemie zarządzania kryzysowego kluczową rolę odgrywają centra zarządzania kryzysowego oraz sprawnie działające systemy ostrzegania ludności. Centra zarządzania kryzysowego (CZK) na różnych szczeblach administracji odpowiadają za całodobowy monitoring zagrożeń, koordynację działań ratunkowych i przekazywanie informacji decyzyjnej, podczas gdy systemy ostrzegania umożliwiają szybkie powiadomianie mieszkańców o niebezpieczeństwach³⁰⁷. Poniższy rozdział przedstawia organizację centrów zarządzania kryzysowego (ich zadania, obsadę i tryb pracy 24/7 oraz współpracę między szczeblami), omawia istniejące w Polsce systemy ostrzegania ludności (syreny alarmowe, SMS-owy Alert RCB, Regionalny System Ostrzegania i komunikaty medialne), a także analizuje przepływ informacji od służb i instytucji, poprzez centra i władze decyzyjne, aż do społeczeństwa.

³⁰⁶ J. Sabak, System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, Serwis Defence24.pl, 2021, <https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych>, [dostęp: 22.09.2025].

³⁰⁷ R. Budzisz, Centra zarządzania kryzysowego w systemie bezpieczeństwa wewnętrznego państwa, Warszawa, Wydawnictwo Szkoły Głównej Służby Pożarniczej, 2020.

System zarządzania kryzysowego w Polsce ma strukturę wieloszczelkową, odpowiadającą podziałowi administracyjnemu państwa. Centra zarządzania kryzysowego na wszystkich poziomach – od RCB po centra wojewódzkie i powiatowe (oraz ewentualnie gminne) – mają zbliżone zadania określone ustawowo. Do ich podstawowych zadań należy przede wszystkim pełnienie całodobowego dyżuru w celu zapewnienia stałego przepływu informacji na potrzeby zarządzania kryzysowego. Realizacja tego zadania oznacza, że centra działają 24 godziny na dobę, 7 dni w tygodniu – w praktyce poprzez system zmianowy dyżurnych operacyjnych wyposażonych w odpowiednie środki łączności. Całodobowa gotowość centrów pozwala niezwłocznie odebrać sygnały o zagrożeniach i przekazać je dalej do właściwych organów. Ustawodawca wymaga, aby wszystkie instytucje współpracujące z RCB i centrami (ministerstwa, służby, inspekcje itd.) utrzymywały całodobowe numery kontaktowe (telefony, adresy e-mail) swoich służb dyżurnych na potrzeby obiegu informacji kryzysowej. Poza ciągłym monitoringiem i dyżurem informacyjnym, centra kryzysowe wykonują szereg innych zadań o charakterze koordynacyjno-informacyjnym. Należą do nich m.in.: współdziałanie z innymi centrami zarządzania kryzysowego organów administracji publicznej różnych szczebli (zapewnianie wymiany informacji pionowej i poziomej między centrami), nadzór nad funkcjonowaniem systemów wykrywania zagrożeń i alarmowania oraz systemu wczesnego ostrzegania ludności, współpraca z podmiotami monitorującymi środowisko (np. Instytut Meteorologii i Gospodarki Wodnej, Państwowa Agencja Atomistyki) celem pozyskiwania danych o potencjalnych zagrożeniach, a także współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne (Państwowa Straż Pożarna, Policja, pogotowie, GOPR i inni). Centra zajmują się również przygotowywaniem i przekazywaniem ostrzeżeń, komunikatów i informacji dotyczących prognozowanych zagrożeń (np. ostrzeżeń meteorologicznych) do właściwych służb i ludności³⁰⁸, dokumentowaniem działań podejmowanych w sytuacjach kryzysowych oraz zadaniami stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa.

³⁰⁸ I. Abgarowicz, T. Plasota, M. Napiórkowski, Nowoczesne technologie wspierające raportowanie o zagrożeniach na potrzeby systemu zarządzania kryzysowego RP, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Administracyjne, 882, 7, 2015, s. 104-118. <https://doi.org/10.18276/sa.2015.7-06>

Typowe centrum zarządzania kryzysowego jest obsadzone przez doświadczony personel dyżurny – np. w WCZK lub PCZK dyżury pełnią oficerowie operacyjni (często przedstawiciele PSP, Policji lub urzędu) wspierani przez dyspozytorów i analityków³⁰⁹. Praca centrum odbywa się w trybie zmianowym, aby zagwarantować nieprzerwaną działalność przez 24 godziny na dobę. W praktyce oznacza to tworzenie grafików dyżurów (zmiany dzienne i nocne, świąteczne itp.), często z wykorzystaniem systemu Służby Dyżurnej Państwa – sieci połączonych dyspozytorni i centrów, które wspólnie zapewniają ciągłe monitorowanie sytuacji³¹⁰. Przykładowo, Wojewódzkie Centrum Zarządzania Kryzysowego w każdym urzędzie wojewódzkim monitoruje na bieżąco sytuację na swoim terenie i co dobę sporządza meldunki sytuacyjne (dzienne i nocne) dla przełożonych: meldunek dobowy z godz. 24:00 kierowany jest do RCB, zaś poranny meldunek (stan na godz. 7:00) – do wojewody. Informacje zbierane są ze wszystkich powiatów i służb, co daje całościowy obraz sytuacji. W razie poważnych zdarzeń centrum uruchamia tryb alarmowy pracy, ściągając dodatkowy personel i ewentualnie zwołując posiedzenie wojewódzkiego/powiatowego zespołu zarządzania kryzysowego (który stanowi sztab doradczy złożony z przedstawicieli służb).

Skuteczność systemu wymaga ścisłej współpracy pionowej i poziomej między centrami wszystkich szczebli. Informacje o zagrożeniach przepływają oddolnie – np. gmina lub powiat zgłasza do WCZK wystąpienie lokalnego zdarzenia (katastrofy, awarii, klęski) przekraczającego ich możliwości, zaś WCZK powiadamia RCB w przypadku zagrożenia o potencjale ponadwojewódzkim lub wymagającego wsparcia centralnego³¹¹. Jednocześnie polecenia i wytyczne przekazywane są odgórnie – RCB zapewnia obsługę Rządowego Zespołu Zarządzania Kryzysowego i premiera, wydając zalecenia wojewodom, wojewoda wydaje polecenia starostom, a ci wójtom/burmistrzom,

³⁰⁹ A. Nowak, Rola i zadania Wojewódzkiego Centrum Zarządzania Kryzysowego, Zeszyty Naukowe WSOSP, 4, 2019, s. 67-80.

³¹⁰ M. Rachwalska, MSWiA przejmuje dyżur. Służba Dyżurna Państwa zastąpi RCB, InfoSecurity24.pl, 2022, <https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/mswia-przejmuje-dyzur-sluzba-dyzurna-panstwa-zastapi-rcb>, [dostęp: 22.09.2025].

³¹¹ Rządowe Centrum Bezpieczeństwa, Obieg informacji i rola RCB w systemie zarządzania kryzysowego, Gov.pl, 2024, <https://www.gov.pl/web/rcb/obieg-informacji-i-rola-rcb-w-systemie-zarzadzania-kryzysowego>, [dostęp: 22.09.2025].

zgodnie z ustawową hierarchią zarządzania kryzysowego³¹². Centra wojewódzkie utrzymują stały kontakt z powiatowymi centrami – np. WCZK przekazuje powiatom komunikaty i ostrzeżenia otrzymane z centralnych instytucji monitorujących (IMGW, PAA itd.)³¹³. Z kolei PCZK informuje wszystkie gminy w powiecie o sytuacji oraz może pełnić funkcję wspólnego centrum dla gmin, które nie mają własnych GCZK (często powiatowe centrum przejmuje dyżur także dla gmin). Takie współdzielenie zasobów jest zgodne z prawem – dopuszcza się tworzenie wspólnych centrów dla miasta na prawach powiatu i powiatu ziemskiego lub innych jednostek w porozumieniu³¹⁴. Współpraca między centrami ma również wymiar ponadnarodowy: RCB pełni funkcję krajowego punktu kontaktowego i współdziała z centrum koordynacji reagowania kryzysowego UE (ERCC w Brukseli) oraz odpowiednikami w NATO, uczestnicząc w wymianie informacji o transgranicznych zagrożeniach i korzystając z mechanizmów wczesnego ostrzegania międzynarodowego³¹⁵.

Warto podkreślić, że centra zarządzania kryzysowego stanowią „nerw informacyjny” całego systemu bezpieczeństwa. Przykładowo, Powiatowe CZK w Chełmie w ciągu jednego roku przyjęło ponad 16 tysięcy zgłoszeń wymagających interwencji dyżurnych (awarie, zdarzenia pogodowe, zagrożenia porządku publicznego), które następnie były przekazywane do właściwych służb i władz³¹⁶. Dzięki stałemu dyżurowi i procedurom obiegu informacji, nawet równoczesne sytuacje kryzysowe mogą być monitorowane i obsługiwane bez opóźnień. Centra sporządzają raporty cząstkowe i raporty dobowe, które trafiają do przełożonych – stanowią one podstawę do podejmowania decyzji przez władze samorządowe i centralne. W kolejnej części rozdziału omówione zostaną narzędzia, za pomocą których decyzje te przekazywane są społeczeństwu, czyli systemy ostrzegania i alarmowania ludności.

³¹² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 17-20).

³¹³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 16, art. 18).

³¹⁴ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 18, ust. 4).

³¹⁵ W. Skomra, Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy, Warszawa, BEL Studio, 2018.

³¹⁶ I. Abgarowicz, T. Plasota, M. Napiórkowski, Nowoczesne technologie wspierające raportowanie o zagrożeniach na potrzeby systemu zarządzania kryzysowego RP, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Administracyjne, 882, 7, 2015, s. 104-118. <https://doi.org/10.18276/sa.2015.7-06>

Równie istotnym zagadnieniem są systemy ostrzegania i alarmowania ludności. Ostrzeganie ludności cywilnej o grożących niebezpieczeństwach jest jednym z fundamentalnych zadań ochrony ludności i zarządzania kryzysowego³¹⁷. W Polsce system ostrzegania i alarmowania ludności oparty jest na kombinacji sygnałów alarmowych (syren), komunikatów nadawanych za pośrednictwem mediów oraz nowoczesnych technologii jak powiadomienia SMS i aplikacje mobilne³¹⁸. Strukturę tego systemu tworzą zarówno tradycyjne środki obrony cywilnej, przejęte z dawnych rozwiązań (syreny alarmowe, komunikaty radiowe/telewizyjne), jak i nowe rozwiązania teleinformatyczne wdrożone w ostatnich latach (system Alert RCB, Regionalny System Ostrzegania). Istotą działania systemu jest dotarcie z informacją o zagrożeniu do możliwie najszerszego grona odbiorców w jak najkrótszym czasie, w formie zrozumiałej i wymuszającej pożądaną reakcję³¹⁹. Poniżej scharakteryzowano główne składowe systemu ostrzegania ludności w Polsce, ich organizację oraz aktualny stan rozwoju.

Syreny alarmowe stanowią klasyczny system akustyczny. To najstarszy element systemu alarmowania – są to stacjonarne lub mobilne urządzenia generujące głośny sygnał dźwiękowy, słyszalny na znaczną odległość, używane do ogłaszania alarmów (np. nalotowego, awaryjnego) lub ich odwołania. W wielu krajach, w tym w Polsce, sieć syren alarmowych jest wciąż powszechnie wykorzystywana. Tradycyjnie zarządzanie syrenami należało do struktur Obrony Cywilnej kraju i realizowane było głównie na wypadek zagrożeń militarnych³²⁰. Współcześnie rola syren została rozszerzona na wszelkie poważne zagrożenia, w tym klęski żywiołowe i katastrofy przemysłowe, a same sygnały zostały ujednolicone. Od 2025 r. obowiązuje jednolity system sygnałów alarmowych w całym kraju – i tak: modulowany dźwięk syreny trwający 3 minuty oznacza ogłoszenie alarmu (bezpośrednie zagrożenie, np. atak, skażenie, katastrofa), zaś ciągły dźwięk syreny przez 3 minuty oznacza

³¹⁷ M. Kowalewski, Ostrzeganie i alarmowanie ludności w sytuacjach zagrożeń – aspekty prawne i organizacyjne, *Bezpieczeństwo. Teoria i Praktyka*, 3, 2014, s. 45-58.

³¹⁸ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 22.09.2025].

³¹⁹ H. Parapura, M. Kowalewski, B. Kowalczyk, Ostrzeganie i alarmowanie ludności w niebezpieczeństwie – rozwiązania w Polsce i na świecie, *Telekomunikacja i Techniki Informacyjne*, 1-2/2013, 2013, s. 74-83.

³²⁰ P. Nalepa, *Obrona Cywilna dziś – stan, wyzwania, perspektywy*, Warszawa, Bellona, 2019.

odwołanie alarmu (koniec zagrożenia). Dodatkowo mogą być przekazywane komunikaty głosowe przez systemy megafonowe lub rozgłośnie lokalne, precyzujące rodzaj zagrożenia. Sieć syren w Polsce jest bardzo rozległa – szacuje się, że obecnie funkcjonuje kilka tysięcy punktów alarmowych na terenie kraju. Jednak wiele urządzeń to syreny starego typu (elektromechaniczne), które wymagają modernizacji. Od 2023 r. realizowany jest program unowocześnienia systemu alarmowania ludności, finansowany ze środków Krajowego Planu Odbudowy. Państwowa Straż Pożarna, we współpracy z MSWiA, modernizuje system alarmowy w 4060 lokalizacjach na terenie całej Polski – istniejące syreny analogowe zostaną zastąpione nowoczesnymi syrenami cyfrowymi, rozbudowana będzie infrastruktura łączności, a systemy gminne i centralne zostaną zintegrowane. Na realizację tego projektu przeznaczono 175 mln zł (środki KPO), a zakończenie prac planowane jest na koniec 2025 r.³²¹ Nowe syreny będą sterowane przy użyciu zaawansowanych technologii komunikacyjnych (m.in. radiowej łączności cyfrowej DMR, sieci GSM oraz sieci bezprzewodowej LoRaWAN), co znacząco zwiększy ich niezawodność i zasięg działania. Modernizacja obejmuje też wyposażenie punktów alarmowych w zasilanie awaryjne (fotowoltaika, akumulatory) oraz włączenie syren do jednolitego, szyfrowanego systemu teleinformatycznego. Dzięki temu możliwe będzie załączenie alarmu jednocześnie na dużym obszarze (np. w całym województwie lub kraju) za pomocą decyzji centralnej, jak i punktowo przez władze lokalne w zależności od potrzeb. Syreny alarmowe mają kilka istotnych zalet: są natychmiastowe (głośny sygnał dociera do wszystkich w zasięgu niemal równocześnie), niezależne od sieci telekomunikacyjnych oraz działają nawet przy przeciążeniu innych kanałów (np. w sytuacji masowego dzwonienia przez ludzi). Stanowią też jedyny środek ostrzegania skuteczny dla osób przebywających na zewnątrz i oderwanych od mediów elektronicznych (sygnał dźwiękowy trudno przeoczyć). Ograniczeniem jest brak informacji szczegółowej – sam dźwięk syreny informuje tylko, że coś zagraża i należy udać się w bezpieczne miejsce i nasłuchiwać komunikatów. Dlatego syrenom towarzyszą komunikaty słowne w mediach i SMS (omówione dalej),

³²¹ Ministerstwo Spraw Wewnętrznych i Administracji, Modernizujemy system alarmowy – ponad 4 tys. lokalizacji z nowoczesnymi syrenami, gov.pl, <https://www.gov.pl/web/obrona-cywilna/modernizujemy-system-alarmowy--ponad-4-tys-lokalizacji-z-nowoczesnymi-syrenami>, [dostęp: 31.10.2025].

które precyzują rodzaj zagrożenia i zalecenia dla obywateli. Warto również zauważyć, że w niektórych krajach stosuje się syreny w węższym zakresie (np. tylko wokół zakładów chemicznych lub w wybranych strefach zagrożenia), natomiast Polska – z uwagi na uwarunkowania historyczne i geograficzne – utrzymuje szeroką sieć syren jako uniwersalny środek alarmowy.

Kolejny przykład to SMS-owy Alert RCB. Dynamiczny rozwój telefonii komórkowej umożliwił wprowadzenie systemu masowego ostrzegania za pomocą wiadomości SMS. W Polsce takim rozwiązaniem jest Alert RCB – system SMS-owego powiadamiania ludności o zagrożeniach, uruchomiony na stałe w 2018 r.³²². Podstawę prawną stanowi nowelizacja ustawy Prawo telekomunikacyjne i ustawy o zarządzaniu kryzysowym z lipca 2018 r., która zobowiązała operatorów komórkowych do rozsyłania komunikatów alarmowych na zlecenie RCB³²³. Alert RCB działa w ten sposób, że w sytuacji wystąpienia poważnego zagrożenia dla życia lub zdrowia na danym obszarze, Rządowe Centrum Bezpieczeństwa formułuje treść ostrzeżenia i – po akceptacji przez właściwy organ (np. MSWiA lub wojewodę) – zleca operatorom GSM wysłanie SMS-a do wszystkich telefonów komórkowych zarejestrowanych w stacjach bazowych na zagrożonym terenie. Wiadomość przychodzi natychmiast, bezpłatnie dla odbiorcy, z nadpisem „Alert RCB”. Treść Alertu RCB jest zwięzła (max. 160 znaków) i zawsze zawiera wskazanie rodzaju zagrożenia oraz podstawowe zalecenia dla ludności. Przykładowe komunikaty to: „Uwaga! Silny wiatr. Możliwe przerwy w dostawach prądu. Zostań w domu, zabezpiecz rzeczy.” lub „Uwaga! Skażenie chemiczne w rejonie X. Nie wychodź z domu, uszczelnij okna, słuchaj komunikatów”³²⁴. Tak sformułowany alert informuje, co się dzieje i jak należy się zachować – bez zbędnych szczegółów, ale wystarczająco, by podjąć natychmiastowe środki ostrożności.

System Alert RCB został pilotażowo wdrożony podczas nawałnic w 2018 r., a od grudnia 2018 r. funkcjonował w pełnym zakresie. Według

³²² Rozporządzenie Rady Ministrów z dnia 31 sierpnia 2020 r. w sprawie współpracy dyrektora Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu (Dz.U. z 2020 r. poz. 1527).

³²³ Ustawa z dnia 10 maja 2018 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. z 2018 r. poz. 1118).

³²⁴ Rządowe Centrum Bezpieczeństwa, Alert RCB – przykładowe wiadomości (SMS), gov.pl, <https://www.gov.pl/web/rcb/alert-rcb---przykladowe-wiadomosci-sms>, [dostęp: 22.09.2025].

badań już w pierwszym roku jego działania ponad 80% Polaków otrzymało co najmniej jednego SMS-a z Alertem RCB, a większość społeczeństwa oceniła to rozwiązanie pozytywnie, uznając je za potrzebne. Istotną zaletą Alertu RCB był bardzo szeroki zasięg, ponieważ wiadomości trafiały do wszystkich telefonów komórkowych znajdujących się na danym obszarze, w tym również do osób czasowo tam przebywających, takich jak turyści. Zapewniało to szybkość przekazu oraz wysoki poziom dostępności komunikatu. W odróżnieniu od syren system mógł również przekazywać konkretną treść i instrukcje postępowania. Jego ograniczeniem pozostawała jednak zależność od sprawności infrastruktury telekomunikacyjnej i dostępności urządzeń końcowych – w sytuacji braku zasilania lub przeciążenia sieci część odbiorców mogła nie otrzymać wiadomości na czas. Mimo to, Alert RCB istotnie zwiększył zdolność ostrzegania – obecnie wysyłany jest kilkanaście-kilkadziesiąt razy w roku, głównie przed gwałtownymi zjawiskami pogodowymi (wichury, gwałtowne burze, ekstremalne upały), ale także przed innymi nadzwyczajnymi zagrożeniami (np. skażenia wody, sytuacje epidemiologiczne, a w 2022 r. ostrzeżenia przed dezinformacją wojenną itp.). Dla przykładu, w 2022 r. Rządowe Centrum Bezpieczeństwa wysłało 20 komunikatów ostrzegawczych dotyczących silnego wiatru oraz 13 komunikatów związanych z upałami, a ponadto po kilka alertów odnoszących się do powodzi, intensywnych opadów śniegu i innych zagrożeń. Treść wszystkich komunikatów ostrzegawczych jest równolegle publikowana w serwisie internetowym RCB oraz w kanałach komunikacji cyfrowej (w tym w mediach społecznościowych), co zwiększa zasięg i dostępność ostrzeżeń. System masowego ostrzegania ludności za pośrednictwem urządzeń mobilnych nie jest jednak rozwiązaniem unikatowym dla Polski. W wielu państwach funkcjonują analogiczne mechanizmy ostrzegania oparte na wiadomościach SMS (Short Message Service) lub na technologii nadawania komórkowego (Cell Broadcast)³²⁵. Przykładami są m.in. Wireless Emergency Alerts (WEA) w Stanach Zjednoczonych³²⁶, rozwiązania wdrażane w państwach Unii Europejskiej w ramach standardu EU-Alert oraz system Alert Ready

³²⁵ ETSI, ETSI TS 102 900, European Public Warning Service (EU-Alert) using Cell Broadcast, ETSI, 2023.

³²⁶ Federal Communications Commission, Wireless Emergency Alerts (WEA), <https://www.fcc.gov/consumers/guides/wireless-emergency-alerts>, [dostęp: 22.09.2025].

w Kanadzie³²⁷. Na poziomie Unii Europejskiej wprowadzono obowiązek wdrożenia publicznych systemów ostrzegania ludności wykorzystujących sieci łączności elektronicznej (często określany jako „Reverse 112”), co oznacza konieczność zapewnienia możliwości szybkiego przekazywania ostrzeżeń do osób znajdujących się na obszarze zagrożenia³²⁸. W Polsce wymaganie to zostało zrealizowane poprzez rozwój krajowego systemu Alert RCB. W perspektywie dalszego doskonalenia systemów ostrzegania istotne znaczenie ma przechodzenie od dystrybucji ostrzeżeń wyłącznie w formie SMS do technologii Cell Broadcast, która umożliwia jednoczesne rozgłaszanie komunikatu alarmowego do wszystkich urządzeń w zasięgu wskazanych stacji bazowych bez mechanizmu sekwencyjnego wysyłania wiadomości. Rozwiązanie to ogranicza ryzyko opóźnień w warunkach bardzo dużej liczby odbiorców oraz poprawia skalowalność systemu. Kierunek ten pozostaje spójny ze standardami technicznymi EU-Alert oraz trendem modernizacji publicznych systemów ostrzegania w państwach europejskich.

Kolejnym komponentem krajowego systemu ostrzegania jest Regionalny System Ostrzegania (RSO) – rozwiązanie uruchomione w 2015 r. z inicjatywy Ministerstwa Spraw Wewnętrznych i Administracji oraz Telewizji Polskiej, przeznaczone do przekazywania komunikatów o zagrożeniach o charakterze regionalnym i lokalnym za pośrednictwem telewizji oraz Internetu³²⁹. System obejmuje kilka uzupełniających się kanałów dystrybucji informacji: bezpłatną aplikację mobilną RSO (dostępną m.in. dla systemów Android i iOS), emisję komunikatów w programach Telewizji Polskiej – w szczególności w formie pasków informacyjnych i teletekstu na kanałach regionalnych (TVP3) oraz infrastrukturę serwisów internetowych urzędów wojewódzkich, w ramach których publikowane są komunikaty dla obszaru danego województwa. Za przygotowanie i publikację treści w RSO odpowiadają Wojewódzkie Centra Zarządzania Kryzysowego, pełniące funkcję redakcyjną i dystrybucyjną w skali regionalnej. W systemie mogą być publikowane m.in. ostrzeżenia

³²⁷ Public Safety Canada, National Public Alerting System (Alert Ready), <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sstm-en.aspx>, [dostęp: 22.09.2025].

³²⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/172 ustanawiająca Europejski kodeks łączności elektronicznej, art. 110 (Dz.U. L 321 z 17.12.2018, 2018).

³²⁹ Ministerstwo Spraw Wewnętrznych i Administracji, Regionalny System Ostrzegania, <https://www.gov.pl/web/mswia/regionalny-system-ostrzegania>, [dostęp: 22.09.2025].

meteorologiczne IMGW, informacje o skażeniach wody, awariach infrastruktury, utrudnieniach komunikacyjnych, poszukiwaniach osób zaginionych oraz inne komunikaty istotne z perspektywy bezpieczeństwa mieszkańców. Po wprowadzeniu komunikatu do systemu jest on udostępniany równolegle w aplikacji (z możliwością aktywacji powiadomień push) oraz w kanałach telewizyjnych, co sprzyja szybkiemu dotarciu do odbiorców wykorzystujących różne media. Funkcją RSO jest uzupełnianie mechanizmów ostrzegania o rozwiązaniach przeznaczone do zdarzeń, które nie zawsze spełniają kryteria uruchomienia Alertu RCB, a jednocześnie wymagają przekazania informacji i zaleceń w skali regionalnej lub lokalnej. System może być wykorzystywany zarówno w działaniach prewencyjnych (komunikaty edukacyjne, ostrzeżenia przed określonymi zjawiskami lub zagrożeniami), jak i w sytuacjach kryzysowych, gdy konieczne jest utrzymanie stałego kanału informacyjnego z mieszkańcami oraz przekazywanie treści bardziej rozbudowanych niż pojedynczy komunikat SMS, w tym zawierających szerszy opis sytuacji, odsyłacze do stron internetowych lub materiały pomocnicze.

Ograniczeniem RSO jest jego zależność od aktywnego korzystania przez odbiorców – skuteczność aplikacji mobilnej zależy od instalacji i utrzymywania jej na urządzeniu, a kanał telewizyjny od bieżącej konsumpcji przekazu. Z tego względu zasięg RSO ma charakter komplementarny wobec powszechnego oddziaływania Alertu RCB. Niezależnie od tego system RSO pozostaje wartościowym elementem architektury ostrzegania, zwiększając elastyczność komunikacji i umożliwiając regionalnym strukturom administracji przekazywanie informacji adekwatnych do specyfiki zagrożeń występujących na danym obszarze. W praktyce europejskiej podobne funkcje pełnią rozwiązania aplikacyjne wykorzystywane m.in. w Niemczech (NINA, KATWARN) oraz w Czechach (eWarn)^{330,331}. Kierunki rozwoju RSO obejmują dalszą integrację z innymi narzędziami ostrzegania i alarmowania, w tym z rozwiązaniami modernizowanego systemu alarmowego, co ma zwiększyć dostępność informacji oraz spójność komunikatów w sytuacjach nadzwyczajnych.

³³⁰ Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Warn-App NINA, https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html, [dostęp: 22.09.2025].

³³¹ Fraunhofer FOKUS / KATWARN, KATWARN – warning system (public warnings and behavioural advice), https://www.fokus.fraunhofer.de/en/espri/projects/en_katwarn.html, [dostęp: 22.09.2025].

Kolejnym komponentem są komunikaty kryzysowe w mediach. Tradycyjne środki masowego przekazu nadal pełnią bardzo ważną funkcję w ostrzeganiu ludności. Media publiczne (telewizja, radio) są zobowiązane do emisji komunikatów organów administracji w razie poważnego zagrożenia. Zgodnie z ustawą o radiu i telewizji oraz przepisami o stanie klęski żywiołowej, nadawcy na polecenie odpowiednich władz muszą niezwłocznie przekazywać oficjalne komunikaty i instrukcje dla ludności (dotyczy to np. zarządzeń o ewakuacji, informacji o skażeniu itp.). Dlatego integralną częścią systemu ostrzegania jest tzw. komunikat kryzysowy – specjalne ogłoszenie nadawane przez stacje radiowe i telewizyjne. W Polsce przyjęto rozwiązanie, że takim komunikatem zarządza wojewoda (na poziomie regionalnym) lub Minister Spraw Wewnętrznych/premier (na poziomie krajowym). Przykładowo, gdy w 2017 r. doszło do dużej awarii zanieczyszczającej wodociąg, lokalne rozgłośnie radiowe na polecenie wojewody cyklicznie informowały mieszkańców o konieczności przegotowywania wody.

Coraz większą rolę odgrywają także media cyfrowe i społecznościowe. Rządowe Centrum Bezpieczeństwa oraz wiele samorządów prowadzi aktywne profile na X, Facebooku i innych platformach, gdzie publikowane są ostrzeżenia i porady. Choć nie są to formalnie część „systemu ostrzegania”, stanowią ważny kanał dystrybucji informacji kryzysowej, zwłaszcza dla młodszej części społeczeństwa. Władze lokalne korzystają również z systemów SMS-owych dla mieszkańców (niezależnych od Alertu RCB) – w niektórych gminach funkcjonują bazy numerów telefonu mieszkańców, którzy zapisali się, by otrzymywać powiadomienia (dotyczące np. przerw w dostawach mediów czy lokalnych zagrożeń). Tego typu systemy (np. SISMS) były popularne przed uruchomieniem Alertu RCB i nadal są wykorzystywane jako uzupełnienie, choć mają mniejszy zasięg i wymagają rejestracji przez użytkownika. Kolejnym nośnikiem informacji są tablice i znaki elektroniczne (np. tablice drogowe VMS wyświetlające ostrzeżenia o wichurach czy smogu) oraz sieci radiowęzłów (np. w niektórych miejscowościach istnieją głośniki na latarniach umożliwiające nadanie komunikatu głosowego).

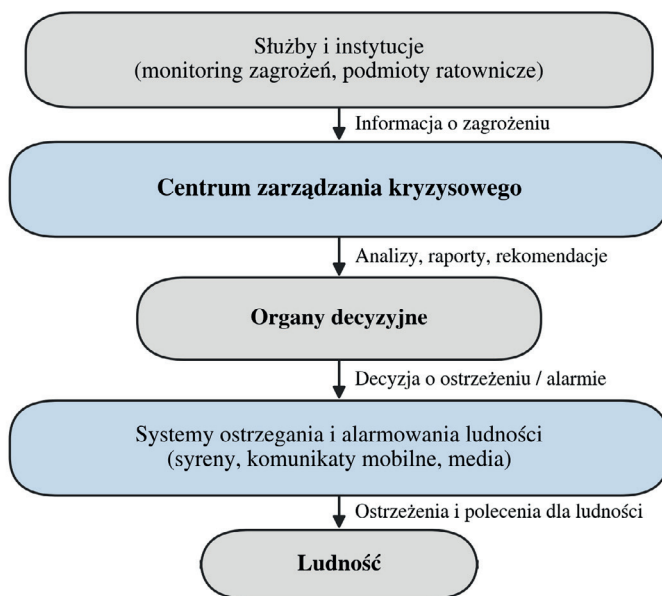
Polski system ostrzegania ludności ma charakter wielokanałowy i opiera się na równoległym wykorzystaniu sygnałów akustycznych oraz narzędzi komunikacji elektronicznej. Zastosowanie redundancji kanałów dystrybucji

ostrzeżeń zwiększa prawdopodobieństwo dotarcia przekazu do odbiorców, niezależnie od ich bieżącej aktywności, miejsca przebywania oraz preferowanego medium. Warunkiem efektywności tak zorganizowanego systemu jest jednak spójność komunikacji: przekazy rozpowszechniane różnymi kanałami powinny być merytorycznie zgodne i wzajemnie się uzupełniać, tak, aby nie generować rozbieżności interpretacyjnych ani nie prowadzić do zakłóceń informacyjnych. W tym celu Rządowe Centrum Bezpieczeństwa oraz centra zarządzania kryzysowego wdrażają rozwiązania proceduralne służące standaryzacji treści komunikatów, obejmujące wskazanie kluczowych elementów ostrzeżenia (charakter zagrożenia, obszar oddziaływania, ramy czasowe oraz zalecane działania ochronne). Równolegle stosowane są zasady eskalacji komunikacji, polegające na dostosowaniu doboru kanałów oraz intensywności przekazu do dynamiki i skali zdarzenia, tak aby w miarę wzrostu poziomu zagrożenia możliwe było uruchamianie kolejnych form ostrzegania oraz uzupełnianie informacji kierowanych do ludności.

Należy podkreślić, iż skuteczne ostrzeganie i alarmowanie ludności jest możliwe tylko wtedy, gdy istnieje sprawny obieg informacji od źródeł zagrożeń, przez organy decyzyjne, do społeczeństwa. Proces ten obejmuje trzy główne etapy przepływu:

- napływ informacji o zagrożeniu od służb i instytucji do centrów zarządzania kryzysowego,
- przekazanie informacji i analiz z centrów do władz decyzyjnych celem podjęcia decyzji,
- dystrybucję decyzji (ostrzeżeń, poleceń) od władz do ludności za pomocą systemów alarmowych.

Rysunek 13 ilustruje schemat tego przepływu informacji w systemie ostrzegania i reagowania kryzysowego.



Rysunek 13. Obieg informacji w systemie ostrzegania i reagowania

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.); Ministerstwo Spraw Wewnętrznych i Administracji, Regionalny System Ostrzegania, <https://www.gov.pl/web/mswia/regionalny-system-ostrzegania>, [dostęp: 22.09.2025].

Pierwsza faza – od służb do centrów – zaczyna się w momencie, gdy dochodzi do niepokojącego zdarzenia lub gdy instytucje monitorujące wykryją potencjalne zagrożenie. Źródłem informacji mogą być tu różne podmioty: służby ratownicze (PSP, Policja, pogotowie – zgłaszające np. poważny wypadek, pożar, skażenie), inspekcje i straże (np. Sanepid informujący o skażeniu wody, Inspekcja Ochrony Środowiska o wycieku chemicznym, Straż Graniczna o incydencie radiacyjnym na granicy), a także instytuty monitorujące środowisko (IMGW wydający ostrzeżenie meteorologiczne o nadchodzącej nawałnicy, Państwowy Instytut Geologiczny rejestrujący wstrząs sejsmiczny, itp.). Informacja o zagrożeniu jest niezwłocznie przekazywana do właściwego centrum zarządzania kryzysowego. Przykładowo, dyżurny operacyjny straży pożarnej, otrzymawszy zgłoszenie o uwolnieniu toksycznej chmury z zakładu przemysłowego, alarmuje równocześnie swoje siły ratownicze i informuje Powiatowe CZK, które pełni dyżur informacyjny (ew. bezpośrednio WCZK, zależnie od procedur). Dzięki całodobowej gotowości, centrum może

odebrać informację o każdej porze i rozpocząć dalsze działania. Informacje spływające do centrów są weryfikowane (często napływają z wielu źródeł jednocześnie) i zbierane w formie raportów lub meldunków. Centra wojewódzkie otrzymują również ostrzeżenia i prognozy od centralnych instytucji (IMGW, PAA, RCB itp.) – np. RCB może przekazać WCZK informację od europejskiego systemu wczesnego ostrzegania o produktach żywnościowych (RASFF) o skażonej partii żywności w regionie.

Druga faza – od centrów do władz decyzyjnych – polega na przekazaniu zebranych informacji i rekomendacji do osób lub organów, które mają kompetencje podjąć działania w reakcji na zagrożenie. Centra zarządzania kryzysowego przygotowują raporty, analizy i prognozy rozwoju sytuacji dla swoich przełożonych³³². Na szczeblu lokalnym takim „przełożonym” centrum jest np. starosta (dla PCZK) lub prezydent miasta, na szczeblu wojewódzkim – wojewoda (dla WCZK), a na szczeblu krajowym – dyrektor RCB raportuje bezpośrednio ministrowi właściwemu (MSWiA) lub premierowi. W praktyce często informacja jest przekazywana równolegle na kilka poziomów: jeśli sytuacja jest poważna, PCZK powiadamia zarówno starostę, jak i WCZK (wojewodę). Następnie, zgodnie z zasadą subsydiarności, decyzje zapadają na najniższym możliwym szczeblu: wójt/burmistrz może sam ogłosić alarm i zarządzić ewakuację pojedynczych budynków, ale już przy zagrożeniu obejmującym całą gminę może potrzebować wsparcia powiatu itd. Władze decyzyjne to zatem osoby piastujące funkcje uprawnione do wydania stosownych poleceń – może to być starosta zarządzający ewakuacją w powiecie, wojewoda wprowadzający pogotowie przeciwpowodziowe w regionie, czy premier ogłaszający stan klęski żywiołowej na terenie państwa. Centra dostarczają tym władzom rekomendacji, scenariuszy działania i wariantów – np. WCZK informuje wojewodę, że zbliża się ekstremalna wichura i rekomenduje uruchomienie alarmowania ludności i pozostanie w domach, a wojewoda na tej podstawie podejmuje decyzję o wysłaniu Alertu RCB i włączeniu syren. Ustawa zobowiązuje RCB do zapewnienia sprawnego obiegu informacji pomiędzy wszystkimi szczeblami administracji – od

³³² I. Abgarowicz, T. Plasota, M. Napiórkowski, Nowoczesne technologie wspierające raportowanie o zagrożeniach na potrzeby systemu zarządzania kryzysowego RP, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Administracyjne, 882, 7, 2015, s. 104-118. <https://doi.org/10.18276/sa.2015.7-06>

wójta po premiera – właśnie po to, by decydenci mogli szybko uzyskać pełny obraz sytuacji i wydać niezbędne dyspozycje.

Trzecia faza – od władz do ludności – to właściwe ostrzeżenie społeczeństwa, realizowane poprzez opisane wcześniej systemy alarmowe. Gdy właściwy organ wyda decyzję (np. wojewoda poleca uruchomienie alarmu lub RCB formułuje treść ostrzeżenia), informacja ta musi jak najszybciej dotrzeć do zagrożonej populacji. W zależności od charakteru zagrożenia i dostępnych środków wykorzystuje się jeden lub kilka kanałów jednocześnie. Alarm powszechny (syrena) ogłaszany jest, gdy niezbędne jest natychmiastowe zaalarmowanie wszystkich w okolicy – np. przy zagrożeniu skażeniem chemicznym czy nadchodzącym uderzeniu tornado. Syreny uruchamia się zdalnie: decyzję o ich włączeniu podejmuje zwykle starosta lub wojewoda, a technicznie realizuje to dyżurny PCZK/WCZK za pomocą systemu sterowania (komendy radiowej lub poprzez sieć). Równolegle, jeśli jest czas na sformułowanie komunikatu, wysyłany jest Alert RCB – wiadomość SMS trafi prosto na telefony mieszkańców, przekazując treść ostrzeżenia. Władze wojewódzkie mogą także skorzystać z RSO – wprowadzić komunikat, który pojawi się w aplikacjach i na ekranach telewizorów. Standardowo uruchamia się także komunikaty w mediach – stacje radiowe i TV przerywają program, aby nadać pilne ogłoszenie (często czytane na antenie przez wojewodę lub innego urzędnika, by dodać powagi i wiarygodności). Dodatkowo, lokalne służby mogą wysłać na ulice patrole z megafonami (np. samochody OSP objeżdżające miejscowość i nadające przez głośnik komunikat „Uwaga, skażenie wody – nie używać kranów!”). Wszystkie te działania mają zapewnić, że informacja dotrze do obywateli różnymi drogami i skłoni ich do właściwej reakcji.

W tym miejscu następuje sprzężenie zwrotne: ludność, otrzymawszy ostrzeżenie, podejmuje działania (chroni się, stosuje do zaleceń), ale też może generować nowe informacje zwrotne – np. obywatele dzwonią na numer alarmowy 112, potwierdzając wystąpienie zjawiska czy prosząc o pomoc. Te informacje znów trafiają do służb i centrów, co pozwala aktualizować sytuację (np. spływają meldunki od patroli, od mieszkańców – centra analizują je i przekazują władzom, które podejmują dalsze decyzje, np. o odwołaniu alarmu gdy zagrożenie minie). W ten sposób obieg informacji jest ciągły i trwa przez cały czas trwania sytuacji kryzysowej – od jej początku, aż do pełnej likwidacji zagrożeń.

Centra zarządzania kryzysowego i systemy ostrzegania ludności są ze sobą nierozzerwalnie powiązane w jednolitym układzie informacyjnym. Centra stanowią mózg i układ nerwowy – zbierają dane, analizują i inicjują działania, natomiast systemy ostrzegania to zmysły i głos systemu – pozwalają dostrzec zagrożenie (czujniki, radary, obserwacje) oraz zaalarmować całe społeczeństwo (syreny, SMS-y, media). Doświadczenia ostatnich lat – od ekstremalnych zjawisk pogodowych po zagrożenia związane z pandemią – pokazały, że szybki przepływ informacji i skuteczne ostrzeganie są w stanie uratować wiele istnień ludzkich³³³. Ciągłe doskonalenie centrów zarządzania kryzysowego (poprzez szkolenia, ćwiczenia, integrację systemów informacyjnych) oraz modernizacja i rozwój systemów alarmowych (cyfryzacja syren, nowe technologie mobilne) pozostają priorytetem polityki bezpieczeństwa państwa. W dobrze zorganizowanym systemie bezpieczeństwa każdy mieszkaniec – od dużego miasta po najmniejszą wieś – powinien w sytuacji zagrożenia otrzymać szybko jasny komunikat: co się dzieje i jak się chronić. Dzięki połączeniu wysiłków profesjonalnych służb, sprawnych centrów kryzysowych i nowoczesnych narzędzi ostrzegawczych, cel ten staje się osiągalny, co bezpośrednio przekłada się na poprawę bezpieczeństwa nas wszystkich.

4.3. Wykorzystanie technologii GIS, dronów i analityki danych

Współczesne zarządzanie bezpieczeństwem i sytuacjami kryzysowymi coraz szerzej korzysta z zaawansowanych technologii informacyjnych. Wśród nich kluczową rolę odgrywają systemy informacji geograficznej (GIS), bezzałogowe statki powietrzne (drony) oraz narzędzia analityki danych i Big Data. Technologie te umożliwiają lepsze zrozumienie zagrożeń, sprawniejsze planowanie działań ratunkowych i podejmowanie decyzji w oparciu o aktualne dane. Zgodnie z badaniami, era dużych zbiorów danych i zaawansowanych analiz otwiera nowe możliwości dla zarządzania kryzysowego, ponieważ Big Data pozwalają wizualizować, analizować,

³³³ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 22.09.2025].

a nawet przewidywać przebieg katastrof, zasadniczo zmieniając działania humanitarne i zarządzanie kryzysowe³³⁴. Poniżej omówiono zastosowania poszczególnych technologii – GIS, dronów oraz analityki danych – w kontekście bezpieczeństwa i sytuacji nadzwyczajnych, wraz z przykładami ich rzeczywistego wykorzystania.

System informacji geograficznej to komputerowy system umożliwiający gromadzenie, analizę i wizualizację danych odniesionych przestrzennie. W zarządzaniu kryzysowym narzędzia GIS stały się fundamentalne dla podejmowania decyzji opartych na lokalizacji zdarzeń i zasobów³³⁵. GIS znajduje zastosowanie we wszystkich fazach cyklu zarządzania katastrofami – od prewencji i przygotowania, poprzez reagowanie, aż po odbudowę. Pozwala m.in. na modelowanie zagrożeń i podatności terenu (tworzenie map ryzyka), planowanie ewakuacji i rozmieszczenia zasobów ratunkowych, wsparcie operacji ratunkowych poprzez bieżący podgląd sytuacji, a także ocenę strat i planowanie odbudowy po zdarzeniu. Innymi słowy, GIS integruje różnorodne dane na mapie, ułatwiając zrozumienie zależności przestrzennych – np. nakładając informacje o infrastrukturze krytycznej, zagrożeniach i danych demograficznych można wyodrębnić najbardziej narażone obszary i społeczności. Jednym z podstawowych zastosowań GIS jest tworzenie map zagrożeń i map ryzyka dla potrzeb planowania kryzysowego. Przykładowo, system GIS może integrować dane o ukształtowaniu terenu, użytkowaniu ziemi oraz historycznych zdarzeniach (np. zasięg powodzi czy pożarów) w celu wyznaczenia stref najbardziej zagrożonych danym typem katastrofy³³⁶. Takie mapy hazardu stanowią podstawę do opracowania strategii minimalizacji skutków zagrożeń. W Stanach Zjednoczonych Federalna Agencja Zarządzania Kryzysowego (FEMA) tworzy oficjalne mapy zagrożenia powodziowego (Flood Hazard Maps) wykorzystywane do planowania przestrzennego i kalkulacji ubezpieczeń. Analizy wykazały, że inwestycje w aktualizację map powodzi przynoszą wymierne korzyści – kosztorysy FEMA wskazują, że mapy

³³⁴ S. Akter, S. F. Wamba, Big data and disaster management: a systematic review and agenda for future research, *Annals of Operations Research*, 283(1), 2019, s. 939-959. <https://doi.org/10.1007/s10479-017-2584-2>

³³⁵ M. Holser, The Importance of GIS in Emergency Management, *Environmental Law Journal* (Environmental Law Review Syndicate – Scholarship), New York University School of Law, 2016.

³³⁶ M. Karimiziarani, Social Media Analytics in Disaster Response: A Comprehensive Review, *arXiv preprint*, 2023. <https://doi.org/10.48550/arXiv.2307.04046>

te wygenerowały oszczędności rzędu 1,33 mld USD przy kosztach ok. 0,8 mld USD, a same mapy są wykorzystywane około 30 milionów razy rocznie przez agencje rządowe, urbanistów, ubezpieczycieli i obywateli na potrzeby oceny ryzyka i planowania przestrzennego³³⁷. Również w Polsce rozwijane są systemy map zagrożeń – wartym odnotowania projektem był Informatyczny System Osłony Kraju (ISOK), w ramach którego opracowano m.in. cyfrowe mapy powodziowe i osuwisk, udostępniane następnie w krajowym geoportalu na potrzeby służb kryzysowych³³⁸. Dzięki temu służby ratownicze oraz administracja publiczna dysponują narzędziem do szybkiej identyfikacji obszarów zagrożonych i podejmowania decyzji o np. konieczności ewakuacji. GIS umożliwia też tworzenie planów ewakuacji poprzez analizę sieci dróg, ukształtowania terenu oraz rozmieszczenia ludności. Za pomocą narzędzi GIS można wyznaczać optymalne trasy ewakuacji z zagrożonych obszarów, uwzględniając przepustowość dróg czy potencjalne wąskie gardła (np. mosty, zwężenia) oraz szacować czas potrzebny na przemieszczenie ludności. Możliwe jest także projektowanie stref ewakuacji – obszarów, z których ludność powinna zostać przemieszczona w razie zagrożenia – oraz komunikowanie tych stref społeczeństwu za pomocą interaktywnych map dostępnych online. Przykładowo, wiele rejonów nadmorskich wdrożyło programy „Know Your Zone” udostępniające mieszkańcom mapy predefiniowanych stref ewakuacyjnych na wypadek huraganu czy tsunami³³⁹. Dzięki temu, gdy zagrożenie wystąpi, władze mogą ogłosić ewakuację konkretnych stref, co upraszcza i przyspiesza akcję opuszczania zagrożonych terenów. Analizy GIS pomagają też zidentyfikować, które obszary wymagają priorytetowej ewakuacji, np. ze względu na gęstość zaludnienia czy brak dostatecznej liczby dróg ewakuacyjnych. Badania nad ewakuacją tsunami wskazują, że z reguły ludność zwleka z rozpoczęciem ucieczki, co może skutkować ofiarami³⁴⁰. Dlatego za-

³³⁷ M. Holser, *The Importance of GIS in Emergency Management*, Environmental Law Journal (Environmental Law Review Syndicate – Scholarship), New York University School of Law, 2016.

³³⁸ P. Zaskórski, D. Żbik, *Monitorowanie zagrożeń z wykorzystaniem systemów informacji geograficznej*, Studia Bezpieczeństwa Narodowego, 9(1), 2016, s. 397-413. <https://doi.org/10.37055/sbn/129836>

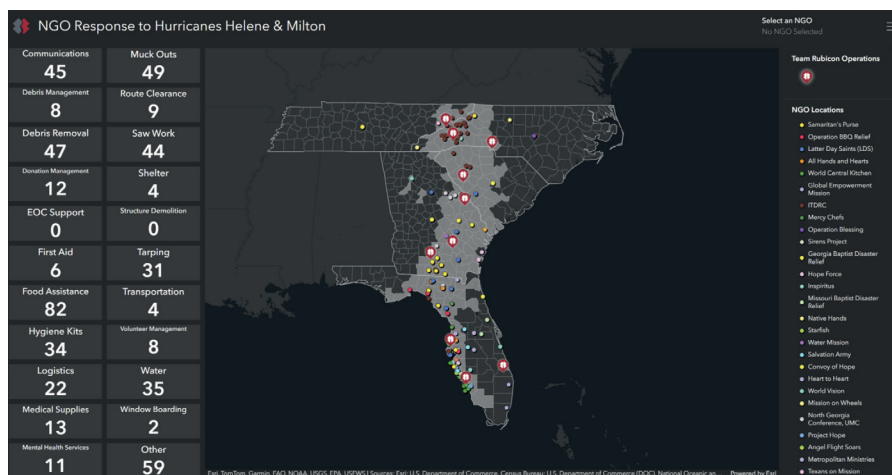
³³⁹ Esri, *ArcGIS Solutions: Introduction to Know Your Zone*, <https://doc.arcgis.com/en/arcgis-solutions/latest/reference/introduction-to-know-your-zone.htm>, [dostęp: 22.09.2025].

³⁴⁰ F. Makinoshima, S. Yotsui, S. Sato, F. Imamura, *Large-scale geolocation data reveal evacuation behaviour during the 2024 Noto Peninsula earthquake and tsunami*, Communications Earth & Environment, 6, 891, 2025. <https://doi.org/10.1038/s43247-025-02819-8>

wczasu opracowane mapy ewakuacji i ćwiczenia z ich wykorzystaniem są kluczowe dla skrócenia czasu reakcji mieszkańców. Przykładem efektywnej ewakuacji może być wydarzenie z Japonii – podczas tsunami na półwyspie Noto w 2024 r. dane geolokalizacyjne z telefonów wskazały, że mieszkańcy rozpoczęli ucieczkę średnio w ciągu 2-6 minut od trzęsienia ziemi, co przyczyniło się do zaskakująco niskiej liczby ofiar³⁴¹. Tak szybka reakcja była możliwa m.in. dzięki świadomości zagrożeń i wcześniejszemu przygotowaniu stref ewakuacji, co potwierdza użyteczność planowania opartego na analizach GIS i Big Data. W trakcie rozwijającej się sytuacji kryzysowej systemy GIS dodatkowo pełnią rolę centralnego panelu sytuacyjnego (tzw. Common Operating Picture), integrując dane z wielu źródeł i prezentując je na mapie w czasie zbliżonym do rzeczywistego. Umożliwia to służbom efektywne śledzenie położenia zasobów (jednostek ratowniczych, pojazdów, sprzętu) oraz monitorowanie rozwoju sytuacji (np. rozprzestrzeniania się pożaru czy zalewania terenu). Przykładowo, podczas akcji przeciwpowodziowej zespół kryzysowy może na bieżąco nanosić na mapę informacje o przerwanych wałach, zalanych drogach, rozmieszczeniu ekip ratunkowych i punktów pomocy. Organizacja humanitarna Team Rubicon opisuje zastosowanie interaktywnych map GIS podczas reagowania na huragany – jeszcze przed uderzeniem żywiołu analitycy nakładają prognozowaną trasę huraganu oraz strefy zagrożenia (np. zalewowe) na mapę gęstości zaludnienia i wskaźników wrażliwości społecznej, a także zaznaczają rozmieszczenie własnych zasobów (magazyny sprzętu, zespoły ratowników). W efekcie powstają dashboards GIS, które pokazują kto i co może znaleźć się w strefie zagrożenia, jak poważne mogą być skutki oraz gdzie rozmieszczać zespoły ratunkowe przed katastrofą. Przykład takiego panelu przedstawiono na rysunku 14, obrazującym mapę sytuacyjną po huraganie Helene w Karolinie Północnej – zaznaczono na nim m.in. zablokowane drogi oraz lokalizacje działań innych organizacji pomocowych, co pomogło zidentyfikować obszary jeszcze nieobjęte wsparciem³⁴²:

³⁴¹ Tamże.

³⁴² J. H. Case, From Satellites to Survivors: How GIS Powers Disaster Response, Team Rubicon, <https://teamrubiconusa.org/news-and-stories/gis-disaster-response>, [dostęp: 22.09.2025].



Rysunek 14. Panel sytuacyjny GIS – rozmieszczenie działań organizacji pozarządowych po huraganach Helene i Milton (dashboard „NGO Response to Hurricanes Helene & Milton”)

Źródło: J. H. Case, From Satellites to Survivors: How GIS Powers Disaster Response, Team Rubicon, <https://teamrubiconusa.org/news-and-stories/gis-disaster-response>, [dostęp: 22.09.2025].

Przykład panelu sytuacyjnego GIS stworzonego po huraganie (Helene, 2018 r.) – mapa pokazuje zablokowane drogi (czerwone symbole) oraz miejsca prowadzenia akcji przez różne organizacje pomocowe. Takie dashboards GIS umożliwiają koordynację działań wielu podmiotów i uniknięcie dublowania wysiłków.

W terenie ratownicy również korzystają z narzędzi geoinformacyjnych – mobilne aplikacje powiązane z systemem GIS pozwalają im zbierać dane i zgłaszać sytuację wprost z miejsca zdarzeń. Na przykład członkowie Team Rubicon używają aplikacji terenowych (Fulcrum, ArcGIS Field Maps, Survey123) do raportowania uszkodzeń budynków, zatorów drogowych czy potrzeb poszkodowanych, a informacje te automatycznie zasilają centralną mapę operacji. Dzięki temu mapa staje się żywym, aktualizowanym obrazem sytuacji – władze mogą na bieżąco widzieć, które drogi są nieprzejezdne, gdzie nie ma prądu, ile domów zostało zniszczonych itp. – i w oparciu o te dane dynamicznie kierować siły tam, gdzie są najbardziej potrzebne. GIS pełni więc rolę „łącznika” między satelitami, dronami, czujnikami a personelem w terenie, integrując wszystkie te informacje przestrzennie. Tak zintegrowana

świadomość sytuacyjna jest kluczowa, by żadna społeczność ani obszar dotknięty kryzysem nie pozostały „niewidoczne” dla organizatorów akcji.

Podsumowując, zastosowanie GIS w bezpieczeństwie opiera się na zasadzie „jeśli coś nie jest na mapie, to nie istnieje w operacji”. Mapy tworzone w systemach informacji geograficznej stają się podstawą planowania i koordynacji działań – od wyznaczania stref ryzyka i ewakuacji, przez rozmieszczanie zasobów i prowadzenie akcji ratunkowej, po dokumentowanie strat. Oczywiście, efektywność GIS zależy od jakości danych – nieaktualne lub niedokładne dane mogą prowadzić do błędnych decyzji, dlatego wyzwaniem jest stałe doskonalenie baz danych geoprzestrzennych oraz ich udostępnianie w przejrzystej formie³⁴³. Mimo to, współczesne przykłady dowodzą, że inwestycje w technologie GIS znacząco podnoszą skuteczność zarządzania kryzysowego i bezpieczeństwem publicznym.

Kolejnym przykładem technologii istotnie wzmacniającej zdolności reagowania są drony, czyli bezzałogowe statki powietrzne (UAV – Unmanned Aerial Vehicles), które – dzięki szybkiemu pozyskiwaniu danych rozpoznawczych, elastyczności użycia oraz możliwości działania w strefach trudno dostępnych i niebezpiecznych – stanowią obecnie jedno z kluczowych narzędzi wspierających służby w ocenie sytuacji, koordynacji działań oraz monitorowaniu przebiegu zdarzeń. Początkowo kojarzone głównie z wojskiem, obecnie są powszechnie wykorzystywane w zastosowaniach cywilnych, w tym w reagowaniu na klęski żywiołowe i inne sytuacje nadzwyczajne³⁴⁴. Drony oferują unikalne możliwości: mogą szybko dostarczyć obraz sytuacji z powietrza, dotrzeć do miejsc niedostępnych lub niebezpiecznych dla ludzi, prowadzić obserwację bez narażania ratowników, a nawet transportować drobne ładunki. W kontekście bezpieczeństwa i ratownictwa można wyróżnić kilka głównych obszarów zastosowań dronów:

- Rozpoznanie terenu i monitoring sytuacji: Drony wyposażone w kamery wizyjne i termowizyjne są wykorzystywane do rekonesansu obszaru dotkniętego katastrofą, dostarczając aktualnych zdjęć i nagrań

³⁴³ M. Holser, The Importance of GIS in Emergency Management, *Environmental Law Journal* (Environmental Law Review Syndicate – Scholarship), New York University School of Law, 2016.

³⁴⁴ E. Yucesoy, B. Balcik, E. Coban, The role of drones in disaster response: A literature review of operations research applications, *International Transactions in Operational Research*, 32(2), 2024, s. 981-1025. <https://doi.org/10.1111/itor.13484>

z powietrza. Umożliwia to ocenę skali zniszczeń, wykrycie nowych zagrożeń (np. pożarów wtórnych, wycieków chemikaliów) oraz ogólną orientację w sytuacji, zanim załogi ratownicze wejdą do terenu. Bezzałogowe rozpoznanie okazało się niezwykle cenne np. po trzęsieniu ziemi w Nepalu w 2015 r. – drony wysłane nad odcięte od świata górskie wioski pomogły ocenić rozmiar zniszczeń i potrzeby pomocowe tych społeczności, do których trudno było dotrzeć drogą lądową³⁴⁵. Również po trzęsieniu ziemi w Ekwadorze w 2016 r. lokalne służby wykorzystywały drony do szybkiej inspekcji sieci dróg – w ciągu kilkunastu godzin od zdarzenia uzyskano wysokiej jakości mapę uszkodzeń drogowych, co umożliwiło sprawne zaplanowanie tras dla ekip ratunkowych. Drony skutecznie wspierają też monitoring pożarów lasów – krążąc nad płonącym obszarem mogą przekazywać obraz termiczny, dzięki czemu sztab widzi gdzie ognisko jest najintensywniejsze i jak się rozprzestrzenia. W porównaniu do tradycyjnego rozpoznania z helikoptera, drony są tańsze i mogą latać bliżej ziemi, dając lepszą rozdzielczość obrazu.

- Dokumentacja i ocena zniszczeń: Po przejściu katastrofy naturalnej drony są wykorzystywane do szacowania strat – wykonują fotografie lotnicze zniszczonych budynków, infrastruktury i terenu, które następnie mogą zostać przetworzone w ortofotomapy i trójwymiarowe modele zniszczeń. Takie dane są bezcenne dla służb oraz władz przy planowaniu pomocy i odbudowy. Przykładowo, po huraganie Maria na Portoryko (2017 r.) drony z kamerami wysokiej rozdzielczości mapowały rozległe tereny zniszczeń, co pozwoliło szybciej oszacować liczbę uszkodzonych budynków niż poprzez pieszą inspekcję. Obecnie łączy się te działania z algorytmami sztucznej inteligencji – zdjęcia z dronów lub satelitów mogą być automatycznie analizowane przez modele głębokiego uczenia w celu klasyfikacji stopnia zniszczeń. Badania pokazują, że z wykorzystaniem AI można w ciągu kilkunastu godzin od zdarzenia zanalizować setki kilometrów kwadratowych

³⁴⁵ A. Ferris-Rotman, How drones are helping Nepal recover from the earthquake, Huffington Post, https://www.huffpost.com/entry/nepal-earthquake-drones_n_7232764, [dostęp: 22.09.2025].

zdjęć i określić, które budynki uległy całkowitemu zniszczeniu, a które np. częściowym uszkodzeniom³⁴⁶. Tego typu model – nazwany DAHiTrA – został ostatnio przetestowany na zdjęciach po huraganie Harvey w Teksasie, osiągając wysoką skuteczność w automatycznej ocenie stopnia zniszczeń budynków³⁴⁷. Drony przyspieszają też ocenę szkód w infrastrukturze – w energetyce stosuje się je do inspekcji linii wysokiego napięcia po wichurach, a w drogownictwie do przeglądu mostów i wiaduktów pod kątem uszkodzeń (np. Federal Highway Administration testowała wykorzystanie UAV do inspekcji mostów). W każdej z tych sytuacji bezzałogowce pozwalają oglądać zniszczenia z bliska bez ryzyka dla inspektorów, co jest szczególnie ważne, gdy konstrukcje mogą grozić zawaleniem.

- Wsparcie w poszukiwaniu i ratowaniu ludzi: Jedno z najważniejszych zastosowań dronów to poszukiwanie osób zaginionych lub uwięzionych w wyniku katastrofy. Wyposażone w kamery termowizyjne drony potrafią wykrywać źródła ciepła ludzkiego ciała nawet nocą lub w gęstej roślinności. W akcjach poszukiwawczych, np. po osunięciach ziemi czy lawinach, dron może szybko przeczesać duży obszar i zlokalizować sygnały świadczące o obecności ludzi, kierując następnie ekipy ratunkowe we właściwe miejsca. Drony ratownicze były z powodzeniem wykorzystywane m.in. podczas poszukiwań ocalałych po huraganie Dorian na Bahamach (2019 r.) czy przy ewakuacji ludzi odciętych przez powódź w Niemczech (2021 r.). Literatura przedmiotu wyróżnia poszukiwanie i ratownictwo (Search and Rescue, SAR) jako jeden z kluczowych obszarów zastosowań UAV w sytuacjach kryzysowych³⁴⁸. Drony zwiększają szanse na znalezienie poszkodowanych w tzw. „złotej dobie” po zdarzeniu, gdyż mogą być wypuszczone natychmiast po przejściu zagrożenia i działać nawet w warunkach,

³⁴⁶ A. Chapman, Leveraging Big Data and AI for Disaster Resilience and Recovery, Texas A&M University College of Engineering News, <https://engineering.tamu.edu/news/2023/06/leveraging-big-data-and-ai-for-disaster-resilience-and-recovery.html>, [dostęp: 22.09.2025].

³⁴⁷ Tamże.

³⁴⁸ E. Yucesoy, B. Balcik, E. Coban, The role of drones in disaster response: A literature review of operations research applications, *International Transactions in Operational Research*, 32(2), 2024, s. 981-1025. <https://doi.org/10.1111/itor.13484>

w których załogowe śmigłowce nie mogłyby operować (np. wąskie kaniony, bardzo niska wysokość lotu). Przykładem spektakularnej akcji z użyciem drona SAR była operacja poszukiwawcza po ogromnym osuwisku w Gjerdrum w Norwegii (2020 r.) – duży dron DJI Matrice z kamerą termalną pomógł tamtejszym służbom przeczesać niestabilny teren osuwiska i zlokalizować ocalałych, co zostało odnotowane jako kluczowe wsparcie akcji. Co więcej, drony mogą przekazywać poszkodowanym środki pierwszej potrzeby zanim dotrą ratownicy – np. zrzucając pakiety z wodą, radiotelefonem czy apteczką.

- Transport i dostarczanie zaopatrzenia: Choć główny nacisk położono na rozpoznanie i poszukiwanie, warto wspomnieć, że drony są także wykorzystywane do dostarczania leków i sprzętu medycznego w trudno dostępne miejsca. W sytuacjach kryzysowych, gdy tradycyjna logistyka jest utrudniona (np. zerwane mosty, blokady drogowe), dron może przenieść niewielki ładunek szybko i bez konieczności udziału personelu. Organizacja Lekarze bez Granic (MSF) już w 2014 r. zastosowała drony do transportu próbek medycznych i materiałów do diagnozowania gruźlicy między odległymi wioskami w Papui-Nowej Gwinei – pozwoliło to przyspieszyć wykrycie i leczenie ogniska choroby w terenie pozbawionym dróg. Obecnie tego typu drony dostawcze są testowane m.in. do transportu krwi i szczepionek (np. słynny projekt Zipline w Rwandzie, gdzie drony regularnie dostarczają krew do klinik oddalonych od centrów krwiodawstwa). W kontekście klęsk żywiołowych drony mogą donieść leki, żywność, koce czy nadajniki radiowe do odizolowanych grup poszkodowanych zanim utworze się drogę lądową.

Zastosowanie dronów w sytuacjach nadzwyczajnych przynosi wiele korzyści. Przede wszystkim znacząco skraca czas pozyskania informacji o sytuacji – podczas gdy kiedyś trzeba było czekać na zdjęcia satelitarne lub wysłać patrole naziemne, dziś dron w ciągu kilkunastu minut od zdarzenia może przekazać sztabowi kryzysowemu obraz z centrum zniszczeń. Po drugie, zwiększa bezpieczeństwo ratowników, którzy nie muszą osobiście zapuszczać się w niezbadany, potencjalnie niebezpieczny teren – dron jako pierwszy „ogłąda” miejsce zdarzenia z powietrza. Badanie przeprowadzone

w straży pożarnej miasta Norfolk (USA) wykazało, że wykorzystanie bezzałogowych maszyn do oceny uszkodzeń jest wysoce korzystne, ponieważ pozwala uzyskać potrzebne informacje przy minimalnej ekspozycji ludzi na zagrożenie³⁴⁹. Raport ten zalecał tamtejszej straży zakup drona i odpowiednie przeszkolenie personelu, argumentując, iż w ten sposób „można sprawniej przeprowadzić inspekcję zniszczeń, jednocześnie trzymając ratowników z dala od niebezpiecznych obszarów”³⁵⁰. Inną zaletą jest dokładność i jakość danych – współczesne drony mogą przenosić bardzo dobre kamery, a także inne czujniki (np. LiDAR do skanowania 3D terenu, detektory promieniowania, czujniki chemiczne), dostarczając bogatych informacji, które trudno uzyskać inaczej.

Należy jednak pamiętać o ograniczeniach i wyzwaniach związanych z użyciem dronów. Techniczne ograniczenia to m.in. ograniczony czas lotu i zasięg – typowe quadcoptery mogą pozostawać w powietrzu kilkadziesiąt minut i muszą wracać na wymianę baterii, co utrudnia długotrwałe misje. Również warunki pogodowe stanowią barierę: silny wiatr, ulewny deszcz czy zadymienie mogą uziemić drony w krytycznym momencie. Kolejna kwestia to infrastruktura łączności – aby dron mógł przekazywać obraz w czasie rzeczywistym lub być sterowany na duże odległości, potrzebne jest stabilne połączenie (radio, sieć komórkowa lub satelitarna). W obszarach dotkniętych katastrofą infrastruktura telekomunikacyjna bywa zniszczona, co może ograniczyć zasięg operowania dronów. Paradoksalnie, drony mogą jednak pomóc i w tym aspekcie, gdyż istnieją modele pełniące rolę powietrznych przekazników komunikacyjnych – unoszą one tymczasowo nadajniki, tworząc ad-hoc sieć dla ratowników³⁵¹. Wreszcie, pozostają kwestie prawne i społeczne: przepisy wielu krajów limitują dopuszczalne pułapy lotu dronów, strefy ich użycia czy konieczność uzyskania pozwoleń (np. od lotnictwa cywilnego). Trzeba także uwzględnić prywatność – mieszkańcy mogą negatywnie reagować na drony filmujące ich posesje, nawet w kontekście akcji ratunkowej.

³⁴⁹ N. Perry, *Examining the Use of Unmanned Aerial Devices to Conduct Damage Assessment in the City of Norfolk*, Executive Fire Officer Program, U.S. Fire Administration, FEMA, Emmitsburg (MD), 2017.

³⁵⁰ Tamże.

³⁵¹ FSD (Fondation Suisse de Déminage), *Drones in Humanitarian Action – A Guide to the Use of Airborne Systems in Humanitarian Crises*, Swiss Foundation for Mine Action, <https://www.updwg.org/wp-content/uploads/2019/04/Drones-in-Humanitarian-Action.pdf#page=3&zoom=auto,-272,559>, [dostęp: 22.09.2025].

Wszystkie te czynniki wymagają opracowania jasnych procedur użycia dronów przez służby. Pomimo wyzwań, trend użycia dronów w bezpieczeństwie jest wyraźnie rosnący. Literatura z 2024 r. odnotowuje gwałtowny wzrost zainteresowania tą tematyką i wskazuje, że drony stały się integralnym elementem logistyki humanitarnej oraz operacji ratunkowych³⁵². Można oczekiwać, że wraz z rozwojem technologii (dłuższy czas lotu, autonomia AI) i lepszym uregulowaniem prawnym, ich rola będzie jeszcze większa.

Ostatnim filarem omawianym w niniejszym rozdziale jest analityka danych, w tym analiza big data (wielkich zbiorów danych), która w ostatnich latach w istotny sposób przekształca podejście do prognozowania zagrożeń oraz wspomagania procesów decyzyjnych w czasie rzeczywistym. Upowszechnienie czujników środowiskowych, smartfonów oraz mediów społecznościowych spowodowało, że dostępne są ogromne wolumeny danych dotyczących niemal wszystkich aspektów życia społecznego i stanu środowiska. Miasta i społeczności generują nieprzerwanie strumienie danych pochodzących m.in. z kamer monitoringu ruchu ulicznego, sygnałów GPS z urządzeń mobilnych mieszkańców, czujników pogodowych i hydrologicznych, liczników energii, a także z treści publikowanych w mediach społecznościowych. Analityka big data ukierunkowana jest na przetwarzanie i integrację tych informacji oraz ich przekształcenie w relewantne, operacyjne wnioski na potrzeby zarządzania bezpieczeństwem. W literaturze przedmiotu można wyróżnić trzy główne obszary zastosowań big data w kontekście sytuacji kryzysowych: prognozowanie zagrożeń, analizę zachowań ludności oraz wsparcie decyzji w czasie rzeczywistym. Prognozowanie i wczesne wykrywanie zagrożeń. Zastosowanie zaawansowanych algorytmów uczenia maszynowego do analiz historycznych i bieżących danych pozwala coraz trafniej przewidywać wystąpienie zagrożeń oraz skalę ich potencjalnych konsekwencji. Przykładem jest wykorzystanie sztucznej inteligencji do prognozowania awarii infrastruktury podczas klęsk żywiołowych. Zespół badawczy z Texas A&M University opracował modele AI, które na podstawie danych z huraganu Harvey (2017 r.) przewidują m.in. odcinki dróg narażone na zalanie podczas powodzi miejskiej. Opracowany głęboki model uczenia

³⁵² E. Yucesoy, B. Balcik, E. Coban, The role of drones in disaster response: A literature review of operations research applications, *International Transactions in Operational Research*, 32(2), 2024, s. 981-1025. <https://doi.org/10.1111/itor.13484>

się osiąga bardzo wysoką trafność (rzędu 98%) w identyfikacji ulic, które będą nieprzejezdne w najbliższych godzinach podczas intensywnych opadów. Informacje tego typu umożliwiają wcześniejsze zamykanie zagrożonych tras oraz kierowanie ruchu na alternatywne, bezpieczniejsze ciągi komunikacyjne. Inny model z tego samego projektu służy do prognozowania awarii sieci energetycznej i przerw w dostawach energii elektrycznej na podstawie danych o infrastrukturze oraz parametrach zjawisk ekstremalnych. Podobne podejścia wykorzystywane są w modelowaniu ryzyka pożarów lasów – poprzez analizę danych meteorologicznych, wilgotności roślinności oraz historii pożarów algorytmy wskazują obszary o podwyższonym ryzyku wystąpienia pożaru w określonym horyzoncie czasowym. W takich zastosowaniach istotną rolę odgrywają dane satelitarne (obrazy termiczne, wskaźniki wysuszenia roślin) oraz sensory naziemne (np. stacje meteorologiczne). Analityka predykcyjna umożliwia dzięki temu wcześniejszą alokację zasobów (np. patroli lotniczych) na obszary najbardziej zagrożone, zanim dojdzie do materializacji ryzyka. Szczególną kategorią zagrożeń, w których big data znajduje szerokie zastosowanie, są zagrożenia zdrowotne, w tym epidemie. Analiza dużych strumieni danych (np. zapytań internetowych dotyczących objawów chorobowych, wpisów w mediach społecznościowych, nietypowych wzorców zakupów leków) może umożliwiać identyfikację wczesnych sygnałów rozwoju epidemii jeszcze przed oficjalnym raportowaniem przypadków. Przykładem jest projekt Google Flu Trends, którego celem było prognozowanie nasilenia zachorowań na grypę w oparciu o dane z wyszukiwarki internetowej. Chociaż projekt ten ostatecznie okazał się obarczony istotnymi ograniczeniami, dobrze ilustruje koncepcję tzw. cyfrowych śladów (digital traces) pozostawianych przez użytkowników, które mogą sygnalizować pojawienie się zagrożenia. Współcześnie rozwijane są bardziej zaawansowane modele, integrujące wiele źródeł danych (np. mobilność na podstawie GPS, raporty medyczne, dane meteorologiczne), wykorzystywane do predykcji kolejnych fal COVID-19 oraz innych chorób zakaźnych. Istotnym z praktycznego punktu widzenia obszarem zastosowań big data jest wykorzystanie danych z urządzeń mobilnych oraz mediów społecznościowych do badania reakcji i zachowań ludności w sytuacjach zagrożenia. Tradycyjnie wiedza na temat tego, jak ludzie reagują na alarmy, jak przebiega ewakuacja oraz jakie są wzorce powrotu po zdarzeniu, opierała się

na badaniach ankietowych prowadzonych po fakcie lub na modelach teoretycznych. Obecnie, dzięki anonimowym danym lokalizacyjnym tysięcy urządzeń mobilnych, możliwe jest empiryczne odtworzenie rzeczywistych wzorców przemieszczania się ludności. Przykładem jest badanie ewakuacji podczas tsunami w Japonii w 2024 r., w którym analiza danych GPS z aplikacji mobilnych ujawniła nie tylko bardzo szybkie rozpoczęcie ewakuacji, lecz także fakt, że część mieszkańców zaczynała powrót do domów już 20-100 minut po trzęsieniu ziemi, czyli przed oficjalnym odwołaniem alarmu³⁵³. Jest to cenna informacja dla służb odpowiedzialnych za bezpieczeństwo, wskazująca na tendencję do skracania czasu przebywania w schronieniach, co w przypadku zagrożenia kolejnymi falami tsunami mogłoby prowadzić do poważnych konsekwencji. Innymi słowy, analityka big data pozwoliła zidentyfikować wzorzec zachowania, który mógłby pozostać niewidoczny w klasycznych badaniach ankietowych. Wykorzystanie zagregowanych danych z sieci komórkowych było również stosowane do mapowania ruchów ludności po katastrofach naturalnych. Po trzęsieniu ziemi na Haiti w 2010 r. organizacja Flowminder przeanalizowała anonimowe dane od operatora sieci komórkowej, aby oszacować kierunki przemieszczania się uchodźców wewnętrznych z Port-au-Prince, co pozwoliło organizacjom humanitarnym lepiej ukierunkować działania pomocowe. Podobne analizy prowadzono m.in. po trzęsieniu ziemi w Nepalu w 2015 r., co dowodzi, że dane telekomunikacyjne mogą służyć jako narzędzie monitorowania przemieszczeń ludności po katastrofie. W przypadku ewakuacji prewencyjnej (np. przed nadejściem huraganu) analiza lokalizacji smartfonów umożliwia oszacowanie odsetka mieszkańców, którzy opuścili obszar zagrożony, kierunków ich przemieszczeń oraz identyfikację osób pozostających na miejscu wbrew zaleceniom ewakuacji. Jest to informacja o dużym znaczeniu dla władz, które mogą w odpowiedzi podejmować dodatkowe działania, np. kierować komunikaty SMS do osób, które nie zastosowały się do zaleceń. Big data pozwala również analizować przygotowania ludności przed wystąpieniem katastrofy. Wykorzystywano także zagregowane dane lokalizacyjne do zbadania wzorców zaopatrywania się mieszkańców Houston przed huraganem Harvey.

³⁵³ F. Makinoshima, S. Yotsui, S. Sato, F. Imamura, Large-scale geolocation data reveal evacuation behaviour during the 2024 Noto Peninsula earthquake and tsunami, *Communications Earth & Environment*, 6, 891, 2025. <https://doi.org/10.1038/s43247-025-02819-8>

Analiza liczby wizyt w sklepach spożywczych, aptekach oraz na stacjach benzynowych ujawniła zróżnicowanie przestrzenne w intensywności gromadzenia zapasów – wskazano dzielnice, w których działania przygotowawcze rozpoczęto wcześniej i prowadzono intensywniej, oraz obszary, gdzie reakcja była opóźniona. Co istotne, wyniki badania sugerowały, że społeczności o niższym statusie ekonomicznym angażowały się w przygotowania bardziej intensywnie niż społeczności zamożniejsze, co interpretowano jako efekt ograniczonych alternatywnych możliwości ochrony (np. brak generatorów, słabsze zabezpieczenia budynków) i większego znaczenia klasycznego gromadzenia zapasów. Tego typu analizy pozwalają identyfikować obszary niedostatecznie przygotowane oraz kierować tam działania informacyjne bądź dodatkowe zasoby przed wystąpieniem katastrofy. Oprócz danych telekomunikacyjnych istotnym źródłem informacji o zachowaniach ludności w warunkach kryzysu są media społecznościowe. W czasie katastrof użytkownicy publikują setki tysięcy postów, opisując obserwowane zjawiska, zgłaszając potrzeby i wyrażając emocje. Analiza tych nieustrukturyzowanych danych (tekstów, zdjęć, nagrań) stała się odrębnym obszarem badawczym określanym jako social sensing. Przy użyciu technik big data oraz narzędzi przetwarzania języka naturalnego (NLP) analizuje się platformy takie jak X, Facebook czy Instagram w poszukiwaniu informacji przydatnych z punktu widzenia zarządzania kryzysowego. Przykładowo, algorytmy klasyfikujące treść wpisów potrafią filtrować wiadomości pod kątem sygnałów świadczących o poważnych zniszczeniach lub ofiarach, dzięki czemu centra zarządzania kryzysowego mogą identyfikować prośby o pomoc z określonych lokalizacji, nawet jeśli nie zostały one zgłoszone oficjalnymi kanałami. Inne narzędzia analizują publikowane zdjęcia – np. po przejściu tornada fotografie zniszczonych budynków zamieszczane przez świadków mogą zostać automatycznie geolokalizowane i przekazane służbom do weryfikacji. Media społecznościowe pełnią ponadto funkcję swoistego barometru nastrojów społecznych – analiza dużej liczby wpisów pozwala badać poziom niepokoju, zaufanie do władz oraz skalę występowania plotek i dezinformacji. Ta ostatnia kwestia ma szczególne znaczenie: analityka big data jest wykorzystywana do identyfikacji i ograniczania zjawiska misinformacji podczas kryzysu, m.in. poprzez wykrywanie najczęściej rozpowszechnianych

falszywych treści i przekazywanie informacji o nich platformom oraz odpowiednim służbom.

Wspomaganie procesów decyzyjnych i zarządzanie w czasie rzeczywistym stanowi naturalne rozwinięcie opisanych wcześniej zastosowań analityki big data. Zastosowania te – od prognozowania po monitorowanie zachowań – służą zasadniczo temu, aby dostarczyć decydującym możliwie pełny i aktualny obraz sytuacji, umożliwiając podejmowanie adekwatnych decyzji pod presją czasu. W operacyjnym zarządzaniu kryzysowym coraz powszechniej wykorzystuje się zaawansowane platformy analityczne i wizualizacyjne, które integrują w czasie rzeczywistym zróżnicowane źródła danych. Obejmują one rozbudowane panele informacyjne (dashboards), prezentujące m.in. dane z czujników Internetu Rzeczy (np. poziomy wody, odczyty sejsmiczne, wskazania detektorów skażeń), dane GIS (mapy zagrożeń, lokalizacje sił i środków), informacje pochodzące z mediów społecznościowych (np. zgrupowane zgłoszenia dotyczące potrzeb pomocy) oraz wyniki modeli prognostycznych (np. przewidywana trajektoria rozprzestrzeniania się chmury toksycznej). Analizy big data mogą wspierać proces decyzyjny poprzez generowanie rekomendacji, takich jak wskazywanie optymalnych lokalizacji punktów pomocy na podstawie analizy rozmieszczenia poszkodowanych i stanu sieci drogowej czy też formułowanie priorytetów działań ratowniczych w oparciu o symulacje przewidywanych skutków zaniechania interwencji w określonym czasie. W warunkach dynamicznie rozwijających się zdarzeń, takich jak powódzie, huragany czy ataki terrorystyczne, automatyczna analiza strumieni danych jest w stanie wykryć nietypowe wzorce szybciej niż obserwator ludzki. Przykładowo, system monitoringu miejskiego może na podstawie odczytów z kamer oraz danych z aplikacji transportowych zasygnalizować nagłe zablokowanie się trasy ewakuacyjnej, kierując uwagę sztabu kryzysowego na potencjalne źródło zaburzeń (np. wypadek, nieplanowany zator). Innym przykładem jest monitorowanie zużycia wody i energii w budynkach – gwałtowny spadek zapotrzebowania może wskazywać, że dany obszar został opuszczony przez mieszkańców, co z kolei pozwala weryfikować skuteczność przeprowadzonej ewakuacji. Kluczowe znaczenie ma integracja różnych typów danych w jednym środowisku analitycznym. Zróżnicowane czujniki i źródła danych odzwierciedlają swoiste „tętno” społeczności, natomiast zadaniem analityki jest scalenie tych

sygnałów i przekształcenie ich w spójną informację użyteczną dla zarządzania kryzysowego. W praktyce coraz większa liczba centrów zarządzania kryzysowego inwestuje w rozwiązania klasy big data. Przykładem może być system HHS emPOWER rozwijany w Stanach Zjednoczonych po doświadczeniach huraganu Katrina, który integruje dane medyczne, socjalne i infrastrukturalne w celu identyfikacji osób szczególnie narażonych podczas katastrof (np. pacjentów uzależnionych od aparatury zasilanej energią elektryczną) i umożliwienia im priorytetowego wsparcia. Inne rozwiązania, takie jak platformy typu IBM Watson for Disaster Response, wykorzystują sztuczną inteligencję do wspomagania operacji ratunkowych, m.in. poprzez analizę obrazowań satelitarnych i treści z mediów społecznościowych w celu określenia obszarów największych zniszczeń oraz identyfikacji najpilniejszych potrzeb ludności. Rozwój i wdrażanie tego rodzaju rozwiązań wiąże się jednak z szeregiem wyzwań. Zasadnicze znaczenie ma zapewnienie ochrony prywatności oraz bezpieczeństwa przetwarzanych danych, w szczególności danych lokalizacyjnych i informacji pochodzących z mediów społecznościowych. Konieczne jest stosowanie odpowiednich metod anonimizacji i pseudonimizacji, a także jasnych ram prawnych regulujących dostęp do danych i ich wykorzystanie. Istotnym problemem jest również jakość danych: algorytmy analityczne mogą generować obciążone błędem wnioski, jeżeli dane wejściowe są niepełne, stroniczne lub niereprezentatywne (np. próbki z mediów społecznościowych mogą słabo odzwierciedlać sytuację grup wykluczonych cyfrowo). Wyzwaniem pozostaje ponadto interoperacyjność systemów i standardów danych, warunkująca sprawną wymianę informacji pomiędzy różnymi podmiotami odpowiedzialnymi za bezpieczeństwo. Mimo tych ograniczeń obserwuje się wyraźny trend przesuwania punktu ciężkości w kierunku podejmowania decyzji opartych na danych. Analityka big data nie zastępuje człowieka w procesie decyzyjnym, lecz stanowi istotne wsparcie, zwiększając trafność, przejrzystość i szybkość reakcji. Umożliwia ona przejście od modelu zarządzania o charakterze przede wszystkim reaktywnym do podejścia proaktywnego, polegającego na przewidywaniu zagrożeń zanim osiągną pełną skalę, precyzyjnym kierowaniu zasobów tam, gdzie są najbardziej potrzebne, oraz systematycznym uczeniu się na podstawie kumulowanych doświadczeń utrwalonych w danych. Jak wskazują Akter i Wamba, big data staje się jednym z kluczowych komponentów

nowoczesnego zarządzania katastrofami, oferując nowe perspektywy analizy problemów i umożliwiając podejmowanie lepiej uzasadnionych decyzji w sytuacjach kryzysowych³⁵⁴.

Technologie GIS, bezzałogowe statki powietrzne oraz analityka big data coraz częściej funkcjonują w sposób synergiczny, tworząc zintegrowany ekosystem wsparcia bezpieczeństwa. Systemy GIS zapewniają platformę do organizowania i prezentacji informacji przestrzennych, drony dostarczają aktualnych danych obserwacyjnych z obszarów trudno dostępnych lub niebezpiecznych, natomiast narzędzia big data i sztucznej inteligencji umożliwiają prowadzenie zaawansowanych analiz i prognoz. Wspólnie rozwiązania te usprawniają kolejne fazy zarządzania kryzysowego – od identyfikacji zagrożeń, poprzez planowanie i reagowanie, aż po etap odbudowy. Co istotne, nie są to wyłącznie koncepcje o charakterze futurystycznym, lecz technologie już obecne w praktyce (często w formie projektów pilotażowych), które przyczyniają się do podnoszenia poziomu bezpieczeństwa. Można oczekiwać, że ich znaczenie będzie nadal wzrastać, zwłaszcza w powiązaniu z dalszym rozwojem sztucznej inteligencji oraz Internetu Rzeczy. Z tego względu instytucje odpowiedzialne za bezpieczeństwo publiczne powinny inwestować zarówno w infrastrukturę techniczną i oprogramowanie, jak i w rozwój kompetencji w zakresie analizy danych, aby w pełni wykorzystać potencjał tych technologii w interesie społecznym.

4.4. Planowanie zasobów i logistyka w sytuacjach kryzysowych

Sprawne zarządzanie zasobami i logistyka należą do kluczowych elementów skutecznego reagowania kryzysowego. Badania wskazują, że nawet około 80% działań ratunkowych ma charakter logistyczny³⁵⁵. W obliczu rosnącej częstości i skali katastrof – liczba zdarzeń kryzysowych wzrosła

³⁵⁴ S. Akter, S. F. Wamba, Big data and disaster management: a systematic review and agenda for future research, *Annals of Operations Research*, 283(1), 2019, s. 939-959. <https://doi.org/10.1007/s10479-017-2584-2>

³⁵⁵ L. N. Van Wassenhove, Humanitarian aid logistics: supply chain management in high gear, *Journal of the Operational Research Society*, 57(5), 2006, s. 475-489. <https://doi.org/10.1057/palgrave.jors.2602125>

z około 220 rocznie w połowie lat 90. do około 350-400 obecnie³⁵⁶ – planowanie zasobów nabiera szczególnego znaczenia. Zasoby w kontekście zarządzania kryzysowego obejmują zarówno ludzi (siły), sprzęt i materiały (środki), rezerwy dóbr (zapas), jak i środki transportu. Celem planowania jest zapewnienie, aby właściwe zasoby znalazły się we właściwym miejscu i czasie, pomimo chaosu, ograniczeń infrastrukturalnych i niepewności towarzyszących katastrofom. W takim ujęciu planowanie zasobów stanowi integralny element logistyki kryzysowej, zorientowanej na zapewnienie ciągłości działań ratowniczych oraz zaspokojenie podstawowych potrzeb poszkodowanej ludności.

Kluczowym wymiarem planowania jest zarządzanie zasobami ludzkimi. Skuteczne reagowanie kryzysowe wymaga zaangażowania odpowiednio przygotowanych sił: służb ratowniczych (straż pożarna, ratownictwo medyczne, policja, wojsko itp.) oraz wolontariuszy, a także ich właściwej koordynacji. Planowanie zasobów ludzkich obejmuje określenie zapotrzebowania na personel, zapewnienie jego dostępności i gotowości do działania, a także przygotowanie pod względem kompetencji (szkolenia, ćwiczenia), wyposażenia oraz odporności psychofizycznej (rotacje, wsparcie psychologiczne). W warunkach dużej katastrofy lokalne służby szybko osiągają kres własnych możliwości, dlatego niezbędne jest uruchomienie mechanizmów wsparcia zewnętrznego – zarówno krajowego (np. siły z innych regionów, Gwardia Narodowa w przypadku USA – ok. 50 000 żołnierzy zmobilizowanych po huraganie Katrina)³⁵⁷, jak i międzynarodowego (np. zespoły poszukiwawczo-ratownicze INSARAG). Planowanie sił musi obejmować także przygotowanie ram prawnych i organizacyjnych przyjmowania takiego wsparcia (ułatwione procedury wjazdowe, jasny podział kompetencji). Istotnym elementem jest współpraca z organizacjami pozarządowymi i społecznymi. Podkreśla się potrzebę pełnego wykorzystania potencjału stowarzyszeń, ochotniczych straży pożarnych, grup ratowniczych, harcerzy

³⁵⁶ S. Negi, Humanitarian logistics challenges in disaster relief operations: A humanitarian organisations' perspective, *Journal of Transport and Supply Chain Management*, 16, 2022, e1167. <https://doi.org/10.4102/jtscm.v16i0.691>

³⁵⁷ C. Edwards, Hurricane Katrina: Remembering the Federal Failures, Cato Institute, Cato at Liberty, 2015.

itp.³⁵⁸ Spontaniczni wolontariusze, którzy masowo zgłaszają się do pomocy, powinni zostać włączeni do uporządkowanego systemu – z rejestracją, przydziałem ról i koordynacją – tak, aby stanowili realne wsparcie, a nie źródło dodatkowego chaosu³⁵⁹. Niezbędne jest również przygotowanie przejrzystych struktur dowodzenia i systemów łączności między różnymi grupami personelu. Zastosowanie systemów typu Incident Command System (ICS) lub ich krajowych odpowiedników pozwala jasno zdefiniować hierarchię, kompetencje i zakres odpowiedzialności. Brak takiej klarowności, co pokazują doświadczenia z huraganu Katrina, skutkuje „niepewnością, kto dowodzi” i dublowaniem zadań, a tym samym obniżeniem efektywności wykorzystania zasobów ludzkich. Równoległe z siłami ludzkimi, niezbędne jest odpowiednie zarządzanie środkami technicznymi – sprzętem i materiałami. Planowanie w tym obszarze obejmuje inwentaryzację dostępnego wyposażenia, budowę rezerw sprzętowych oraz przygotowanie procedur szybkiego rozdysponowania środków w miejsca, gdzie są najbardziej potrzebne. Do typowych kategorii środków zalicza się m.in. sprzęt ratowniczy (łodzie, pompy wysokiej wydajności, agregaty prądotwórcze, narzędzia hydrauliczne), sprzęt medyczny (zestawy pierwszej pomocy, aparaturę do segregacji medycznej, szpitale polowe), środki łączności (radiostacje, telefony satelitarne), sprzęt inżynierski (buldożery, dźwigi, koparki) oraz materiały budowlane do doraźnych napraw infrastruktury. W sytuacjach kryzysowych zapotrzebowanie na sprzęt specjalistyczny rośnie gwałtownie, a czas jego dostarczenia staje się czynnikiem krytycznym. Dlatego już na etapie przygotowań tworzy się rezerwy sprzętowe na poziomie państwa np. strategiczne rezerwy materiałowe gromadzone przez Rządową Agencję Rezerw Strategicznych oraz magazyny służb ratowniczych (np. kontenery logistyczne PSP). Planowanie wymaga określenia miejsc składowania sprzętu, zasad jego uruchamiania oraz dróg transportu na miejsce zdarzenia. Integracja systemów zaopatrzenia ma kluczowe znaczenie dla ograniczenia zarówno braków, jak i nadmiarów. Doświadczenia z huraganu Katrina ujawniły przypadki marnotrawstwa – m.in. nadmierne zamówienia lodu i wody przez FEMA, przy jednoczesnych

³⁵⁸ B. Pac, Istota zarządzania zabezpieczeniem logistycznym w sytuacjach kryzysowych i stanach nadzwyczajnych, *Ekonomiczne, społeczne i środowiskowe uwarunkowania logistyki*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 383, 2015, s. 132-153.

³⁵⁹ Z. Ciekanowski, J. Nowicka, H. Wyrębek, Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych, Warszawa, CeDeWu, 2017.

niedoborach innego sprzętu. Dlatego planowanie środków powinno być oparte na scenariuszach zagrożeń (np. odrębne plany dla powodzi, pożarów, epidemii), uwzględniających specyficzne kategorie niezbędnego wyposażenia. Niezbędne jest także zapewnienie alternatywnych źródeł zaopatrzenia na wypadek zniszczenia lokalnej infrastruktury – w tym mechanizmów wsparcia międzyregionalnego i międzynarodowego oraz możliwości sięgnięcia po zasoby sektora prywatnego (w tym ewentualną rekwizycję środków w stanach nadzwyczajnych). Warunkiem skuteczności jest utrzymywanie sprzętu w pełnej sprawności – systematyczne przeglądy, serwis i rotacja zasobów stanowią integralną część planowania logistycznego.

Kolejnym krytycznym obszarem jest zarządzanie zapasami dóbr podstawowych, w szczególności żywności, wody, leków, środków sanitarnych oraz paliwa. Zapewnienie odpowiedniego poziomu tych zapasów decyduje zarówno o przetrwaniu ludności dotkniętej kryzysem, jak i o ciągłości operacji ratowniczych. Planowanie obejmuje tworzenie rezerw oraz systemu dystrybucji dóbr w warunkach załamania standardowych łańcuchów dostaw. Państwowe rezerwy żywności i wody (w Polsce – m.in. w ramach Agencji Rezerw Strategicznych) powinny być projektowane z uwzględnieniem międzynarodowych standardów, takich jak zalecenia Sphere Project (np. co najmniej 2100 kcal żywności i 15 litrów wody na osobę na dobę). Równocześnie niezbędne są mechanizmy reglamentacji i priorytetyzacji – w warunkach niedoboru wprowadza się limity wydawanych racji oraz ścisłą kontrolę dystrybucji, aby ograniczyć marnotrawstwo i panikę oraz zapewnić w pierwszej kolejności zaopatrzenie najbardziej wrażliwych grup (niemowlęta, osoby chore, osoby starsze). Odrębną kategorię stanowią paliwa i inne materiały eksploatacyjne (paliwo do pojazdów i generatorów, gaz, środki smarne, tlen medyczny). Braki w tym obszarze mogą sparaliżować całą operację logistyczną, czego przykładem były trudności na Haiti w 2010 r., gdy część samolotów z pomocą nie dysponowała paliwem na powrót, co chwilowo zablokowało możliwości operacyjne lotniska. Stąd konieczne jest utrzymywanie zapasów paliwowych, zawieranie umów z dostawcami o priorytetowym zaopatrzeniu służb oraz stosowanie zasad priorytetyzacji (paliwo w pierwszej kolejności dla pojazdów ratowniczych, generatorów zasilających szpitale itp.). Szczególne wyzwania dotyczą logistyki leków i materiałów medycznych, które wymagają nie tylko szybkiego transportu, ale

i zachowania ciągłości łańcucha chłodniczego. Plany muszą zatem uwzględniać awaryjne rozwiązania w tym zakresie (mobilne chłodziarki, zasilanie awaryjne, alternatywnych dostawców).

Transport stanowi kluczowy element logistyki kryzysowej, warunkujący fizyczne przemieszczenie ludzi, sprzętu i zapasów do stref dotkniętych kryzysem. Planowanie zasobów transportowych dotyczy zarówno infrastruktury (drogi, mosty, linie kolejowe, porty, lotniska), środków transportu (pojazdy, statki, samoloty, śmigłowce), jak i organizacji przewozów (harmonogramy, konwoje, priorytety, korytarze humanitarne). Katastrofy często poważnie uszkadzają infrastrukturę – trzęsienia ziemi i powodzie niszczą mosty i drogi, huragany blokują porty i lotniska. Przykład Haiti w 2010 r., gdzie zniszczony port morski, uszkodzone lotnisko i nieprzejezdne drogi stworzyły poważne wąskie gardła dla napływającej pomocy, dobrze ilustruje skalę wyzwań. Plany logistyczne muszą przewidywać alternatywne trasy (objazdy, drogi niższej kategorii), możliwość użycia transportu powietrznego i wodnego oraz tworzenie tymczasowej infrastruktury (mosty powietrzne, przeprawy promowe, polowe pasy startowe). Na etapie przygotowania szczególnego znaczenia nabiera wzmocnienie infrastruktury krytycznej (np. wałów przeciwpowodziowych, zapasowych mostów w dyspozycji wojska). Zasoby transportowe obejmują flotę pojazdów ratowniczych, transport ciężki (ciężarówki, cysterny), pojazdy specjalistyczne (amfibie, wysokowodne pojazdy terenowe), tabor kolejowy oraz środki lotnicze (samoloty transportowe, śmigłowce). Planowanie określa ich liczbę, rozmieszczenie i tryb mobilizacji, z uwzględnieniem możliwości wykorzystania zasobów wojska oraz sektora prywatnego (firm transportowych). Organizacja transportu wymaga centralnej koordynacji – tworzy się struktury dyspozycyjne zarządzające ruchem konwojów, wydawaniem przepustek, ustalaniem okien czasowych i korytarzy humanitarnych. Szczególnym wyzwaniem jest tzw. „ostatnia mila” – dostarczenie pomocy bezpośrednio do poszkodowanych, zwłaszcza rozproszonych lub odciętych geograficznie. W tym obszarze konieczna jest elastyczność, włącznie z wykorzystaniem małych łodzi, pojazdów terenowych, a nawet transportu pieszo czy przy użyciu zwierząt jucznych,

wspomaganego magazynami pośrednimi zlokalizowanymi bliżej potencjalnych stref izolacji³⁶⁰.

Na tym tle logistyka kryzysowa (humanitarna) jawi się jako szczególny przypadek logistyki, funkcjonujący w warunkach wysokiej niepewności, presji czasu i niedoborów³⁶¹. Specyfika łańcucha dostaw w kryzysie polega na nagłym, nieregularnym, trudnym do oszacowania popycie na pomoc oraz ograniczonej, rozproszonej podaży zasobów. Klasyczne koncepcje minimalizacji zapasów czy just-in-time są w takich warunkach niewystarczające – kluczowe znaczenie zyskują redundancja, elastyczność i zwinność. Jak podkreśla Van Wassenhove, łańcuch dostaw w sytuacji awaryjnej musi być z natury adaptacyjny, zdolny do szybkiej zmiany planów, przekierowywania transportów oraz ścisłej współpracy między wszystkimi ogniwami³⁶². Logistyka kryzysowa obejmuje fazy przygotowania, reagowania i odbudowy, powiązane z klasycznym cyklem zarządzania kryzysowego. W fazie reagowania szczególne znaczenie ma segmentacja potrzeb różnych grup poszkodowanych (szpitale, ludność ogółem, dzieci, osoby przewlekle chore) oraz zdolność do działania zarówno w trybie „push” (wysyłka pomocy na podstawie doświadczeń i standardów, zanim spłyną pełne dane), jak i „pull” (dostosowanie do zgłaszanych potrzeb). Złożoność łańcuchów dostaw w kryzysie wynika m.in. z udziału wielu aktorów – organizacji międzynarodowych, agencji rządowych, wojska, NGO, firm prywatnych – co rodzi duże wyzwania koordynacyjne. Brak skoordynowanego zarządzania prowadzi do powstawania wąskich gardeł (infrastrukturalnych, magazynowych, informacyjnych, decyzyjnych), czego ilustracją są doświadczenia Haiti 2010 i innych dużych operacji humanitarnych³⁶³. W odpowiedzi rozwijane są struktury koordynacyjne, takie jak Logistics Cluster pod auspicjami WFP/ONZ, wspólne platformy wymiany danych czy standardowe procedury współpracy.

³⁶⁰ K. Sienkiewicz-Małyjurek, *Skuteczne zarządzanie kryzysowe*, Warszawa, Difin, 2015.

³⁶¹ A. Szymonik, *Logistyka w bezpieczeństwie*, Warszawa, Difin, 2011.

³⁶² L. N. Van Wassenhove, Humanitarian aid logistics: supply chain management in high gear, *Journal of the Operational Research Society*, 57(5), 2006, s. 475-489. <https://doi.org/10.1057/palgrave.jors.2602125>

³⁶³ V. Beiser, Organizing Armageddon: What We Learned From the Haiti Earthquake, *Wired*, <https://www.wired.com/2010/04/ff-haiti/>, [dostęp: 30.09.2025].

Istotnym dopełnieniem planowania zasobów jest współpraca z sektorem prywatnym. Prywatne przedsiębiorstwa – od globalnych operatorów logistycznych po sieci handlowe i lokalne firmy – dysponują zasobami, infrastrukturą i kompetencjami, które mogą znacząco zwiększyć efektywność logistyki kryzysowej. Współpraca ta przybiera formę partnerstw publiczno-prywatnych, darowizn rzeczowych, udostępniania usług i infrastruktury, a także wspólnego planowania na etapie przygotowań. Przykładem jest inicjatywa Logistics Emergency Team (LET) pod auspicjami Światowego Forum Ekonomicznego, w ramach której globalni operatorzy (UPS, DHL, Maersk i inni) udostępniają magazyny, flotę i ekspertów logistycznych w razie katastrof – w ciągu 20 lat LET wsparł kilkadziesiąt operacji w kilkudziesięciu krajach. W reakcji na kryzys humanitarny w Strefie Gazy w 2023 r. Maersk nieodpłatnie udostępnił magazyn w Jordaniі o powierzchni 5000 m², a UPS magazyn w Bejrucie o powierzchni 3400 m², służące jako huby dla tysięcy ton pomocy. Sieci handlowe i firmy produkcyjne mogą wykorzystywać swoje łańcuchy dostaw i sieci sklepów jako kanały dystrybucji pomocy, czego wzorcowym przykładem była reakcja Wal-Martu po huraganie Katrina – szybka mobilizacja zapasów, konwoje z pomocą i elastyczne decyzje lokalnych menedżerów. Coraz częściej współpraca ta ma charakter strategiczny: firmy uczestniczą w ćwiczeniach i planowaniu, przygotowują programy wolontariatu pracowniczego (np. DHL Disaster Response Team), udostępniają systemy IT do śledzenia dostaw i analiz danych. Światowe Forum Ekonomiczne podkreśla, że sektor prywatny może działać najefektywniej, gdy jego wkład jest przygotowany i skoordynowany ze społecznością humanitarną. Oznacza to potrzebę instytucjonalizacji partnerstw – jasnych porozumień zawieranych jeszcze w okresie „pokoju”, zamiast improwizowania dopiero w obliczu katastrofy.

Planowanie zasobów i logistyka w sytuacjach kryzysowych obejmują spójny, wielowymiarowy system zarządzania siłami ludzkimi, środkami technicznymi, zapasami, transportem oraz całym łańcuchem dostaw – z rosnącą rolą współpracy z sektorem prywatnym. W warunkach rosnącej liczby i intensywności katastrof, przy ograniczonych zasobach publicznych, logistyka kryzysowa staje się jednym z kluczowych obszarów profesjonalizacji systemów bezpieczeństwa. Integracja doświadczeń logistyki biznesowej i wojskowej z praktyką humanitarną, rozwój struktur koordynacyjnych oraz

wykorzystanie nowoczesnych technologii (GIS, drony, big data, AI) stanowią podstawę budowy bardziej odpornych, elastycznych i efektywnych łańcuchów dostaw w sytuacjach nadzwyczajnych.

4.5. Komunikacja i informacja w zarządzaniu kryzysowym

Komunikacja i informacja w zarządzaniu kryzysowym to obszar o krytycznym znaczeniu, obejmujący zarówno wymianę informacji wewnątrz struktur zarządzania, jak i komunikowanie się z otoczeniem zewnętrznym. Skuteczne reagowanie na kryzys wymaga sprawnej komunikacji pionowej i poziomej pomiędzy zaangażowanymi instytucjami³⁶⁴. Badania wskazują, że wysokie standardy koordynacji działań wielu podmiotów zależą właśnie od dobrze funkcjonujących kanałów komunikacji pionowej (hierarchicznej) oraz poziomej (między różnymi służbami i organizacjami). Oznacza to konieczność zapewnienia szybkiego przepływu informacji w górę i w dół struktury administracyjnej (np. od władz lokalnych do centralnych i odwrotnie) oraz między służbami na tym samym szczeblu – na przykład pomiędzy policją, strażą pożarną a zespołami ratownictwa medycznego działającymi na miejscu zdarzenia. Praktyka pokazuje, że braki w takiej komunikacji prowadzą do opóźnień, niespójnych działań, a nawet chaosu, dlatego budowanie procedur i systemów zapewniających płynny obieg informacji jest priorytetem^{365,366}. Olejnik podkreśla, że rzetelne informacje przekazywane we właściwym czasie usprawniają komunikację zarówno ze społeczeństwem, jak i pomiędzy współdziałającymi służbami w trakcie akcji kryzysowych³⁶⁷. Innymi słowy, jasny podział kompetencji informacyjnych oraz sprawne kanały łączności wewnętrznej (np. między centrami zarządzania kryzysowego

³⁶⁴ J. Nowicka, M. Chodyka, M. R. Chodkowski (red.), *Wyzwania w obszarze komunikacji i bezpieczeństwa*, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103243>

³⁶⁵ B. Kożuch, K. Sienkiewicz-Małyjurek, A. J. Kożuch, *Communication in local emergency management networks (Part 2)*, *International Journal of Contemporary Management*, 14(1), 2015, s. 91-104.

³⁶⁶ T. Olejnik, *Zarządzanie kryzysowe a komunikacja, czyli jak i kiedy informować ludzi*, *Security, Economy & Law*, 1(14), 2017, s. 37-46.

³⁶⁷ Tamże.

a służbami terenowymi) przekładają się na skuteczniejsze reagowanie w sytuacji zagrożenia.

Równie ważnym wymiarem jest komunikacja z ludnością, prowadzona we wszystkich fazach zarządzania kryzysowego – od prewencji, przez reagowanie, po fazę odbudowy. W okresie przedkryzysowym kluczowe jest informowanie i edukowanie społeczeństwa o potencjalnych zagrożeniach oraz procedurach postępowania (np. poprzez kampanie informacyjne), co buduje zaufanie i przygotowuje obywateli na ewentualne nadzwyczajne sytuacje. Gdy kryzys nadchodzi, niezbędne jest jak najszybsze przekazanie ostrzeżeń i zaleceń – szybkość komunikatu może zadecydować o skutecznej ewakuacji czy podjęciu właściwych działań ochronnych przez mieszkańców. Komunikaty kierowane do ludności muszą być przy tym jasne i zrozumiałe, tak, aby odbiorcy od razu pojęli ich sens i wiedzieli, co robić³⁶⁸. Unikanie specjalistycznego żargonu, stosowanie prostego języka i konkretnych zaleceń zwiększa szansę, że przekaz zostanie właściwie zrozumiany nawet w warunkach stresu. Ważna jest także empatia i tonalność komunikatów – okazywanie troski, współczucia ofiarom oraz uznanie emocji, jakich doświadcza społeczność, wpływa pozytywnie na odbiór informacji³⁶⁹. Ludzie w kryzysie potrzebują poczucia, że władze rozumieją ich obawy i cierpienie; taki empatyczny ton podnosi wiarygodność nadawcy komunikatu. Wreszcie, komunikacja z ludnością powinna wykorzystywać różnorodne kanały – od tradycyjnych mediów masowych (telewizja, radio, prasa) po nowoczesne platformy (media społecznościowe, aplikacje alarmowe, SMS-y). Zapewnienie wielokanałowego obiegu informacji gwarantuje dotarcie do najszerszego grona odbiorców, co ma znaczenie np. przy ostrzeganiu przed nagłym zagrożeniem³⁷⁰. Osoby czerpiące informacje wyłącznie z telewizji muszą otrzymać ten sam przekaz, co użytkownicy Internetu i mediów społecznościowych – tylko wtedy komunikacja kryzysowa będzie powszechna i skuteczna.

³⁶⁸ Rządowe Centrum Bezpieczeństwa, *Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie*, Warszawa, RCB, 2018.

³⁶⁹ W. T. Coombs, *Ongoing crisis communication: planning, managing, and responding*, 4th ed., Thousand Oaks, CA, Sage, 2015.

³⁷⁰ Rządowe Centrum Bezpieczeństwa, *Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie*, Warszawa, RCB, 2018.

W ramach komunikacji zewnętrznej szczególną rolę odgrywa współpraca z mediami masowymi oraz przemyślane prowadzenie przekazu medialnego. Media (telewizja, radio, portale informacyjne) są dla społeczeństwa podstawowym źródłem wiadomości o kryzysie, dlatego władze muszą ściśle współdziałać z dziennikarzami i redakcjami. Standardem jest wyznaczenie oficjalnego rzecznika prasowego lub zespołu prasowego, który staje się głównym komunikatorem kryzysowym i „twarzą” instytucji w mediach. Centralizacja przepływu informacji przez rzecznika zapewnia spójność – unika się sytuacji, w której różni przedstawiciele instytucji przekazują sprzeczne komunikaty. Zgodnie z wytycznymi, rzecznik prasowy powinien być włączony w wewnętrzny obieg informacji od samego początku kryzysu, tak, aby posiadał pełen obraz sytuacji i nie został zaskoczony przez media pytaniami, na które nie zna odpowiedzi. Rzecznik, mając dostęp do najświeższych danych, może rzetelnie informować opinię publiczną o rozwoju wydarzeń i działaniach zaradczych, a także odpowiednio interpretować „suche fakty” dla odbiorców. Kolejnym elementem jest utrzymywanie regularnych kontaktów z mediami – organizowanie briefingów i konferencji prasowych, wydawanie komunikatów dla prasy o ustalonych porach – co pozwala kontrolować bieg informacji i zaspokajać oczekiwanie społeczeństwa na wiadomości. Ważne jest przy tym nastawienie władz do mediów: nawet jeśli dziennikarze są dociekliwi lub krytyczni, powinni być traktowani jak partnerzy w misji informowania społeczeństwa, a nie jak przeciwnicy. Olejnik zauważa, że przedstawiciele instytucji nie mogą postrzegać mediów jako wrogów – media w istocie wspomagają działania kryzysowe, nagłaśniając ważne komunikaty, a ich przekaz może zbudować pozytywną reputację instytucji albo ją podważyć³⁷¹. Dlatego należy utrzymywać transparentność i udzielać mediom wyczerpujących, prawdziwych informacji nawet w dynamicznie zmieniających się okolicznościach. Proaktywna, otwarta komunikacja z prasą (np. szybkie dementowanie nieścisłych informacji, udostępnianie mediom materiałów z miejsca zdarzenia) przekłada się na lepsze poinformowanie społeczeństwa i ograniczenie rozwoju niepotrzebnych plotek. Spójna strategia medialna – z jednym głównym źródłem informacji w postaci

³⁷¹ T. Olejnik, Zarządzanie kryzysowe a komunikacja, czyli jak i kiedy informować ludzi, *Security, Economy & Law*, 1(14), 2017, s. 37-46.

rzecznika i skoordynowanym przekazem – jest obecnie uznawana za najlepszą praktykę w zarządzaniu kryzysowym³⁷².

Niezależnie od użytych kanałów, kluczowa jest odpowiednia jakość i forma samych komunikatów kryzysowych. Specjaliści wyodrębniają kilka fundamentalnych zasad, którymi należy kierować się przy formułowaniu komunikatów w sytuacji kryzysu. Po pierwsze – szybkość reakcji. Pierwszy komunikat powinien zostać przekazany możliwie jak najszybciej, najlepiej w ciągu tzw. „złotej godziny” od wystąpienia zdarzenia, aby zapobiec powstawaniu plotek i wypełnić próżnię informacyjną. Szybkie dostarczenie wstępnych informacji (choćby częściowych) pozwala opinii publicznej poczuć, że sytuacja jest pod kontrolą, a władze działają – brak oficjalnego głosu przez dłuższy czas sprzyja natomiast panice i rozprzestrzenianiu się niesprawdzonych teorii. Po drugie – prawdziwość i wiarygodność przekazu. W komunikacji kryzysowej absolutnym imperatywem jest mówienie prawdy: wszelkie próby ukrywania faktów lub podawania fałszywych informacji są nieetyczne i zwykle kończą się utratą zaufania, gdyż prędzej czy później prawda wychodzi na jaw. Instytucja informująca o kryzysie musi więc być źródłem rzetelnym – jeśli czegoś nie wie, powinna otwarcie to przyznać zamiast spekulować lub unikać komentarza. Po trzecie – empatia. Każdy komunikat powinien być formułowany z poszanowaniem wrażliwości odbiorców, w szczególności ofiar i ich rodzin. Wyrażenie współczucia, żalu czy solidarności z poszkodowanymi jest nie tylko etyczne, ale i skuteczne komunikacyjnie: jak pokazują analizy, komunikaty ukierunkowane na dobro ofiar i uznające ich cierpienie przyczyniają się do ograniczenia szkód wizerunkowych dla instytucji oraz łagodniejszego odbioru sytuacji przez społeczeństwo. Coombs podkreśla, że organizacje w kryzysie powinny najpierw zatroszczyć się o ludzi dotkniętych zdarzeniem, a dopiero potem o własny wizerunek – empatyczny ton przekazu buduje kapitał zaufania, który procentuje w dłuższej perspektywie³⁷³. Po czwarte – prostota języka. Treść komunikatów musi być klarowna i zrozumiała dla osób niemających specjalistycznej wiedzy. Zaleca się unikanie technicznego żargonu i długich,

³⁷² Rządowe Centrum Bezpieczeństwa, *Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie*, Warszawa, RCB, 2018.

³⁷³ W. T. Coombs, *Ongoing crisis communication: planning, managing, and responding*, 4th ed., Thousand Oaks, CA, Sage, 2015.

złożonych form – zamiast tego komunikat powinien przekazywać konkrety prostymi słowami. Im bardziej stresująca sytuacja, tym większe ryzyko niezrozumienia przekazu, dlatego prostota staje się warunkiem skuteczności. Po piąte – spójność informacji. Wszystkie kanały i osoby przekazujące oficjalne informacje (rzecznicy różnych służb, urzędy, profile instytucji w mediach społecznościowych) muszą przekazywać jednolite, uzgodnione komunikaty. Sprzeczne informacje pochodzące z różnych źródeł natychmiast obniżą wiarygodność i wywołają zamieszanie, stąd konieczna jest ścisła koordynacja przekazu. Rządowe Centrum Bezpieczeństwa zaleca m.in. ustalanie wspólnych kluczowych przekazów i przekazywanie ich do wiadomości wszystkich zaangażowanych rzeczników, co gwarantuje jednolitość informacji. Zasady szybkości, prawdy, empatii, prostoty i spójności stanowią obecnie kanon komunikacji kryzysowej, opisywany w licznych poradnikach oraz literaturze przedmiotu. Ich przestrzeganie zwiększa skuteczność przekazu, ułatwia odbiorcom zrozumienie sytuacji i sprzyja utrzymaniu zaufania do działań instytucji w obliczu kryzysu.

Coraz poważniejszym wyzwaniem związanym z komunikacją kryzysową jest dezinformacja i plotki. W dobie mediów społecznościowych fałszywe pogłoski mogą rozprzestrzeniać się błyskawicznie, zanim zostaną zweryfikowane, co potrafi zdestabilizować zarządzanie kryzysowe. Dlatego konieczny jest ciągły monitoring przestrzeni informacyjnej, zwłaszcza Internetu, w celu wychwytywania pojawiających się nieprawdziwych narracji. Jak wskazują badania, identyfikacja i szybkie zdementowanie fałszywych pogłosek to kluczowy element skutecznego reagowania – niekontrolowane plotki w warunkach wysokiej niepewności potrafią potęgować chaos i negatywne nastroje. Zeng podkreśla, że przy wysokiej niepewności informacyjnej w kryzysie organizacje muszą aktywnie zarządzać obiegiem informacji, natychmiast reagując na wszelkie nieprawdziwe doniesienia³⁷⁴. Oznacza to, że instytucje powinny proaktywnie korygować błędne informacje – np. poprzez wydawanie oficjalnych sprostowań, aktualizowanie FAQ na stronach internetowych, a także stanowcze wypowiedzi rzeczników w mediach, gdy

³⁷⁴ L. Zeng, K. Starbird, E. S. Spiro, Rumors at the speed of light? Modeling the rate of rumor transmission during crisis, w: Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Honolulu, IEEE, 2016, s. 1969-1978. <https://doi.org/10.1109/HICSS.2016.248>

tylko pojawi się szkodliwa plotka. Przydatne są specjalne narzędzia, takie jak dedykowane strony lub profile do walki z dezinformacją. Przykładem dobrej praktyki jest amerykańska agencja FEMA, która podczas klęsk żywiołowych tworzy na swojej stronie internetowej sekcje „Rumor Control”, gdzie na bieżąco zbiera najczęściej pojawiające się plotki i każdą z nich oficjalnie dementuje, podając jednocześnie fakty. Takie działanie pozwala uspokoić mieszkańców, zapobiega rozprzestrzenianiu się paniki i kieruje odbiorców do wiarygodnych źródeł. W Polsce podobną rolę odgrywają komunikaty Rządowego Centrum Bezpieczeństwa – np. podczas kryzysów RCB na swoich profilach w mediach społecznościowych prostuje popularne fake newsy i apeluje o sprawdzanie informacji w oficjalnych kanałach³⁷⁵. Studium przypadku pożaru katedry Notre Dame w 2019 r. ukazuje skalę wyzwania związanego z dezinformacją: w kilka chwil po nagłośnieniu pożaru w serwisach społecznościowych pojawiły się tysiące komentarzy i hipotez co do przyczyn zdarzenia, w tym niesprawdzone teorie o celowym podpaleniu katedry. Analiza tej sytuacji wykazała, że szybkie wdrożenie działań komunikacyjnych przez władze – w tym kategoryczne zdementowanie pogłosek o podpaleniu – pomogło opanować narrację publiczną i zapobiec eskalacji napięć społecznych. Oficjalne komunikaty francuskich władz i przedstawicieli Kościoła, podawane regularnie i w sposób transparentny, uspokoiły opinię publiczną i skierowały uwagę mediów na faktyczne ustalenia dochodzenia. Ogólnie rzecz biorąc, walka z dezinformacją opiera się nie tylko na reagowaniu tu i teraz, ale również na działaniu wyprzedzającym. Ważnym elementem jest edukacja społeczeństwa: podnoszenie świadomości na temat istnienia dezinformacji, uczenie krytycznego odbioru treści medialnych oraz promowanie nawyku sprawdzania komunikatów u źródeł (np. na oficjalnych stronach rządowych czy samorządowych) może znacząco ograniczyć podatność ludzi na fałszywe wiadomości³⁷⁶. Im bardziej świadomi odbiorcy, tym trudniej rozprzestrzeniać szkodliwe plotki – dlatego długofalowe programy informacyjne i kampanie społeczne dotyczące higieny informacyjnej stają się coraz ważniejszym komponentem zarządzania kryzysowego.

³⁷⁵ Rządowe Centrum Bezpieczeństwa, *Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie*, Warszawa, RCB, 2018.

³⁷⁶ A. Kielczykowska, *Badanie: 73 proc. Polaków uważa, że w mediach społecznościowych celowo rozprzestrzeniane są nieprawdziwe lub niedokładne informacje*, Nauka w Polsce – PAP, 2022.

Media cyfrowe zrewolucjonizowały krajobraz komunikacyjny, co stawia przed zarządzającymi kryzysami wyzwanie efektywnego wykorzystania zarówno mediów tradycyjnych, jak i społecznościowych. Oba typy mediów mają swoje unikalne właściwości i rolę do odegrania. Media tradycyjne (telewizja, radio, prasa) odznaczają się dużą wiarygodnością i nadal docierają do szerokiej publiczności – zwłaszcza do osób mniej aktywnych w Internecie – jednak ich cykl informacyjny bywa wolniejszy, a przepływ informacji jednokierunkowy. Media społecznościowe (Facebook, X, YouTube i in.) umożliwiają natomiast natychmiastowe przekazanie komunikatu i wejście w interakcję z odbiorcami w czasie rzeczywistym (np. poprzez komentarze, pytania od użytkowników), co czyni je niezwykle przydatnymi na etapie ostrzegania i bieżącego informowania o rozwoju wydarzeń. Dzięki mediom społecznościowym służby kryzysowe mogą np. w ciągu minut rozesłać ostrzeżenie o zagrożeniu na telefony mieszkańców danej okolicy, a także monitorować reakcje i potrzeby społeczne poprzez analizę wpisów użytkowników. Z drugiej strony, internetowy obieg informacji cechuje się brakiem kontroli redakcyjnej, co – jak wspomniano wyżej – sprzyja pojawianiu się niezweryfikowanych treści i plotek³⁷⁷. Tym samym media społecznościowe stanowią narzędzie o podwójnym skutku: są nieodzownym kanałem komunikacji kryzysowej, ale wymagają stałego nadzoru i szybkiego reagowania na potencjalnie nieprawdziwe treści. Media tradycyjne z kolei oferują przekaz bardziej uporządkowany i filtrowany – informacje podawane w głównych serwisach informacyjnych telewizji czy radia zazwyczaj zostały wcześniej potwierdzone i opracowane, co zwiększa ich rzetelność. W sytuacjach kryzysowych wiele osób oczekuje właśnie oficjalnych komunikatów w tradycyjnych mediach (np. konferencja prasowa premiera transmitowana w telewizji), zwłaszcza jeżeli kryzys budzi silne emocje i potrzeba autorytatywnego stanowiska władz. Synergia mediów polega na tym, by wykorzystywać mocne strony obu tych sfer – nowej i tradycyjnej. Najlepsze efekty przynosi prowadzenie komunikacji równoległe na wielu platformach, przy zachowaniu spójności treści. Informacje podawane na konferencji prasowej

³⁷⁷ L. Zeng, K. Starbird, E. S. Spiro, Rumors at the speed of light? Modeling the rate of rumor transmission during crisis, w: *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, Honolulu, IEEE, 2016, s. 1969-1978. <https://doi.org/10.1109/HICSS.2016.248>

powinny natychmiast pojawić się również na oficjalnym profilu danej instytucji w social media i w komunikacie na stronie internetowej, a ważne ostrzeżenia wysyłane SMS-em (np. Alert RCB) powinny być jednocześnie nagłaśniane przez stacje radiowe i telewizyjne. Taka zintegrowana strategia zapewnia, że każda grupa odbiorców – niezależnie od preferowanego medium – otrzyma ważny komunikat³⁷⁸. Oczywiście wdrożenie tego podejścia wymaga wcześniejszego przygotowania: opracowania listy kanałów komunikacji, harmonogramów przekazu oraz mechanizmów koordynacji, by uniknąć rozbieżności. RCB w swoich wytycznych kładzie nacisk na łączenie mediów starych i nowych oraz na ćwiczenie scenariuszy komunikacyjnych, w których informacje są równolegle dystrybuowane różnymi drogami³⁷⁹. W konsekwencji rola tradycyjnych i społecznościowych mediów w kryzysie nie powinna być postrzegana konkurencyjnie, lecz komplementarnie. Każdy z tych kanałów może wzmacniać przekaz drugiego – np. media społecznościowe mogą natychmiast wychwycić i skorygować błędne interpretacje pojawiające się na bieżąco, a media tradycyjne mogą dostarczyć pogłębiony, ekspercki komentarz i usystematyzować wiedzę o zajściu. Podejście łączące oba rodzaje mediów zwiększa zasięg i szybkość komunikacji kryzysowej, jednocześnie zachowując rzetelność i uporządkowanie informacji.

Informacja i komunikacja stanowią zatem fundament efektywnego zarządzania kryzysowego. W przeszłości element ten bywał niedoceniany – zdarzało się, że część decydentów wolała milczeć niż otwarcie komunikować o kryzysie – jednak doświadczenia wielu sytuacji zagrożeń wykazały, iż brak informacji lub chaotyczny przekaz mogą pogłębiać skutki kryzysu. Z kolei przemyślana, profesjonalna komunikacja potrafi realnie zmniejszyć skalę szkód, ograniczyć panikę, usprawnić akcje ratunkowe, a także ochronić wizerunek instytucji^{380,381}. Jest to możliwe tylko wtedy, gdy komunikacja obejmuje wszystkie omówione aspekty: sprawny obieg informacji między

³⁷⁸ A. Kielczykowska, Badanie: 73 proc. Polaków uważa, że w mediach społecznościowych celowo rozprzestrzeniane są nieprawdziwe lub niedokładne informacje, Nauka w Polsce – PAP, 2022.

³⁷⁹ Rządowe Centrum Bezpieczeństwa, Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie, Warszawa, RCB, 2018.

³⁸⁰ T. Olejnik, Zarządzanie kryzysowe a komunikacja, czyli jak i kiedy informować ludzi, *Security, Economy & Law*, 1(14), 2017, s. 37-46.

³⁸¹ W. T. Coombs, *Ongoing crisis communication: planning, managing, and responding*, 4th ed., Thousand Oaks, CA, Sage, 2015.

instytucjami (wewnętrzna koordynacja pionowa i pozioma), skuteczne informowanie ludności (szybkie, jasne i empatyczne komunikaty), udaną współpracę z mediami (transparentność i jeden spójny głos) oraz aktywne zarządzanie treściami w infosferze (zapobieganie dezinformacji). Komunikacja kryzysowa wyewoluowała obecnie w pełnoprawny komponent zarządzania kryzysowego, równorzędny innym działaniom operacyjnym. Kozuch i inni zauważają, że wysokie standardy reagowania są nierozzerwalnie związane z jakością komunikacji, traktuje zarządzanie informacją jako integralną część krajowego systemu bezpieczeństwa³⁸². Wnioski te prowadzą do konkluzji, że umiejętność skutecznego komunikowania się w kryzysie jest jednym z kluczowych czynników warunkujących powodzenie działań zaradczych – stanowi swoiste spoiwo łączące wszystkie elementy zarządzania kryzysowego w spójny, sprawnie działający system³⁸³.

³⁸² B. Kozuch, K. Sienkiewicz-Małyjurek, A. J. Kozuch, Communication in local emergency management networks (Part 2), *International Journal of Contemporary Management*, 14(1), 2015, s. 91-104.

³⁸³ Rządowe Centrum Bezpieczeństwa, *Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie*, Warszawa, RCB, 2018.

Rozdział V.

Zarządzanie kryzysowe w wymiarze lokalnym, krajowym i międzynarodowym

5.1. Zarządzanie kryzysowe w jednostkach samorządu terytorialnego

Zarządzanie kryzysowe w Polsce tworzy zintegrowany, wieloszczelowy system, obejmujący organy administracji publicznej od poziomu centralnego aż po gminy. Zgodnie z definicją ustawową jest to działalność organów administracji publicznej stanowiąca element kierowania bezpieczeństwem narodowym, polegająca na zapobieganiu sytuacjom kryzysowym, przygotowaniu się na ich wystąpienie, reagowaniu w przypadku ich zaistnienia oraz na odtwarzaniu infrastruktury i przywracaniu normalnego funkcjonowania po kryzysie³⁸⁴. W ramach systemu wyróżnia się trzy główne komponenty: organy zarządzania kryzysowego (podejmujące decyzje i realizujące zadania), organy opiniotawczo-doradcze (zespoły koordynujące i doradzające) oraz centra zarządzania kryzysowego (prowadzące stały monitoring i zapewniające łączność). Pionowa struktura kompetencji odpowiada zasadzie subsydiarności – każdy szczebel samorządu terytorialnego wykonuje zadania kryzysowe we własnym zakresie, a w razie przekroczenia jego możliwości zwraca się o wsparcie do poziomu wyższego. Jednocześnie funkcjonują mechanizmy koordynacji poziomej, zapewniające współpracę

³⁸⁴ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

między służbami, inspekcjami i podmiotami ratowniczymi na danym szczeblu oraz między administracją publiczną a podmiotami społecznymi (OSP, organizacje pozarządowe itp.).

Na poziomie centralnym najważniejszą rolę pełni Rada Ministrów z Prezesem Rady Ministrów na czele – odpowiada ona za kierowanie całością systemu zarządzania kryzysowego, w tym podejmowanie strategicznych decyzji i ogłaszanie stanów nadzwyczajnych w razie potrzeby. Rada Ministrów zatwierdza m.in. Krajowy Plan Zarządzania Kryzysowego oraz może uruchamiać rezerwy budżetowe na działania kryzysowe³⁸⁵. Organem pomocniczym rządu jest Rządowy Zespół Zarządzania Kryzysowego (RZZK) – międzyresortowy zespół opiniodawczo-doradczy, w skład którego wchodzi kluczo- wi ministrowie, przedstawiciele służb i instytucji państwowych właściwych w sprawach bezpieczeństwa. RZZK zapewnia skoordynowane wypracowanie rekomendacji i ocen sytuacji na potrzeby Premiera i Rady Ministrów w obliczu poważnych zagrożeń. Z kolei operacyjne wsparcie na szczeblu krajowym zapewnia Rządowe Centrum Bezpieczeństwa (RCB) – specjalistyczna jednostka podległa bezpośrednio Prezesowi Rady Ministrów. RCB pełni całodobowy dyżur, monitoruje i analizuje pojawiające się zagrożenia, obsługuje posiedzenia RZZK oraz odpowiada za sprawny obieg informacji między wszystkimi szczeblami administracji zaangażowanymi w reagowanie kryzysowe³⁸⁶. W sytuacji kryzysu o zasięgu krajowym RCB działa jako centrum koordynacyjne – zbiera dane od wojewodów, ministerstw i służb, przygotowuje raporty dla decydentów, a także uruchamia procedurę Alertu RCB (systemu SMSowego ostrzegania ludności). Na szczeblu centralnym funkcjonują również ministrowie resortowi oraz centralne organy administracji (np. Komendant Główny PSP), którzy w swoich działach odpowiadają za zarządzanie kryzysowe branżowo. Każdy minister tworzy w swoim resorcie centrum zarządzania kryzysowego oraz powołuje resortowy zespół zarządzania kryzysowego, aby zapewnić ciągłość monitorowania zagrożeń i koordynacji działań w obszarze swojej właściwości. Przykładowo Minister Infrastruktury odpowiada za plany ciągłości działania w transporcie,

³⁸⁵ Najwyższa Izba Kontroli, Informacja o wynikach kontroli: Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, Nr P/17/039, Warszawa, NIK, 2019.

³⁸⁶ Z. Ciekanowski, J. Nowicka, H. Wyřbek, Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych, Warszawa, CeDeWu, 2017.

a Minister Zdrowia – za reakcję na zagrożenia sanitarno-epidemiologiczne. Centralne organy utrzymują również łączność z analogicznymi strukturami zagranicą np. poprzez RCB w systemie UE integrującym centra kryzysowe państw członkowskich.

Kolejny szczebel stanowi poziom wojewódzki, na którym kluczową rolę odgrywa wojewoda jako przedstawiciel Rady Ministrów w terenie. Wojewoda jest ustawowo organem zarządzania kryzysowego na obszarze województwa. Do jego zadań należy m.in. ocena ryzyka wystąpienia zagrożeń na terenie województwa, opracowanie i aktualizacja Wojewódzkiego Planu Zarządzania Kryzysowego, kierowanie działaniami w przypadku sytuacji kryzysowych przekraczających możliwości poszczególnych powiatów, a także wnioskowanie do premiera o pomoc Sił Zbrojnych RP, gdy inne siły i środki okażą się niewystarczające³⁸⁷. Wojewoda koordynuje również realizację zadań z zakresu ochrony infrastruktury krytycznej na swoim terenie, wydając wytyczne i polecenia jej operatorom. Organem doradczym i koordynacyjnym jest Wojewódzki Zespół Zarządzania Kryzysowego (WZZK) złożony m.in. z kierowników wojewódzkich służb, inspekcji i straży (komendanci PSP, Policji, Państwowej Inspekcji Sanitarnej, itd.), przedstawicieli administracji zespolonej i niezespolonej, a w razie potrzeby także np. reprezentantów organizacji pozarządowych. WZZK, pod przewodnictwem wojewody, ocenia rozwój sytuacji, uzgadnia podział zadań między służbami oraz wydaje rekomendacje dla starostów i wójtów. Zaplecze wykonawcze stanowi Wojewódzkie Centrum Zarządzania Kryzysowego (WCZK), funkcjonujące zazwyczaj w strukturze urzędu wojewódzkiego (często w wydziale bezpieczeństwa i zarządzania kryzysowego). WCZK utrzymuje 24-godzinną gotowość, monitoruje bieżącą sytuację (np. stany rzek, prognozy pogody, zdarzenia na drogach), przyjmuje meldunki z powiatów i od służb, a w sytuacji kryzysu obsługuje pracę sztabu wojewody oraz zapewnia przepływ informacji do RCB. Wojewoda, realizując zasady polityki rządu w terenie, może wydawać polecenia organom samorządu terytorialnego (starostom, wójtom) w zakresie zapobiegania i zwalczania skutków klęsk żywiołowych i innych zagrożeń – takie polecenia, na mocy ustawy, podlegają niezwłocznemu

³⁸⁷ K. Pilarz, Specyfika relacji organów administracji publicznej z otoczeniem w sytuacjach kryzysowych, *Acta Universitatis Wratislaviensis, Przegląd Prawa i Administracji* CXI, 3802, 2017, s. 123-138. <https://doi.org/10.19195/0137-1134.111.9>

wykonaniu (nawet jeśli skutkują obciążeniem budżetu samorządu, koszty te są refundowane ze środków państwowych). Ważnym zadaniem wojewody jest również przekazywanie niższym szczeblom tzw. zaleceń do planów – po opracowaniu Wojewódzkiego Planu Zarządzania Kryzysowego wojewoda formułuje wnioski i zalecenia, które powinny zostać uwzględnione w planach powiatowych i gminnych, co służy zachowaniu spójności planowania³⁸⁸. Województwo stanowi też obszar, na którym w razie katastrof o dużej skali mogą być uruchamiane mechanizmy pomocy międzywojewódzkiej lub międzynarodowej – wojewoda wnioskuję do właściwych ministrów o wsparcie spoza regionu, np. dodatkowe siły PSP spoza województwa, jednostki wojskowe (na wniosek wojewody Minister Obrony Narodowej może skierować do akcji pododdziały Sił Zbrojnych) lub uruchomienie unijnego mechanizmu ochrony ludności.

Poziom powiatowy w zarządzaniu kryzysowym reprezentuje starosta, będący organem zarządzania kryzysowego na obszarze powiatu ziemskiego lub grodzkiego. Starosta odpowiada za przedsięwzięcia przekraczające możliwości pojedynczych gmin lub wymagające koordynacji ponadgminnej³⁸⁹. Do jego zadań należy m.in. przygotowanie Powiatowego Planu Zarządzania Kryzysowego (integrującego analizy zagrożeń i plany z gmin) oraz nadzorowanie realizacji zadań z zakresu zarządzania kryzysowego przez podległe powiatowe służby i jednostki organizacyjne. W sytuacjach kryzysowych starosta może przejąć koordynację akcji ratunkowej na terenie powiatu, szczególnie gdy zdarzenie dotyka więcej niż jedną gminę lub ma zasięg powiatowy (np. epidemia, rozległa awaria infrastruktury, katastrofa transportowa). W celu zapewnienia współdziałania powołany jest Powiatowy Zespół Zarządzania Kryzysowego (PZZK) pod przewodnictwem starosty. W skład PZZK wchodzi m.in. przedstawiciele gmin (np. wybrani wójtowie lub burmistrzowie z terenu powiatu), komendanci powiatowi Państwowej Straży Pożarnej i Policji, powiatowy inspektor sanitarny, przedstawiciele powiatowych inspekcji (np. weterynaryjnej, budowlanej), a także – w zależności od potrzeb – reprezentanci innych podmiotów, takich jak organizacje

³⁸⁸ M. Romaniuk, *Gmina w procesie zarządzania kryzysowego*, Wrocławskie Studia Politolologiczne, Uniwersytet Wrocławski, 2023, s. 45-62. <https://doi.org/10.34616/150574>

³⁸⁹ Z. Ciekankowski (red.), *Infrastruktura bezpieczeństwa publicznego: ogólnokrajowe i lokalne wyzwania cywilizacyjne*, Warszawa, Wyższa Szkoła Zarządzania i Prawa, 2010.

pozarządowe czy ochotnicze straże pożarne. Zadaniem PZZK jest wypracowanie rozwiązań i rekomendacji dla starosty oraz bieżąca koordynacja działań ratowniczych i pomocowych w czasie kryzysu. W powiecie funkcjonuje również Powiatowe Centrum Zarządzania Kryzysowego (PCZK), najczęściej ulokowane w strukturze starostwa (np. jako stanowisko pracy ds. zarządzania kryzysowego lub wydział bezpieczeństwa). PCZK, podobnie jak centra wojewódzkie, pełni całodobowy dyżur i zapewnia monitoring sytuacji na poziomie powiatu, a ponadto utrzymuje kontakt z gminami i WCZK. Do typowych zadań PCZK należy zbieranie informacji od gminnych ogniw (np. o lokalnych podtopieniach, sytuacji na drogach powiatowych), alarmowanie właściwych służb oraz alarmowanie społeczności (np. poprzez powiatowy system alarmowy syren), a także organizowanie telekonferencji lub spotkań sztabu kryzysowego powiatu. Starosta, podobnie jak wojewoda, może w sytuacjach nadzwyczajnych wydawać polecenia wójtom z obszaru powiatu³⁹⁰, choć o mniejszym zakresie niż polecenia wojewody. Powiat pełni zatem rolę pośrednią między szczeblem wojewódzkim a gminnym – wzmacnia działania gmin oraz przekazuje informacje i pomoc w obie strony (od gmin do wojewody i odwrotnie).

Poziom gminny jest najniższym, lecz często najważniejszym z praktycznego punktu widzenia, ogniwem systemu zarządzania kryzysowego. To właśnie wójt, burmistrz lub prezydent miasta (jako organ wykonawczy gminy) stanowi pierwszy podmiot reagujący na większość lokalnych zagrożeń – pożarów, podtopień, skażeń, awarii – jeszcze zanim na miejsce dotrą służby wojewódzkie czy wsparcie z zewnątrz. Zapewnienie bezpieczeństwa mieszkańców i porządku publicznego należy do zadań własnych każdej gminy i powiatu, wynikających z ustawy o samorządzie gminnym. Organy gminy mogą też wykonywać w tym obszarze zadania zlecone z administracji rządowej. Wójt (burmistrz, prezydent) realizuje zadania zarządzania kryzysowego przy pomocy swojej gminnej administracji – często wyznaczana jest w urzędzie gminy komórka lub stanowisko ds. zarządzania kryzysowego, odpowiedzialne za planowanie cywilne i reagowanie. Na podstawie art. 19 ust. 4 ustawy organem pomocniczym wójta jest Gminny Zespół Zarządzania

³⁹⁰ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 25).

Kryzysowego (GZZK)³⁹¹. W skład GZZK zwykle wchodzi: przedstawiciele kluczowych ogniw lokalnych (sekretarz gminy, kierownicy referatów odpowiedzialnych za sprawy bezpieczeństwa, ochrony środowiska, infrastruktury), kierownicy gminnych jednostek organizacyjnych (np. dyrektorzy szkół – na wypadek konieczności organizacji schronienia lub ewakuacji ludności, kierownik ośrodka pomocy społecznej – ds. pomocy poszkodowanym, itp.), a także lokalni komendanci służb – choć Policja i PSP podlegają powiatowi i wojewodzie, to ich posterunki i jednostki działają na terenie gminy i zwykle uczestniczą w pracach zespołu. Często w skład GZZK wchodzi również przedstawiciele Ochotniczych Straży Pożarnych oraz innych organizacji społecznych zaangażowanych w bezpieczeństwo. Posiedzeniom GZZK przewodniczy wójt lub osoba przez niego wyznaczona, a zespół zbiera się regularnie (np. kilka razy do roku celem aktualizacji planów, treningów alarmowych) oraz natychmiast w sytuacji wystąpienia poważnego zdarzenia. Zadaniem gminnego zespołu jest ocena zagrożeń na poziomie lokalnym, opracowanie procedur postępowania (np. instrukcji ewakuacji sołectw zagrożonych powodzią), a także zapewnienie wymiany informacji i współdziałania wszystkich lokalnych podmiotów zaangażowanych w ochronę ludności. Gmina opracowuje i utrzymuje aktualny Gminny Plan Zarządzania Kryzysowego, który zawiera m.in. charakterystykę lokalnych zagrożeń, siatkę bezpieczeństwa (wykaz dostępnych sił i środków ratowniczych na terenie gminy), procedury reagowania na poszczególne scenariusze oraz zasady uruchamiania rezerw i pomocy z zewnątrz. Wójt ma obowiązek uwzględnić w tym planie zalecenia otrzymane od starosty i wojewody, tak, aby plany wyższego i niższego szczebla były ze sobą zharmonizowane. W strukturach wielu gmin (szczególnie miejskich) działają stałe gminne lub miejskie centra zarządzania kryzysowego (GCZK), jednak nie jest to obowiązkowe ustawowo rozwiązanie. Zwykle powołuje się je w większych miastach na prawach powiatu – np. w Warszawie, Krakowie czy Łodzi funkcjonują całonocowe miejskie centra operacyjne, monitorujące sytuację i alarmujące służby. W mniejszych gminach rolę centrum pełni po prostu dyżurny urzędu gminy lub pracownik odpowiedzialny za kontakty z PCZK. Niezależnie od formy

³⁹¹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 19 ust 4).

organizacyjnej, na poziomie gminy dokonuje się pierwszej oceny sytuacji kryzysowej i podejmuje pierwsze działania ratownicze. Gmina jako podstawowa wspólnota samorządowa jest najbliższej obywateli i najlepiej zna ich potrzeby oraz lokalne uwarunkowania. Jak zauważa Romaniuk, to właśnie gminy wyrastają na kluczowe podmioty systemu zarządzania kryzysowego, zwłaszcza wobec nowych wyzwań, takich jak pandemia czy nagłe klęski żywiołowe, wymagające natychmiastowej reakcji na miejscu.

Planowanie kryzysowe stanowi istotny element funkcjonowania systemu na każdym szczeblu. Ustawa z 2007 r. wprowadziła hierarchiczny system planów zarządzania kryzysowego – od Krajowego Planu Zarządzania Kryzysowego (KPZK), poprzez plany wojewódzkie i powiatowe, aż po plany gminne. KPZK jest przygotowywany przez RCB we współpracy z ministerstwami, a zatwierdzany przez Radę Ministrów³⁹². Zawiera on ogólnokrajową analizę ryzyka, scenariusze reagowania na najpoważniejsze zagrożenia oraz wytyczne dla administracji wszystkich szczebli. Na jego podstawie wojewodowie sporządzają wojewódzkie plany zarządzania kryzysowego, uwzględniające specyfikę regionalną (np. zagrożenia powodziowe na dużych rzekach, zakłady o zwiększonym ryzyku awarii na terenie województwa, itp.). Następnie starostowie przygotowują powiatowe plany, integrujące informacje z gmin i wojewódzkich zaleceń, zaś wójtowie – gminne plany dostosowane do lokalnych warunków. Ważną zasadą jest spójność planowania: każdy plan niższego szczebla powinien być zgodny z planem wyższego szczebla i realizować wytyczne i zalecenia w nim zawarte³⁹³. Same plany dzielą się na cztery zasadnicze części: opis potencjalnych zagrożeń i ocenę ryzyka, zadania i obowiązki uczestników systemu na wypadek kryzysu, procedury reagowania (tzw. plany operacyjne na określone sytuacje) oraz ustalenia finansowo-logistyczne dotyczące zabezpieczenia działań. Niestety, kontrola NIK wykazała poważne niedociągnięcia w zakresie jakości tych planów na poziomie samorządowym³⁹⁴. Jak stwierdza NIK, żaden z 20 skontrolowanych planów zarządzania

³⁹² Związek Banków Polskich (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, rozdz. 9: Współpraca z jednostkami publicznymi, Warszawa, ZBP, 2017, s. 145-160.

³⁹³ M. Romaniuk, *Gmina w procesie zarządzania kryzysowego*, Wrocławskie Studia Politológiczne, Uniwersytet Wrocławski, 2023, s. 45-62. <https://doi.org/10.34616/150574>

³⁹⁴ Najwyższa Izba Kontroli, NIK: gminy i powiaty nieprzygotowane organizacyjnie na sytuacje kryzysowe, Serwis Samorządowy PAP, 2019.

kryzysowego w gminach i powiatach nie był rzetelnie przygotowany ani kompletny – plany tworzone dla zasady, by spełnić ustawowy obowiązek, często metodą „kopiuj-wklej”, bez realnej przydatności praktycznej³⁹⁵. W skrajnych przypadkach gminny plan okazywał się całkowicie oderwany od rzeczywistości – NIK opisała przypadek gminy dotkniętej skutkami nawałnicy (burzy z 2017 r.), gdzie lokalny plan kryzysowy powielał w znacznej części treść powiatowego planu i nie zawierał nawet aktualnych danych o dostępnych na terenie gminy zasobach. W efekcie, gdy w sierpniu 2017 r. przez Pomorze przeszła niszczycielska wichura, działania ratownicze w wielu miejscach prowadzono ad hoc, bez oparcia o zapisy planów, które okazały się nieprzydatne. NIK oceniła też krytycznie brak ćwiczeń i aktualizacji – plany często „leżały w szufladzie”, a personel gminny nie był z nimi dostatecznie zapoznany. Te wnioski pokazują, że planowanie cywilne na poziomie samorządów bywa traktowane formalnie, co stanowi poważne ograniczenie skuteczności zarządzania kryzysowego. Konieczne jest zatem bardziej realistyczne podejście do planów – regularne aktualizacje, konsultacje ze służbami i społecznością lokalną, a przede wszystkim testowanie planów poprzez ćwiczenia (np. symulacje powodzi czy ewakuacji) i korygowanie ich na podstawie wniosków z takich treningów.

Współpraca między szczeblami oraz relacje pionowe i poziome są fundamentem polskiego systemu zarządzania kryzysowego. Organy wyższych szczebli pełnią funkcję wspierającą i nadzorczą wobec niższych – np. wojewoda monitoruje stan przygotowań powiatów i gmin, może zarządzać przemieszczenie sił (PSP, policji, ratowników) z obszarów nieobjętych kryzysem do rejonu dotkniętego katastrofą, a w razie potrzeby wnioskuje o wsparcie centralne. Z kolei administracja lokalna jest zobowiązana raportować sytuacje nadzwyczajne do szczebla wyższego: wójt informuje starostę i wojewodę o poważnych zdarzeniach, co zapewnia uruchomienie dalszych mechanizmów pomocy. Kluczową rolę odgrywa tu jednolity obieg informacji – art. 11 ustawy zobowiązuje RCB do zapewnienia wymiany informacji między wszystkimi ogniwami od wójta aż po premiera³⁹⁶. Temu służy

³⁹⁵ Najwyższa Izba Kontroli, NIK: gminy i powiaty nieprzygotowane organizacyjnie na sytuacje kryzysowe, Serwis Samorządowy PAP, 2019.

³⁹⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm., art. 11).

m.in. system całodobowych punktów kontaktowych (służb dyżurnych) na każdym poziomie – każda gmina, powiat, służba i urząd wojewódzki utrzymuje numery alarmowe i adresy e-mail, pod którymi można przez całą dobę przekazać ostrzeżenie lub zgłoszenie. Informacja o zagrożeniu (np. wykryciu skażenia wody pitnej czy zbliżającej się fali powodziowej) jest w ten sposób szybko transmitowana w górę i w dół struktury – do wojewody i RCB, a równocześnie do wszystkich potencjalnie zagrożonych gmin i powiatów. Współpraca pozioma natomiast przejawia się w ramach zespołów zarządzania kryzysowego i nawiązanych porozumień sąsiedzkich. Na poziomie lokalnym często kilka sąsiadujących gmin łączy siły – dobrym przykładem jest międzygminne porozumienie 21 gmin Aglomeracji Opolskiej, które wspólnie z PSP opracowały zasady wzajemnej pomocy w sytuacjach kryzysowych. Również powiaty w razie potrzeby dzielą się zasobami – np. jednostki OSP czy sprzęt ciężki z jednego powiatu mogą zostać skierowane do pomocy w sąsiednim powiecie na mocy porozumień zawartych jeszcze przed wystąpieniem zagrożenia. Ta solidarność terytorialna jest ważnym elementem budowania odporności – zwłaszcza w obliczu zjawisk przekraczających granice administracyjne (powodzie, wichury). Warto podkreślić, że w zespołach kryzysowych uczestniczą przedstawiciele różnych służb i instytucji, co sprzyja wypracowaniu wspólnego języka i procedur między nimi (tzw. podejście zintegrowane). Przykładowo, gminny zespół może uzgodnić z lokalnym posterunkiem policji i OSP zasady ewakuacji mieszkańców zalewanej wioski – kto odpowiada za transport osób o ograniczonej mobilności, gdzie zorganizować punkt przyjęcia ewakuowanych – tak, aby przy realnym zagrożeniu każdy znał swoją rolę.

Współdziałanie z organizacjami pozarządowymi (NGO), Ochotniczą Strażą Pożarną (OSP) i społecznością lokalną stanowi coraz ważniejszy wymiar zarządzania kryzysowego na poziomie samorządu. Jednostki OSP – zrzeszające lokalnych ochotników – są nieodłącznym elementem systemu ochrony przeciwpożarowej i ratownictwa na terenach wiejskich i w małych miastach. Działają one na mocy ustawy o ochronie przeciwpożarowej jako część krajowego systemu ratowniczo-gaśniczego (po spełnieniu określonych wymogów) lub poza KSRG, zawsze jednak pozostają pod zwierzchnictwem lokalnych władz samorządowych i komend PSP. W praktyce to właśnie druhowie OSP często pierwsi docierają na miejsce pożaru czy

wypadku w odległej miejscowości, niosąc pomoc zanim pojawią się służby państwowe. Wójtowie i starostowie ściśle współpracują z OSP – finansują ich wyposażenie, szkolenia, paliwo; włączają do gminnych i powiatowych planów reagowania (np. przypisując konkretne jednostki OSP do zadań przy umacnianiu wałów przeciwpowodziowych, dystrybucji wody pitnej, itp.). Społeczność lokalna jako całość także odgrywa istotną rolę – mieszkańcy bywają nazywani „pierwszymi ratownikami na miejscu zdarzenia”, gdyż to oni zazwyczaj najszybciej reagują, alarmują służby, podejmują początkowe działania (jak gaszenie zarzewia ognia czy udzielanie pierwszej pomocy poszkodowanym) jeszcze przed przybyciem profesjonalnych jednostek. Takie spontaniczne zaangażowanie społeczne szczególnie było widoczne podczas katastrof naturalnych w Polsce – np. podczas powodzi w 2010 r. w gminie Wilków mieszkańcy, strażacy OSP i wolontariusze z całego kraju ramię w ramię walczyli o umocnienie wałów przeciwpowodziowych, a po ich przerwaniu wspólnie organizowali ewakuację i pomoc dla poszkodowanych. Pandemia COVID-19 również zaowocowała licznymi oddolnymi inicjatywami (szycie maseczek, dostarczanie zakupów osobom na kwarantannie, itp.), podobnie jak kryzys uchodźczy w 2022 r. – pokazując ogromny potencjał drzemiący w społeczeństwie obywatelskim. Organizacje pozarządowe (m.in. Polski Czerwony Krzyż, grupy ratownictwa medycznego, fundacje pomocowe jak PCPM) wniosły istotny wkład w uzupełnienie działań państwa, nierzadko reagując szybciej i bardziej elastycznie niż urzędy³⁹⁷. Jak zauważa Romaniuk, największe możliwości współpracy z NGO istnieją właśnie na poziomie lokalnym – gminnym i powiatowym – gdzie partnerstwo administracji ze stowarzyszeniami czy fundacjami może realnie zwiększyć skuteczność działań³⁹⁸. Przykładowo, lokalne oddziały PCK mogą prowadzić punkty pomocy doraźnej podczas ewakuacji, a organizacje wolontariackie – pomagać w dystrybucji żywności i wody. Dotychczas współdziałanie to opierało się głównie na ogólnych zapisach ustawy o działalności pożytku publicznego i wolontariacie. Nowe przepisy jednak idą krok dalej. Wejście w życie ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie

³⁹⁷ D. Sześciło, *Ustawa o ochronie ludności i obronie cywilnej – jak zorganizować współpracę samorządu z organizacjami pozarządowymi?*, Warszawa, Fundacja im. Stefana Batorego, 2025, s. 1-12.

³⁹⁸ M. Romaniuk, *Gmina w procesie zarządzania kryzysowego*, Wrocławskie Studia Politologiczne, Uniwersytet Wrocławski, 2023, s. 45-62. <https://doi.org/10.34616/150574>.

cywilnej stworzyło formalne ramy dla trwałego włączenia organizacji społecznych w system zarządzania kryzysowego³⁹⁹. Ustawa ta pozwala samorządom gminnym i powiatowym zawierać porozumienia z organizacjami pozarządowymi, ochotniczymi strażami czy innymi podmiotami non-profit w zakresie realizacji zadań zwiększających bezpieczeństwo mieszkańców. Na mocy takiego porozumienia NGO mogą przejąć realizację określonych przedsięwzięć: prowadzenie akcji informacyjnych o zagrożeniach, organizowanie szkoleń i ćwiczeń dla ludności, przygotowanie i utrzymanie miejsc schronienia (np. prowizorycznych noclegowni w szkołach, punktów wydawania posiłków), czy też zakup i magazynowanie sprzętu do pomocy humanitarnej. Co ważne, porozumienia te mogą przewidywać finansowanie zadań ze środków samorządu, co pozwala NGO utrzymywać gotowość do działania. Nowe prawo stanowi odpowiedź na wnioski płynące z ostatnich kryzysów: pandemii, wojny na Ukrainie czy katastrofalnej powodzi z 2024 r., które dobitnie pokazały kluczową rolę organizacji społecznych w reagowaniu na zagrożenia. Ekspertki podkreślają, że nie można już polegać wyłącznie na spontanicznym zrywie obywateli – konieczne jest systemowe włączenie NGO i liderów lokalnych we wspólne planowanie i przygotowania do kryzysów. Dzięki temu potencjał społeczny zostanie lepiej wykorzystany, a gotowość lokalnych struktur – zwiększona. Dobrym przykładem są tu projekty w rodzaju „Odporni na kryzys”, w ramach których samorządowcy i organizacje społeczne wspólnie wypracowują lokalne strategie reagowania i dzielą się zadaniami⁴⁰⁰.

Pomimo rozbudowania formalnych struktur, zarządzanie kryzysowe na poziomie samorządowym w Polsce stoi przed licznymi wyzwaniami i ograniczeniami. Jednym z podstawowych jest kwestia kompetencji kadr i zasobów. NIK w 2019 r. wskazała, że pracownicy urzędów gmin i starostw odpowiedzialni za sprawy zarządzania kryzysowego często nie mieli wystarczającego przygotowania merytorycznego – brakowało szkoleń specjalistycznych, a co więcej do obsady tych stanowisk nie wymagano ustawowo żadnych kwalifikacji (stanowiska te nieraz powierzano „z klucza”

³⁹⁹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

⁴⁰⁰ PCPM, Odporni na kryzys – rekomendacje dla włączenia społeczności lokalnej w system zarządzania kryzysowego, Warszawa, Fundacja PCPM, 2025.

innym urzędnikom)⁴⁰¹. Powoduje to, że jakość planów i działań bywa niższa, a współpraca ze służbami ratowniczymi – utrudniona. Kolejnym problemem jest niedobór środków finansowych w samorządach na realizację zadań z zakresu bezpieczeństwa. Choć zgodnie z prawem powiaty i gminy powinny zabezpieczać w budżetach fundusze na zarządzanie kryzysowe, w praktyce wydatki te bywają niewystarczające lub porozrzucane po różnych pozycjach (utrudnia to ich identyfikację i kontrolę). Dopiero poważne kryzysy ujawniają luki – np. przed wspomnianą nawałnicą w 2017 r. żaden ze skontrolowanych samorządów nie przewidział w planach alternatywnych źródeł zasilania i łączności, co sparaliżowało przepływ informacji po zniszczeniu sieci energetycznej i telekomunikacyjnej⁴⁰². Istotną barierą jest też niska aktywność zespołów zarządzania kryzysowego w okresach „spokojnych”. Zespoły te zbierają się często tylko pro forma kilka razy do roku lub – co gorsza – wyłącznie podczas realnego kryzysu. Powoduje to brak praktyki we współdziałaniu; uczestnicy zespołów nie znają dobrze procedur ani siebie nawzajem, co wydłuża reakcję w nagłej sytuacji. Częstotliwość zwoływania posiedzeń GZZK zależy od wójta, a brak regularnych spotkań utrudnia ocenę stanu przygotowań i gotowości faktycznej. Kultura proaktywnego planowania dopiero się kształtuje – nadal dominuje podejście reagowania dopiero po wystąpieniu szkody („mądrość Polaka po szkodzie”), zamiast inwestowania w prewencję i budowanie odporności lokalnej na zagrożenia. Pewnym problemem bywa również rozmycie odpowiedzialności i potencjalne spory kompetencyjne – np. między gminą a powiatem w kwestii utrzymania wałów przeciwpowodziowych czy dróg (na szczęście ustawa o ochronie ludności z 2024 r. doprecyzowuje wiele z tych kwestii, wskazując jednoznacznie gospodarza danego zadania). W sytuacjach kryzysowych nie ma jednak miejsca na spory kompetencyjne – kluczowe jest skuteczne przywództwo kryzysowe i współdziałanie ponad podziałami.

System zarządzania kryzysowego w jednostkach samorządu terytorialnego w Polsce jest rozbudowany i oparty na jasno zdefiniowanych szczeblach – od centralnego przez wojewódzki i powiatowy po gminny – z przypisaniem konkretnych zadań i instrumentów na każdym z poziomów. Jego

⁴⁰¹ Najwyższa Izba Kontroli, NIK: gminy i powiaty nieprzygotowane organizacyjnie na sytuacje kryzysowe, Serwis Samorządowy PAP, 2019.

⁴⁰² Tamże.

efektywność zależy jednak od rzeczywistego wypełnienia treścią tych ram organizacyjnych: od fachowości kadr, poprzez rzetelne planowanie i ćwiczenie procedur, po wykorzystanie potencjału drzemiącego w społecznościach lokalnych. Praktyka pokazała zarówno przykłady sprawnego działania – jak choćby skoordynowana akcja ewakuacji podczas powodzi czy szybka reakcja części samorządów na pierwszy szok pandemii – jak i przypadki poważnych zaniechań, ujawnione choćby w raporcie NIK z 2019 r.⁴⁰³ Nowe uwarunkowania – zmiany klimatyczne przynoszące częstsze klęski żywiołowe, zagrożenia hybrydowe i epidemiczne, a także oczekiwania społeczne co do bezpieczeństwa – wymuszają dalsze usprawnienia systemu. Kierunki zmian wyznacza wspomniana ustawa z 2024 r. o ochronie ludności, integrująca zarządzanie kryzysowe z obroną cywilną oraz przewidująca znaczące środki finansowe na wzmocnienie lokalnych zdolności (na realizację zadań ustawy zaplanowano ponad 4 mld zł do końca 2025 r.). Włączenie organizacji społecznych w przygotowania, rozwój lokalnych systemów wczesnego ostrzegania (np. SMS-owy Alert RCB rozbudowany o poziom gminny), tworzenie planów ciągłości działania dla kluczowych usług komunalnych – to elementy budowania odporności samorządów na kryzysy. Równie istotne jest kształtowanie świadomości i edukacja mieszkańców, aby stawali się partnerami w systemie bezpieczeństwa, a nie tylko jego adresatami⁴⁰⁴. Wszystkie te działania mają sprawić, że zarządzanie kryzysowe na poziomie lokalnym będzie nie tylko formalnie poprawne, ale przede wszystkim skuteczne i sprawne w obliczu realnych zagrożeń.

5.2. Zarządzanie kryzysowe na poziomie wojewódzkim i krajowym

Wojewoda pełni kluczową funkcję w systemie zarządzania kryzysowego na poziomie regionalnym. Ustawa jednoznacznie wskazuje wojewodę jako organ właściwy w sprawach zarządzania kryzysowego na terenie

⁴⁰³ Tamże.

⁴⁰⁴ J. Wołęjszo, K. Rejman, M. Wilczyńska (red.), Bezpieczeństwo informacji w zarządzaniu kryzysowym, Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2025.

województwa⁴⁰⁵. Oznacza to, że wojewoda odpowiada za koordynację działań ponadlokalnych w sytuacjach kryzysowych, obejmujących więcej niż jedną jednostkę samorządu terytorialnego. W praktyce wojewoda koordynuje działania powiatów i gmin, szczególnie gdy skala zagrożenia przekracza możliwości pojedynczego powiatu lub gminy⁴⁰⁶. Do zadań wojewody należy m.in. kierowanie monitoringiem i analizą zagrożeń na terenie województwa, organizacja planowania cywilnego i reagowania kryzysowego oraz wspieranie organów samorządowych niższego szczebla w realizacji ich zadań z zakresu zarządzania kryzysowego. Wsparcie to przejawia się choćby poprzez wydawanie zaleceń do powiatowych i gminnych planów reagowania kryzysowego oraz poprzez udostępnianie zasobów i informacji niezbędnych do działań ratowniczych i usuwania skutków kryzysu. Wojewoda, działając z ramienia administracji rządowej w terenie, może uruchamiać siły i środki spoza danej gminy czy powiatu – np. dysponować wsparciem służb zespolonych (Państwowej Straży Pożarnej, Policji, inspekcji itp.) działających na obszarze województwa. W ten sposób wojewoda zapewnia, że lokalne władze nie pozostają same w obliczu większego zagrożenia.

Narzędziem operacyjnym wojewody jest Wojewódzkie Centrum Zarządzania Kryzysowego (WCZK) – całodobowa komórka działająca w urzędzie wojewódzkim, która gromadzi dane o zagrożeniach, koordynuje przepływ informacji oraz inicjuje procedury reagowania. Przy wojewodzie funkcjonuje także Wojewódzki Zespół Zarządzania Kryzysowego (WZZK) jako organ opiniotawczo-doradczy. Wojewoda powołuje skład WZZK według potrzeb – mogą w nim zasiadać przedstawiciele administracji rządowej i samorządowej oraz eksperci. WZZK wspomaga wojewodę w ocenie sytuacji i rekomendowaniu działań, jednak decyzje podejmowane są jednoosobowo przez wojewodę (zgodnie z zasadą jednoosobowego kierownictwa w zarządzaniu kryzysowym). Warto podkreślić, że wojewoda realizuje zadania zarządzania kryzysowego poprzez komórki organizacyjne urzędu (np. wydział bezpieczeństwa i zarządzania kryzysowego) oraz poprzez podporządkowane mu służby zespolone. Integracja tych służb na poziomie województwa (tzw.

⁴⁰⁵ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 14, ust. 1).

⁴⁰⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 14, ust. 2, pkt 1).

zasada zespolenia) umożliwia jednolite kierowanie akcją w sytuacji kryzysowej. Dzięki temu w razie potrzeby wojewoda może skoordynować np. działania PSP, Policji, inspekcji sanitarnych i innych podmiotów państwowych na danym terenie. Wojewoda odgrywa również rolę łącznika między poziomem krajowym a lokalnym. To on przekazuje polecenia i wytyczne wydane na szczeblu centralnym do starostów i wójtów, a zarazem raportuje do centrum o rozwoju sytuacji na dole. Ustawa przewiduje, że organ, który pierwszy uzyska informację o zagrożeniu, niezwłocznie informuje organy wyższego i niższego szczebla. Często tym organem jest właśnie wojewoda – szczególnie gdy zagrożenie ma charakter ponadpowiatowy lub potencjalnie ponadregionalny. Koordynacja ponadlokalna w wykonaniu wojewody oznacza m.in. organizowanie wspólnych ćwiczeń z udziałem różnych powiatów, uzgadnianie planów ewakuacji (wojewoda zatwierdza wojewódzki plan ewakuacji ludności obejmujący rejony z wielu powiatów) czy zarządzanie relokacją zasobów (np. przesunięcie sprzętu ratowniczego do rejonu dotkniętego klęską). Przykładowo, wojewoda opracowuje wojewódzki plan ewakuacji i w razie potrzeby może zarządzić ewakuację ludności z terenów zagrożonych, w porozumieniu z sąsiednimi województwami lub z poziomem krajowym, jeśli ewakuacja wykracza poza obszar jednego województwa.

Wsparcie gmin i powiatów przez wojewodę ma także wymiar finansowy i organizacyjny. Wojewoda dysponuje środkami z budżetu państwa (np. z rezerwy celowej na zarządzanie kryzysowe) przeznaczonymi na dofinansowanie zadań z zakresu ochrony ludności i usuwania skutków klęsk żywiołowych na poziomie lokalnym. Może przyznać samorządom środki na odbudowę infrastruktury po katastrofie czy na szkolenia z zakresu reagowania kryzysowego. Ponadto wojewodowie prowadzą wojewódzkie centra logistyczne (magazyny interwencyjne), które gromadzą sprzęt i rezerwy materiałowe do użycia w sytuacjach nadzwyczajnych – dostępne dla powiatów i gmin w razie kryzysu. Należy zaznaczyć, że obecny model prawny w Polsce nie daje wojewodzie pełnej władzy dyrektywnej wobec samorządów w sytuacji kryzysowej – formalne wydawanie poleceń organom gmin czy powiatów (oraz przedsiębiorcom) jest zastrzeżone dla Prezesa Rady Ministrów

i ministrów⁴⁰⁷. W ostatnim czasie pojawiła się jednak dyskusja nad zmianą tego stanu. Ministerstwo Klimatu i Środowiska postulowało, aby wojewoda mógł wydawać wiążące polecenia podczas kryzysu, co miałoby usprawnić reakcję – dotąd podobne uprawnienia nadawano wojewodom tylko na podstawie specustaw w szczególnych sytuacjach (np. powódź). Przykładem jest powódź, podczas której specustawa dała wojewodom prawo wydawania poleceń dot. usuwania odpadów z terenów zalanych, co przyspieszyło działania porządkowe. Jednak autorzy projektu nowelizacji z Rządowego Centrum Bezpieczeństwa (RCB) byli sceptyczni wobec takiego rozszerzenia kompetencji wojewodów, argumentując, że zarządzanie kryzysowe zgodnie z ustawą sprawuje rząd i to premier oraz ministrowie powinni zachować wyłączne prawo wydawania poleceń, aby uniknąć ewentualnych kolizji decyzji oraz problemów z finansowaniem tych poleceń. Ostateczny kształt przepisów w tym zakresie pozostaje przedmiotem prac legislacyjnych, lecz sama debata uwidacznia rosnącą świadomość roli wojewody jako koordynatora działań kryzysowych i potrzebę zapewnienia mu odpowiednich narzędzi decyzyjnych. Wojewoda, sprawując nadzór nad zarządzaniem kryzysowym w regionie, musi jednocześnie ściśle współpracować z centralnymi strukturami zarządzania kryzysowego. W przypadku eskalacji zagrożenia wojewoda informuje właściwe organy centralne (Ministra Spraw Wewnętrznych i Administracji, Rządowe Centrum Bezpieczeństwa) o sytuacji oraz o podjętych działaniach. Dzięki nowoczesnym technologiom komunikacyjnym, wymiana informacji jest bieżąca, co pozwala centrum szybko reagować i wydawać decyzje, jeśli kryzys wymaga interwencji ponadwojewódzkiej. Reasumując, wojewoda pełni funkcję regionalnego menedżera kryzysowego, będącego ogniwem łączącym poziom lokalny z krajowym – koordynuje i wspiera działania na dole, a gdy sytuacja tego wymaga, uruchamia mechanizmy wsparcia ze szczybla centralnego. Na poziomie krajowym za zarządzanie kryzysowe odpowiada Rada Ministrów z Premierem na czele – to najwyższy organ kierujący i ponoszący odpowiedzialność za reagowanie na zagrożenia obejmujące więcej niż jedno województwo lub o znaczeniu ogólnopolskim. Prezes Rady Ministrów może – w sytuacji kryzysowej – wydawać polecenia

⁴⁰⁷ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 7).

obowiązujące organy administracji rządowej i samorządowej oraz inne podmioty⁴⁰⁸, co stanowi najsilniejszy instrument zarządczy w systemie. W trybie pilnym, jeśli wymaga tego dobro państwa, rolę tę może tymczasowo pełnić Minister Spraw Wewnętrznych i Administracji, zobowiązany jednak do niezwłocznego powiadomienia premiera o swoich działaniach⁴⁰⁹.

Centralnym organem o charakterze doradczo-koordynacyjnym jest Rządowy Zespół Zarządzania Kryzysowego (RZZK). Zespół ten, utworzony przy Radzie Ministrów, odpowiada za inicjowanie i koordynowanie działań w zakresie zarządzania kryzysowego na szczeblu państwa. RZZK nie ma osobowości decyzyjnej (jego ustalenia mają charakter rekomendacji), ale zgodnie z planowanymi reformami ma zyskać większe umocowanie – postuluje się uczynienie go organem o charakterze decyzyjnym, aby skupić centrum kierowania kryzysowego w jednym miejscu (pod przewodnictwem premiera). Aktualnie w skład RZZK wchodzi najważniejsze osoby rządowe: Prezes Rady Ministrów (przewodniczący), jego zastępcy – Minister Obrony Narodowej oraz Minister Spraw Wewnętrznych i Administracji, a także m.in. Minister Spraw Zagranicznych, Minister – Koordynator Służb Specjalnych (jeśli jest powołany) oraz inni właściwi ministrowie i szefowie urzędów centralnych, zależnie od rodzaju kryzysu. Sekretarzem RZZK jest Dyrektor Rządowego Centrum Bezpieczeństwa. RZZK może obradować w trybie jawnym lub niejawnym, w zależności od wrażliwości tematu. Posiedzenia Zespołu zwoływane są w sytuacjach poważnych zagrożeń – np. przed podjęciem decyzji o wprowadzeniu stanu nadzwyczajnego, w obliczu katastrofy naturalnej o dużej skali czy kryzysu bezpieczeństwa narodowego.

Najważniejszą wyspecjalizowaną instytucją na poziomie centralnym jest Rządowe Centrum Bezpieczeństwa (RCB), utworzone na mocy ustawy z 2007 r. RCB pełni rolę krajowego centrum zarządzania kryzysowego, działającego w systemie 24/7. Główne zadania RCB obejmują: całodobowy monitoring i analizę zagrożeń w kraju (oraz monitorowanie zagrożeń poza

⁴⁰⁸ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 11).

⁴⁰⁹ M. Krawczyk, G. Nowacki, Functioning of the Crises Management System at the Country and Commune Including the Aspects of Transport, *Journal of Civil Engineering and Transport*, 5(2), 2023, s. 9-24. <https://doi.org/10.24136/tren.2023.005>

granicami, mogących wpłynąć na Polskę)⁴¹⁰, przekazywanie właściwym organom ostrzeżeń i rekomendacji, a także koordynację obiegu informacji między wszystkimi szczeblami administracji w czasie sytuacji kryzysowej. RCB zapewnia obsługę merytoryczno-techniczną Rady Ministrów, Prezesa RM, RZZK oraz ministra właściwego ds. wewnętrznych w sprawach zarządzania kryzysowego⁴¹¹. Innymi słowy, RCB przygotowuje analizy, raporty i projekty decyzji dla najważniejszych organów państwa, aby ułatwić im podejmowanie trafnych działań w obliczu zagrożeń. Strukturalnie RCB jest centrum, które integruje informacje z wojewódzkich centrów zarządzania kryzysowego (WCZK) oraz resortowych centrów zarządzania kryzysowego. Na każdym poziomie administracji istnieje organ decyzyjny odpowiedzialny za zarządzanie kryzysowe (jednoosobowy, zgodnie z zasadą personalnej odpowiedzialności: wójt, starosta, wojewoda, premier), wspierany przez organ kolegialny o charakterze doradczym (zespoły zarządzania kryzysowego) oraz odpowiednie centrum zarządzania kryzysowego zapewniające zaplecze operacyjne i wymianę informacji. Na poziomie gminnym utworzenie centrum nie jest obowiązkowe – zależy od decyzji lokalnych władz i możliwości (w praktyce większe miasta posiadają centra zarządzania kryzysowego, natomiast małe gminy często nie tworzą osobnych centrów). Ten brak obligatoryjnych centrów na najniższym szczeblu bywa wskazywany jako potencjalna luka w systemie – może powodować przerwy w ciągłości przepływu informacji i utrudniać sprawne reagowanie, jeśli gmina nie dysponuje dedykowanym całodobowym centrum⁴¹². Niemniej jednak, nawet tam, gdzie nie ma stałego centrum gminnego, w razie kryzysu wójt/burmistrz uruchamia doraźne stanowisko kierowania (np. w ramach urzędu gminy lub lokalnej jednostki PSP), a powiatowe i wojewódzkie centra przejmują rolę węzłów komunikacyjnych.

Wracając do struktur centralnych – Rządowe Centrum Bezpieczeństwa pełni szereg kluczowych funkcji. Po pierwsze, odpowiada za cywilne

⁴¹⁰ G. Pietrek, Poziomy, struktura i zadania systemu zarządzania kryzysowego administracji rządowej, Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu, 3 (161), 2011, s. 376-388.

⁴¹¹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 11, ust. 2).

⁴¹² M. Krawczyk, G. Nowacki, Functioning of the Crises Management System at the Country and Commune Including the Aspects of Transport, Journal of Civil Engineering and Transport, 5, 2, 2023, s. 9-24, <https://doi.org/10.24136/tren.2023.005>

planowanie kryzysowe na poziomie państwa. RCB we współpracy z innymi organami opracowuje strategiczne dokumenty planistyczne, o których mowa w kolejnej części (m.in. Krajowy Plan Zarządzania Kryzysowego). Po drugie, RCB koordynuje działania prewencyjne takie jak opracowanie katalogu zagrożeń krajowych, przygotowywanie procedur postępowania i standardów reagowania. Po trzecie, w sytuacjach kryzysów o charakterze krajowym RCB zapewnia sprawny obieg informacji pomiędzy wszystkimi zaangażowanymi podmiotami – od szczebla gminnego po centralny. W praktyce, gdy dochodzi do poważnego zdarzenia, RCB zbiera meldunki od wojewodów i innych instytucji, przygotowuje zintegrowany obraz sytuacji dla kierownictwa państwa, uruchamia odpowiednie procedury (np. z zakresu ostrzegania ludności – Alert RCB), a także inicjuje posiedzenia RZZK lub sztabu kryzysowego w Kancelarii Premiera, jeśli wymagane są decyzje międzyresortowe. W strukturze rządowej funkcjonują również resortowe elementy systemu zarządzania kryzysowego. Każdy minister kierujący określonym działem administracji publicznej oraz kierownik centralnego urzędu ma obowiązek posiadać własny plan zarządzania kryzysowego oraz powołać zespół zarządzania kryzysowego wewnątrz swojej instytucji. Przykładowo, Minister Zdrowia dysponuje zespołem kryzysowym na wypadek epidemii, Minister Infrastruktury – na wypadek katastrofy transportowej, itp. Resortowe centra i zespoły współdziałają z RCB, zapewniając specjalistyczną wiedzę i wykonując zadania w swoim sektorze podczas sytuacji kryzysowej. W praktyce, przy kryzysach sektorowych (np. epidemia, awaria energetyczna), to resort właściwy prowadzi działania operacyjne, a RCB i RZZK pełnią funkcję koordynującą między różnymi sektorami i regionami. Należy też wspomnieć o roli Szefa Obrony Cywilnej Kraju, którą pełni z urzędu Komendant Główny Państwowej Straży Pożarnej. Obrona cywilna, choć formalnie odrębna od zarządzania kryzysowego, jest z nim ściśle powiązana w zakresie ochrony ludności⁴¹³. Dotychczasowe przepisy obrony cywilnej były jednak przestarzałe – w 2022 r. uchylono starą ustawę o powszechnym obowiązku obrony, pozostawiając lukę prawną w tym obszarze.

⁴¹³ K. Ochrya-Żurawska, J. Nowicka, Z. Ciekankowski, Organizacje pozarządowe w systemie bezpieczeństwa państwa na przykładzie Ochotniczych Straży Pożarnych, w: *Prakseologia w zarządzaniu i dowodzeniu*, t. 8: *Etyczność w dowodzeniu*, W. Kieźun, J. Wojejszo, K. Mikurenda (red.), Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2020, s. 23-40.

Struktury centralne (Rada Ministrów/Premier, RZZK, RCB i resorty) pełnią zatem przede wszystkim rolę koordynującą i wspierającą wobec działań realizowanych w terenie. Zgodnie z zasadą subsydiarności, poziom lokalny jest wykonawczy, natomiast wyższe poziomy zapewniają przywództwo, zasoby i jednolitą politykę reagowania. Dzięki istnieniu rozbudowanych centralnych struktur, państwo może reagować na zagrożenia, które przekraczają granice administracyjne pojedynczych województw, oraz zapewnić jednolite standardy przygotowań w całym kraju.

Skuteczne zarządzanie kryzysowe wymaga jednak nie tylko reagowania na bieżące zagrożenia, ale również wcześniejszego planowania i regularnych ćwiczeń. Na poziomie krajowym kluczowym dokumentem strategicznym jest Krajowy Plan Zarządzania Kryzysowego (KPZK). Plan ten, opracowywany przez Rządowe Centrum Bezpieczeństwa we współpracy z innymi podmiotami (ministerstwami, urzędami centralnymi oraz wojewodami), stanowi bazę dla planowania kryzysowego w całym kraju. KPZK jest dokumentem wyjściowym dla tworzenia planów zarządzania kryzysowego na niższych szczeblach – ministrowie, kierownicy urzędów centralnych i wojewodowie muszą swoje plany dostosować do ram wyznaczonych w KPZK. W tym sensie KPZK pełni rolę „matrycy planistycznej” dla systemu. Zawartość Krajowego Planu obejmuje wszystkie cztery fazy zarządzania kryzysowego – zapobieganie, przygotowanie, reagowanie i odbudowę – co czyni go kompleksowym narzędziem dla administracji. Plan identyfikuje katalog możliwych zagrożeń o znaczeniu krajowym, ocenia ich prawdopodobieństwo i potencjalne skutki, przypisuje podmioty wiodące dla każdego rodzaju zagrożenia (tzn. wskazuje, który resort lub instytucja będzie koordynować działania w razie wystąpienia danego typu kryzysu), a także opisuje procedury reagowania i usuwania skutków. Przykładowo, w najnowszej aktualizacji KPZK uwzględniono zagrożenia, które wysunęły się na pierwszy plan w ostatnich latach: skażenie środowiska wodnego (dodane po katastrofie ekologicznej na Odrze latem 2022 r.) oraz masową migrację ludności (doświadczoną m.in. wskutek kryzysu na granicy i wojny na Ukrainie). Wprowadzenie tych zagrożeń do planu oznacza przygotowanie scenariuszy i procedur na wypadek ich materializacji – np. przypisano Ministrowi Infrastruktury rolę podmiotu wiodącego dla zagrożenia zanieczyszczenia wód, a MSWiA – dla scenariusza masowej migracji. Co ważne,

KPKZ jest dokumentem żywym, regularnie aktualizowanym nie rzadziej niż co 2 lata, a w razie potrzeby częściej – jeśli pojawiają się nowe rodzaje zagrożeń bądź wnioski z przebiegu realnych sytuacji kryzysowych sugerujące konieczność korekt. Najnowsza wersja KPKZ została zaktualizowana i obowiązuje od 4 sierpnia 2025 r., zastępując poprzednią edycję z marca 2022 r. Aktualizacja w 2025 r. (ósma z kolei) objęła m.in.: zmiany w procedurach udzielania pomocy psychologicznej ofiarom zdarzeń (położono nacisk na interwencję psychologiczną wykonywaną także przez przeszkolony personel niemający formalnie tytułu psychologa), uwzględnienie wspomnianych nowych zagrożeń (Odra 2022, migracje) oraz dostosowanie zapisów do zmian w strukturze administracji rządowej (np. uwzględnienie utworzenia nowego działu administracji – gospodarka surowcami energetycznymi, czy zmiana podległości Rządowej Agencji Rezerw Strategicznych). Ciągłe doskonalenie planu krajowego odzwierciedla zasadę uczenia się na doświadczeniach – wydarzenia takie jak pandemia COVID-19, katastrofy naturalne (np. powodzie) czy zagrożenia hybrydowe skłaniają do rewizji scenariuszy i procedur. W 2024 r. rząd przyjął Raport o zagrożeniach bezpieczeństwa narodowego, z którego wnioski zostały uwzględnione przy aktualizacji KPKZ, zapewniając zgodność planowania z realnie zidentyfikowanymi lukami systemu bezpieczeństwa.

Obok planu krajowego istnieją analogiczne wojewódzkie plany zarządzania kryzysowego (opracowywane przez każdego wojewodę), a także powiatowe i gminne plany. Plany te muszą być wzajemnie spójne – plany niższego szczebla uwzględniają wytyczne i zalecenia z planów wyższych szczebli. Wojewoda zatwierdza plany powiatowe, natomiast plany wojewódzkie są opiniowane i zatwierdzane na poziomie centralnym (przez RCB i ministra ds. administracji). Niestety, według kontroli NIK zdarzało się, że sporządzanie tych planów bywało traktowane przez samorządy czysto formalnie – jako obowiązek papierowy – co obniżało ich praktyczną przydatność. Niemniej trwające prace nad nową ustawą o ochronie ludności przewidują stworzenie jednolitego, elektronicznego systemu planistycznego dla gmin, co ma ujednolicić i uprościć proces aktualizacji planów na dole.

Drugim filarem przygotowań – obok planowania – są ćwiczenia kryzysowe. Regularne ćwiczenia na poziomie krajowym i wojewódzkim pozwalają sprawdzić procedury w praktyce, zidentyfikować ewentualne

niejasności kompetencyjne czy braki w zasobach, a także wypracować współdziałanie różnych służb i instytucji. W Polsce organizuje się zarówno ćwiczenia sztabowe (decyzyjne), jak i praktyczne z udziałem sił ratowniczych. Ćwiczenia krajowe nierzadko przybierają formę wielkoskalowych symulacji obejmujących wiele województw jednocześnie. Przykładem może być ćwiczenie o kryptonimie LIBERO 2023, przeprowadzone na terenie całego kraju w listopadzie 2023 r. Jego celem było sprawdzenie procedur systemu zarządzania kryzysowego w zakresie ostrzegania i alarmowania ludności cywilnej oraz wojska o zagrożeniach z powietrza. Organizatorem ćwiczenia było Rządowe Centrum Bezpieczeństwa we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji oraz Ministerstwem Obrony Narodowej. W trakcie LIBERO 2023 wielokrotnie uruchamiano system alarmowy (syreny) i testowano dystrybucję komunikatów alarmowych, symulując scenariusz ataku rakietowego na Polskę. Takie ćwiczenia pozwalają ocenić sprawność łączności alarmowej między RCB, centrami wojewódzkimi i lokalnymi, sprawdzić skuteczność systemu Alert RCB (rozesłania SMS z ostrzeżeniem) oraz gotowość społeczeństwa do właściwego reagowania na sygnały alarmowe. Innym przykładem z ostatnich lat są cykliczne ćwiczenia RENEGADE/SAREX, organizowane we współpracy z Siłami Zbrojnymi, które symulują sytuacje naruszenia przestrzeni powietrznej przez statek powietrzny stanowiący zagrożenie (Renegade) oraz akcje poszukiwawczo-ratownicze (Sarex). W ich ramach testowane jest m.in. uruchamianie systemów ostrzegania przed uderzeniami z powietrza oraz współdziałanie wojska, RCB i służb cywilnych w przypadku konieczności ewakuacji lub ratowania ludności. Na poziomie resortowym również odbywają się ćwiczenia obronne i kryzysowe – np. MON i MSWiA organizowały w 2023 r. ćwiczenie pk. RADOMKA 2023, sprawdzające przygotowanie służb mundurowych, medycznych oraz wydziałów zarządzania kryzysowego na wypadek sytuacji obronnej na zapleczu działań wojskowych. Ćwiczenia krajowe są często przygotowywane w oparciu o scenariusze zagrożeń uznane za najbardziej prawdopodobne lub najbardziej niebezpieczne. Scenariusze te wynikają z ocen ryzyka i Raportu o zagrożeniach bezpieczeństwa narodowego, stanowiącego przegląd strategiczny zagrożeń. Przykładowo, po doświadczeniach z lat 2019-2020 do priorytetowych scenariuszy ćwiczonych włączono zarządzanie pandemią oraz kryzys migracyjny. W 2020 r. (jeszcze

w trakcie trwania realnej pandemii COVID-19) przeprowadzono serię ćwiczeń sztabowych z zakresu dystrybucji szczepionek i utrzymania ciągłości działania instytucji państwowych. Z kolei w 2021 r., w obliczu narastającego napięcia na granicy z Białorusią, zorganizowano ćwiczenia z symulacją masowego napływu uchodźców i konieczności rozlokowania dużej liczby osób w różnych regionach – co przygotowało administrację na wyzwania, jakie rzeczywiście wystąpiły w 2022 r. po wybuchu wojny na Ukrainie. Nie tylko administracja ćwiczy – równie ważne są treningi służb ratunkowych (Państwowej Straży Pożarnej, Policji, ratownictwa medycznego) o zasięgu krajowym lub regionalnym. Strażacy organizują corocznie duże manewry ratownicze, często z udziałem oddziałów z kilku województw (np. manewry pk. RATOWNIK lub ćwiczenia przeciwpowodziowe w dorzeczu dużych rzek). Pozwala to zgrać działania jednostek spoza macierzystego terenu – co bywa nieocenione przy wzajemnej pomocy międzywojewódzkiej podczas powodzi czy po przejściu gwałtownych wichur. Ważnym elementem przygotowań są również gry decyzyjne i symulacje komputerowe, pozwalające trenować kadrę kierowniczą w podejmowaniu decyzji kryzysowych bez angażowania realnych sił. Przykładowo, województwa prowadzą okresowo gry symulujące przebieg katastrofy (np. skażenie chemiczne czy rozległy black-out energetyczny) – wojewoda wraz z członkami WZZK muszą wówczas przećwiczyć podejmowanie decyzji, wydawanie komunikatów dla ludności, uruchamianie rezerw itp. Całość tych działań – planowania i ćwiczeń – służy budowaniu scenariuszy reagowania. Scenariusze te to rozwinięte opisy hipotetycznych sytuacji kryzysowych, wraz z przypisaniem ról poszczególnym podmiotom i krok po kroku rozpisany przebiegiem zdarzeń i reakcji. Krajowe plany i instrukcje operacyjne często zawierają tzw. wariantowe scenariusze – np. scenariusz powodzi powolnej vs powodzi błyskawicznej, scenariusz ataku terrorystycznego chemicznego vs biologicznego, itp. Dzięki temu osoby odpowiedzialne (wojewodowie, ministrowie, służby) dysponują swoistym zbiorem receptur na różne kryzysy. Oczywiście życie może zaskoczyć i rzeczywistość nie przebiega dokładnie według scenariusza, jednak posiadanie wcześniej przećwiczonych schematów działania skraca czas reakcji i zmniejsza ryzyko popełnienia błędów w chaosie kryzysu. Warto nadmienić, że Polska aktywnie uczestniczy także w ćwiczeniach międzynarodowych w ramach Unijnego Mechanizmu Ochrony Ludności i struktur

NATO⁴¹⁴. Ćwiczenia te pozwalają na wymianę doświadczeń i wypracowanie procedur współpracy transgranicznej. Przykładem może być ćwiczenie EU MOLDEX 2017, gdzie polscy strażacy ćwiczyli wspólnie z innymi krajami UE reagowanie na trzęsienie ziemi w Mołdawii. Również co roku NATO organizuje ćwiczenie zarządzania kryzysowego CMX, w którym Polska uczestniczy na szczeblu polityczno-wojskowym. Te wszystkie inicjatywy przekładają się na lepsze przygotowanie krajowego systemu na scenariusze ponadregionalne i ponadnarodowe.

Kolejny rodzaj stanowią kryzysy ponadregionalne. To takie kryzysy, które rozciągają się na obszar większy niż jedno województwo lub zagrażają funkcjonowaniu państwa jako całości. Przykładami kryzysów ponadregionalnych z ostatnich lat były m.in. katastrofalna powódź w 2010 r. (dotykająca jednocześnie kilka województw), pandemia COVID-19 od 2020 r. (o charakterze ogólnokrajowym), czy długotrwały blackout energetyczny (hipotetyczny, ale analizowany w scenariuszach jako zagrożenie obejmujące wiele regionów). Reagowanie na tego typu sytuacje wymaga uruchomienia mechanizmów centralnych oraz ścisłego współdziałania między województwami. Pierwszym mechanizmem jest zwołanie na szczeblu centralnym posiedzenia Rządowego Zespołu Zarządzania Kryzysowego lub powołanie rządowego sztabu kryzysowego. Premier, korzystając z raportów RCB i wojewodów, może w trybie pilnym zebrać kluczowych ministrów i służby, aby ocenić sytuację i podjąć decyzje o użyciu sił i środków z poziomu krajowego. Takie posiedzenia RZZK miały miejsce m.in. na początku pandemii koronawirusa w marcu 2020 r., podczas kryzysu na granicy w 2021 r., czy też w trakcie kryzysu zanieczyszczenia Odry w sierpniu 2022 r. – wówczas rząd centralnie koordynował działania zaradcze na różnych odcinkach rzeki (w kilku województwach jednocześnie). RZZK wypracowuje wspólne kierunki działania, np. rekomenduje wprowadzenie stanu klęski żywiołowej lub innych nadzwyczajnych instrumentów prawnych, jeżeli zwykłe środki są niewystarczające. Warto przypomnieć, że polskie prawo przewiduje trzy stany nadzwyczajne (stan klęski żywiołowej, wyjątkowy i wojenny) – spośród

⁴¹⁴ S. Żurawski, J. Nowicka, Z. Ciekankowski, Systemy zarządzania kryzysowego w wybranych państwach NATO, w: *Prakseologia w zarządzaniu i dowodzeniu*, t. 8: *Etyczność w dowodzeniu*, W. Kieżun, J. Wołęjszo, K. Mikurenda (red.), Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2020, s. 41-54.

nich stan klęski żywiołowej może być wprowadzony przez Radę Ministrów na wniosek właściwego ministra lub wojewody, gdy katastrofa naturalna lub techniczna zagraża w dużej skali i wymaga użycia nadzwyczajnych środków we współdziałaniu różnych służb^{415,416}. W III Rzeczypospolitej stan klęski żywiołowej został formalnie wprowadzony wyjątkowo rzadko. W praktyce, mimo wystąpienia zdarzeń o charakterze masowym i długotrwałym – takich jak powódź z 2010 r. czy pandemia COVID-19 – decyzja o uruchomieniu tego konstytucyjnego instrumentu nie została podjęta, co w debacie publicznej łączono z uwarunkowaniami prawnymi i politycznymi, w tym konsekwencjami dla funkcjonowania instytucji państwa. Jednocześnie w sytuacjach o podwyższonym poziomie zagrożenia stosowano rozwiązania nadzwyczajne w trybach przewidzianych w ustawodawstwie zwykłym, w szczególności poprzez regulacje szczególne (tzw. specustawy) oraz akty wykonawcze, a także poprzez uruchamianie instrumentów takich jak stopnie alarmowe oraz reżimy sanitarne (np. stan epidemii na podstawie przepisów dotyczących chorób zakaźnych). Drugim istotnym mechanizmem reagowania na kryzysy o zasięgu ponadregionalnym jest uruchamianie zasobów centralnych państwa, w tym rezerw strategicznych oraz wsparcia logistycznego. W sytuacji, gdy skala zdarzenia przekracza możliwości reagowania na poziomie regionalnym, aktywowane są zasoby pozostające w dyspozycji administracji centralnej. Rządowa Agencja Rezerw Strategicznych może uruchamiać rezerwy materiałowe obejmujące m.in. środki niezbędne do zabezpieczenia infrastruktury i ludności, takie jak paliwo dla agregatów prądotwórczych, zasoby żywnościowe dla osób ewakuowanych, sprzęt przeciwpowodziowy (np. pompy) oraz środki i wyposażenie wykorzystywane w ochronie zdrowia. W okresie pandemii COVID-19 realizowano dystrybucję zasobów ochrony osobistej oraz sprzętu medycznego, natomiast w przypadku zdarzeń hydrometeorologicznych kierowane bywało wsparcie w postaci agregatów prądotwórczych, kontenerów tymczasowych lub elementów infrastruktury zastępczej.

⁴¹⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78 poz. 483, art. 228 oraz art. 232).

⁴¹⁶ Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62, poz. 558 z późn. zm.).

Uzupełnieniem wsparcia centralnego jest mechanizm relokacji zasobów kadrowych i sprzętowych pomiędzy regionami. W szczególności system ratowniczy Państwowej Straży Pożarnej przewiduje możliwość kierowania do działań tzw. odwodów krajowych, tj. kompanii oraz wyspecjalizowanych modułów ratowniczych z innych województw, w celu wzmocnienia sił lokalnych w sytuacji zdarzeń o dużej skali. Rozwiązanie to umożliwia elastyczne zwiększenie potencjału reagowania w rejonie dotkniętym kryzysem oraz zapewnia spójność organizacyjną działań ratowniczych na poziomie krajowym⁴¹⁷. Przykładowo, w następstwie nawałnic na Pomorzu w 2017 r. do działań skierowano siły i środki Państwowej Straży Pożarnej oraz jednostek włączonych do Krajowego Systemu Ratowniczo-Gaśniczego z wielu województw, w celu realizacji zadań wymagających znacznego zaangażowania zasobów, w tym usuwania skutków zniszczeń w drzewostanie, udrażniania ciągów komunikacyjnych oraz zabezpieczania uszkodzonych obiektów budowlanych. Analogiczne mechanizmy stosowane są w przypadku działań długotrwałych i specjalistycznych, takich jak poszukiwania osób zaginionych, w których wykorzystywane bywają zespoły poszukiwawczo-ratownicze z psami, kierowane do wsparcia z innych regionów. Międzywojewódzka relokacja zasobów stanowi trwały element krajowego systemu reagowania, umożliwiający elastyczne wzmacnianie potencjału operacyjnego w rejonach szczególnie obciążonych skutkami zdarzeń. Proces ten podlega koordynacji na poziomie centralnym, w szczególności przez Komendę Główną Państwowej Straży Pożarnej oraz w ramach mechanizmów obiegu informacji i koordynacji działań na poziomie krajowym, z uwzględnieniem konieczności utrzymania wymaganej gotowości operacyjnej w województwach przekazujących siły i środki.

Kolejnym instrumentem wykorzystywanym w reagowaniu na kryzysy o zasięgu ponadregionalnym jest wsparcie Sił Zbrojnych Rzeczypospolitej Polskiej. W warunkach normalnego funkcjonowania państwa Siły Zbrojne nie podlegają organom administracji terenowej, natomiast w sytuacjach kryzysowych mogą zostać użyte do realizacji zadań o charakterze pomocniczym, w szczególności w obszarze logistyki, ewakuacji, zabezpieczenia

⁴¹⁷ G. Pietrek, Poziomy, struktura i zadania systemu zarządzania kryzysowego administracji rządowej, Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu, nr 3(161), 2011, s. 376-388.

infrastruktury oraz wsparcia działań ratowniczych. Zasadniczą podstawę prawną stanowi w tym zakresie ustawa o zarządzaniu kryzysowym, która przewiduje możliwość przekazania oddziałów i pododdziałów Sił Zbrojnych do dyspozycji wojewody na jego wniosek, na podstawie decyzji Ministra Obrony Narodowej, w celu wykonywania zadań związanych z reagowaniem kryzysowym⁴¹⁸. Dodatkową podstawę ogólną dla organizacji i użycia Sił Zbrojnych stanowi ustawa o obronie Ojczyzny⁴¹⁹. W praktyce wsparcie wojska może obejmować m.in. ewakuację ludności, dostarczanie wody i środków pierwszej potrzeby, prace inżynierskie i odtworzeniowe, odśnieżanie, zabezpieczanie ciągów komunikacyjnych oraz działania porządkowe prowadzone w ramach właściwych reżimów prawnych i kompetencyjnych. Doświadczenia ostatnich lat potwierdzają operacyjną użyteczność tego instrumentu, w tym w zakresie wsparcia zadań związanych z kryzysem migracyjnym na granicy oraz przedsięwzięć logistyczno-organizacyjnych realizowanych w okresie pandemii.

W kryzysach o dużej skali kluczowe znaczenie ma również koordynacja przepływu informacji i decyzji, tak, aby zapewnić spójność poleceń kierowanych do podmiotów wykonawczych oraz ograniczyć ryzyko rozbieżności decyzyjnych. W sytuacjach ogólnokrajowych Rządowe Centrum Bezpieczeństwa pełni funkcję węzła koordynacyjno-informacyjnego w systemie zarządzania kryzysowego, wspierając obsługę procesów decyzyjnych na szczeblu centralnym i zapewniając dystrybucję informacji w pionie administracji. W praktyce do narzędzi o znaczeniu operacyjnym należy m.in. system Alert RCB, umożliwiający przekazywanie ostrzeżeń ludności na określonym obszarze lub – w razie potrzeby – w skali ogólnokrajowej. Równolegle przygotowywane i dystrybuowane są raporty sytuacyjne, które w warunkach eskalacji zagrożenia mogą być aktualizowane z większą częstotliwością w celu zapewnienia bieżącej świadomości sytuacyjnej interesariuszy. Współpraca między województwami przyjmuje również formę bezpośrednią, w tym uzgadniania relokacji zasobów, przyjmowania osób ewakuowanych lub koordynacji działań logistycznych. Ustrukturyzowaną formą takiej współpracy są narady prowadzone w resorcie właściwym do

⁴¹⁸ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm. art. 11).

⁴¹⁹ Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655 z późn. zm.).

spraw wewnętrznych oraz wideokonferencje koordynacyjne z udziałem wojewodów, wykorzystywane zwłaszcza w sytuacjach wymagających równoważenia obciążeń pomiędzy regionami (np. w przypadku masowego napływu uchodźców).

W sytuacjach podwyższonego zagrożenia wykorzystywane mogą być również instrumenty formalne służące podniesieniu poziomu gotowości systemu bezpieczeństwa, w tym stopnie alarmowe ALFA, BRAVO, CHARLIE i DELTA oraz stopnie alarmowe CRP, uruchamiane w związku z ryzykiem zdarzeń terrorystycznych i cybernetycznych. Ich stosowanie wpływa na intensyfikację działań prewencyjnych oraz zwiększenie czujności służb w skali ponadregionalnej.

W przypadku kryzysów przekraczających zdolności państwa uruchamiane są mechanizmy wsparcia międzynarodowego, w szczególności w ramach Unii Europejskiej i NATO. Istotnym narzędziem pozostaje Unijny Mechanizm Ochrony Ludności, umożliwiający uruchamianie zasobów ratowniczych innych państw oraz koordynację pomocy rzeczowej i operacyjnej. Wsparcie międzynarodowe może przyjmować postać zarówno zasobów fizycznych (np. modułów ratowniczych, sprzętu specjalistycznego), jak i wsparcia logistycznego oraz wymiany know-how. W obszarze zagrożeń hybrydowych – obejmujących m.in. cyberataki i dezinformację – współpraca międzynarodowa ma dodatkowo wymiar analityczny i operacyjny, jednak oceny kontrolne wskazywały w ostatnich latach na potrzebę bardziej jednolitego uwzględniania tych zagrożeń w dokumentach planistycznych i pracach zespołów kryzysowych.

Doświadczenia ostatnich lat ujawniły jednocześnie zarówno mocne strony krajowego systemu zarządzania kryzysowego, jak i obszary wymagające dalszej poprawy. Wskazuje się, że system wykazuje zdolność mobilizacji i relatywnie sprawnej koordynacji w sytuacjach o dużej dynamice, natomiast trwałymi wyzwaniem pozostają niedobory kadrowe na poziomie części jednostek samorządu terytorialnego, nierówna jakość planowania oraz ograniczona standaryzacja szkoleń i ćwiczeń. W konsekwencji postulowane jest wzmacnianie profesjonalizacji kadr, rozwój praktyk ćwiczeniowych i scenariuszowych oraz zwiększenie spójności międzyresortowej, co ma ograniczać ryzyko „silosowości” kompetencyjnej. W wymiarze systemowym kierunek zmian zmierza do lepszej integracji elementów zarządzania

kryzysowego, ochrony ludności i innych polityk bezpieczeństwa w ramach podejścia całościowego (comprehensive approach), z naciskiem na zdolność adaptacji do ewoluującej natury zagrożeń. Mechanizmy reagowania na kryzysy ponadregionalne w Polsce opierają się na zasadzie stopniowania wsparcia: lokalne podmioty realizują działania pierwszej reakcji, natomiast koordynacja, relokacja zasobów, uruchamianie rezerw oraz instrumenty prawne i logistyczne wzmacniane są na szczeblu regionalnym i centralnym. Efektywność tego modelu zależy od jakości koordynacji pionowej i poziomej, sprawności obiegu informacji, interoperacyjności służb oraz konsekwentnego doskonalenia procedur w oparciu o doświadczenia kolejnych zdarzeń.

5.3. Zarządzanie kryzysowe w Unii Europejskiej i NATO

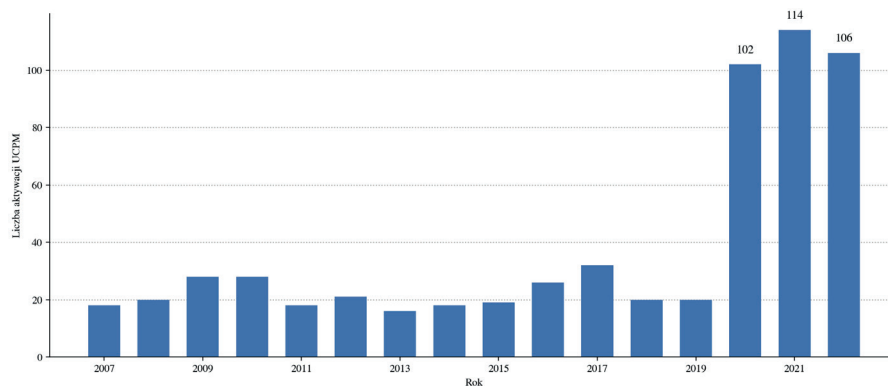
Zarządzanie kryzysowe w Unii Europejskiej i NATO obejmuje skoordynowane działania państw członkowskich oraz instytucji międzynarodowych w zakresie zapobiegania, przygotowania i reagowania na sytuacje nadzwyczajne, zwłaszcza o charakterze transgranicznym lub przekraczającym możliwości pojedynczego państwa. W ramach UE kluczową rolę pełni Unijny Mechanizm Ochrony Ludności (UCPM), który umożliwia uruchamianie pomocy ratowniczej i humanitarnej oraz koordynację zasobów przez ERCC. Z kolei NATO rozwija instrumenty cywilnego reagowania kryzysowego (EADRCC) oraz programy wzmacniania odporności cywilnej, traktowane jako element bezpieczeństwa zbiorowego.

Unijny Mechanizm Ochrony Ludności (ang. Union Civil Protection Mechanism, UCPM) jest podstawowym instrumentem koordynacji pomocy ratowniczej i humanitarnej w sytuacjach nadzwyczajnych na poziomie europejskim. Został ustanowiony w 2001 r. w celu wspólnego przygotowania, zapobiegania i reagowania na klęski żywiołowe oraz katastrofy spowodowane działalnością człowieka, które swoją skalą przerastają możliwości reagowania państwa dotkniętego zdarzeniem. Mechanizm ten stanowi platformę współdziałania państw uczestniczących (wszystkie państwa UE oraz obecnie 8 państw stowarzyszonych spoza UE, m.in. Norwegia, Islandia, Serbia, Turcja) z instytucjami unijnymi odpowiedzialnymi za ochronę ludności. W ramach Mechanizmu udzielana jest pomoc polegająca na wysyłaniu

wyspecjalizowanych, wyposażonych zespołów ratowniczych (tzw. modułów) oraz dostarczaniu pomocy rzeczowej i eksperckiej. Udział w Mechanizmie opiera się na dobrowolnym udostępnianiu przez państwa swoich zasobów do wspólnej europejskiej puli. Gdy któreś państwo (członkowskie UE lub jedno z państw stowarzyszonych) zostanie dotknięte katastrofą przekraczającą jego możliwości, może oficjalnie zwrócić się o pomoc za pośrednictwem Mechanizmu. Co ważne, o wsparcie mogą wnioskować nie tylko uczestnicy Mechanizmu – w wyjątkowych sytuacjach prośbę o pomoc kierować mogą również inne państwa świata lub uprawnione organizacje międzynarodowe. Po otrzymaniu takiego apelu uruchamiane są działania w ramach UCPM. W Brukseli działa całodobowe Centrum Koordynacji Reagowania Kryzysowego (ERCC), które monitoruje sytuacje kryzysowe i po aktywacji Mechanizmu koordynuje napływające oferty pomocy oraz organizuje ich sprawne dostarczenie do kraju poszkodowanego⁴²⁰. Informacje o potrzebach i dostępnych zasobach wymieniane są za pomocą specjalnej platformy (dawniej Monitoring and Information Centre, MIC) obsługiwanej przez Komisję Europejską. Każde państwo uczestniczące ma krajowy punkt kontaktowy – w Polsce funkcję tę pełni Komenda Główna Państwowej Straży Pożarnej, która odbiera i przekazuje informacje dotyczące Mechanizmu.

Unijny Mechanizm Ochrony Ludności jest aktywowany stosunkowo często przy różnego rodzaju zagrożeniach. W latach 2007-2019 uruchamiano go średnio ok. 25 razy rocznie, najczęściej w związku z pożarami lasów (średnio 6,5 raza na rok) oraz powodzią (3,6 raza na rok). Rządziej dotyczyły sytuacji takich jak ekstremalne zjawiska pogodowe, trzęsienia ziemi, skażenia środowiska czy incydenty chemiczne. W ostatnich latach liczba interwencji znacząco wzrosła – m.in. z powodu pandemii COVID-19 i wojny w Ukrainie. Dla porównania, w 2019 r. Mechanizm uruchomiono 20 razy, natomiast w 2020 r. aż 102 razy, w 2021 r. 114 razy, a w 2022 r. 106 razy. Dane te zestawiono na rysunku 15.

⁴²⁰ Rada Unii Europejskiej, Unijna ochrona ludności, <https://www.consilium.europa.eu/pl/policies/civil-protection/>, [dostęp: 10.10.2025].



Rysunek 15. Liczba aktywacji Unijnego Mechanizmu Ochrony Ludności (UCPM) w latach 2007-2022

Źródło: opracowanie własne na podstawie danych: Rada Unii Europejskiej, Unijna ochrona ludności, <https://www.consilium.europa.eu/pl/policies/civil-protection/>, [dostęp: 10.10.2025].

Oznacza to, że okres 2020-2022 był rekordowy pod względem liczby aktywacji UCPM. Gwałtowny wzrost wynikał z globalnego kryzysu zdrowotnego (COVID-19) oraz konieczności wsparcia Ukrainy i państw sąsiednich w obliczu wojny. Również nasilające się zjawiska naturalne przyczyniły się do większej liczby uruchomień Mechanizmu – np. fala pożarów lasów w Europie latem 2022 r. sprawiła, że tamtego roku szczególnie często koordynowano pomoc gaśniczą. Mechanizm działa zarówno wewnątrz Unii, jak i poza jej obszarem – pomoc kierowana jest tam, gdzie jest potrzebna. Przykładowo w 2022 r. wsparcie otrzymało aż 72 kraje świata, przy czym 30 aktywacji dotyczyło zdarzeń na terytorium UE, a 76 poza UE. Największą operacją w historii Mechanizmu okazała się pomoc dla Ukrainy po agresji rosyjskiej – w 2022 r. poprzez UCPM dostarczono na Ukrainę 84 tys. ton pomocy materialnej (generatory prądu, schronienia, leki, żywność, pompy itp.), a także ewakuowano 1700 chorych i rannych do szpitali w 18 krajach europejskich⁴²¹. Równolegle Mechanizm wsparł kraje frontowe – m.in. Polskę, Słowację czy Mołdawię – w radzeniu sobie z masowym napływem uchodźców z Ukrainy. Była to bezprecedensowa skala zaangażowania i przykład, jak Mechanizm może zostać użyty także w sytuacji kryzysu uchodźczego. Mechanizm służy solidarności i wzajemnej pomocy między

⁴²¹ Rada Unii Europejskiej, Unijna ochrona ludności, <https://www.consilium.europa.eu/pl/policies/civil-protection/>, [dostęp: 10.10.2025].

państwami – Polska również aktywnie z niego korzysta, zarówno jako biorca pomocy w sytuacjach krajowych katastrof, jak i dawca wsparcia dla innych państw. Przykładem wykorzystania UCPM przez Polskę była katastrofalna powódź, która nawiedziła nasz kraj w maju 2010 r. Skala zniszczeń i przewidywane kolejne ulewę groziły przekroczeniem możliwości reagowania służb krajowych, dlatego 20 maja 2010 r. Polska oficjalnie uruchomiła Mechanizm Ochrony Ludności, zwracając się do partnerów w Europie o pomoc. Wniosek dotyczył pilnego przysłania wysokowydajnych pomp do wody oraz dodatkowych zespołów ratowniczych. Dzięki Mechanizmowi już w kilkadziesiąt minut od apelu oferty pomocy zaczęły napływać – Francja zaoferowała w ciągu godziny cztery potężne pompy o wydajności 5400 m³/h każda, kilka mniejszych pomp oraz wsparcie logistyczne i techniczne. Ofertę tę niezwłocznie przyjęto, a francuskie grupy ratunkowe wyruszyły do Polski i dotarły na zalane tereny w ciągu 15 godzin. Również Niemcy szybko zadeklarowały przysłanie pięciu wysokowydajnych pomp (15 m³/min) oraz kolejnego sprzętu. Wsparcie międzynarodowe pomogło opanować sytuację – przypadek ten często przywołuje się jako dowód skuteczności unijnej solidarności w obliczu klęski żywiołowej.

Z kolei jako dawca pomocy Polska regularnie oferuje swoje zasoby innym państwom dotkniętym katastrofami za pośrednictwem UCPM. Bardzo wymownym przykładem była akcja gaszenia rekordowych pożarów lasów w Szwecji latem 2018 r. W odpowiedzi na oficjalny apel władz Szwecji wy stosowany poprzez Mechanizm, polski rząd zdecydował o wysłaniu dużego kontyngentu ratowniczego. Już następnego dnia, 21 lipca 2018 r., do Szwecji promem wyruszyła grupa prawie 140 polskich strażaków z 44 pojazdami gaśniczymi, głównie z województw zachodniopomorskiego i wielkopolskiego. Polscy strażacy przez dwa tygodnie wspólnie ze służbami szwedzkimi walczyli z pożarami, będąc w pełni samowystarczalni logistycznie (zapewnili sobie własne namioty, wyżywienie i zaplecze medyczne). Misja ta została bardzo pozytywnie oceniona i stała się symbolem europejskiej współpracy ratowniczej – łącznie w akcji w Szwecji brało udział 340 ratowników z różnych krajów Europy, w tym silna polska grupa stanowiąca największy kontyngent zagraniczny. Podobnie Polska wysyłała pomoc m.in. do Grecji (pożary lasów), Albanii (trzęsienie ziemi) czy na Karaiby (huragan) – zawsze wtedy, gdy nasi partnerzy zwracali się o wsparcie w ramach Mechanizmu.

Warto podkreślić, że Polska jest aktywnym uczestnikiem rozwoju Mechanizmu Ochrony Ludności. Bierze udział w inicjatywach doskonalących europejski system reagowania kryzysowego – np. w projektach tworzenia wspólnych rezerw sprzętowych rescEU. Inicjatywa rescEU, zapoczątkowana w 2019 r., to dodatkowa „ostatnia deska ratunku” w ramach UCPM – strategiczna rezerwa kluczowych zasobów ratowniczych finansowana ze środków UE, uruchamiana gdy możliwości poszczególnych państw są niewystarczające. Obejmuje ona m.in. flotę samolotów gaśniczych, zapasy sprzętu medycznego, mobilne szpitale, rezerwy w zakresie CBRN (chemiczne, biologiczne, radiologiczne, nuklearne) czy właśnie wysokowydajne pomp przeciwpowodziowe i moduły tymczasowych schronień⁴²². Polska zaangażowała się w budowę tych zdolności – nasz kraj pełni rolę gospodarza dedykowanej zdolności lotniczej rescEU, utrzymując w gotowości trzy samoloty (w tym specjalistyczny samolot ewakuacji medycznej) na potrzeby misji ratunkowych UE. Ponadto Rządowa Agencja Rezerw Strategicznych realizuje obecnie aż 7 projektów w ramach rescEU o łącznej wartości blisko 500 mln euro, obejmujących m.in. utworzenie rezerw do dekontaminacji CBRN, zapasów medycznych, magazynów sprzętu energetycznego (agregatów prądotwórczych), modułów tymczasowych schronień, a także zdolności transportowo-logistycznych. Dzięki temu Polska stała się jednym z filarów unijnego systemu odporności cywilnej – rozwijając własne zasoby, jednocześnie wzmacnia bezpieczeństwo całej wspólnoty⁴²³.

Unijny Mechanizm Ochrony Ludności jest dziś kluczowym narzędziem zarządzania kryzysowego w Europie, z którego Polska aktywnie korzysta. Zapewnia on dwukierunkową solidarność: umożliwia szybkie otrzymanie pomocy zagranicznej w razie katastrofy krajowej, a zarazem pozwala Polsce nieść pomoc innym, co wzmacnia naszą pozycję i wiarygodność na arenie międzynarodowej. Mechanizm ten – wraz z towarzyszącymi instrumentami (jak rescEU) – podnosi zdolność reagowania na największe współczesne zagrożenia, od klęsk żywiołowych po kryzysy zdrowotne i humanitarne.

⁴²² Rada Unii Europejskiej, Unijna ochrona ludności, <https://www.consilium.europa.eu/pl/policies/civil-protection>, [dostęp: 10.10.2025].

⁴²³ Rządowa Agencja Rezerw Strategicznych, Projekty EU, <https://www.gov.pl/web/rars/projekty-eu>, [dostęp: 10.10.2025].

Istotną rolę w reagowaniu kryzysowym pełni NATO. Choć Sojusz Północnoatlantycki postrzegany jest głównie jako organizacja obronna, od wielu lat rozwija również zdolności w obszarze cywilnego reagowania kryzysowego. Podstawowym mechanizmem NATO do koordynacji pomocy w sytuacjach klęsk i katastrof jest Euro-Atlantic Disaster Response Coordination Centre (EADRCC) – Euroatlantyckie Centrum Koordynacji Reagowania na Katastrofy. Centrum to powstało w 1998 r. i obecnie stanowi główne narzędzie Sojuszu do reagowania na sytuacje nadzwyczajne o charakterze niemilitarnym. EADRCC działa całodobowo w kwaterze głównej NATO w Brukseli i jest dostępne dla wszystkich państw sojuszniczych oraz krajów partnerskich NATO (łącznie ponad 70 państw)⁴²⁴. Jego zasadniczą funkcją jest pośredniczenie między państwami zgłaszającymi zapotrzebowanie na pomoc a tymi oferującymi wsparcie – pełni więc rolę centrum koordynacji ofert i próśb o pomoc w ramach społeczności euroatlantyckiej. W przypadku wystąpienia katastrofy międzynarodowej to poszczególne państwa decydują suwerennie, czy i jakie wsparcie udzielą, na podstawie informacji rozpowszechnianych przez EADRCC. Innymi słowy, Centrum działa jako clearing house – zbiera od państwa poszkodowanego listę potrzeb oraz przekazuje ją sojusznikom i partnerom, którzy następnie dobrowolnie deklarują pomoc. Taki model sprzyja maksymalnemu wykorzystaniu dostępnych zasobów i unikaniu dublowania wysiłków, podobnie jak ma to miejsce w unijnym mechanizmie. Warto zaznaczyć, że EADRCC od początku ściśle współpracuje z ONZ (UNOCHA) oraz – tam gdzie to możliwe – z unijnym ERCC, tak, aby działania NATO komplementarnie uzupełniały międzynarodowe operacje humanitarne. Przykładowo, podczas dużych katastrof NATO oferuje wsparcie logistyczne (np. wojskowy transport lotniczy ciężkich ładunków) i koordynację polityczno-wojskową, uzupełniając cywilne wysiłki ONZ czy UE. EADRCC może zostać uruchomione w reakcji na bardzo szerokie spektrum sytuacji kryzysowych – od klęsk żywiołowych (powódzie, pożary, trzęsienia ziemi, huragany), przez katastrofy spowodowane przez człowieka (awarie przemysłowe, skażenia CBRN), aż po incydenty terrorystyczne czy sytuacje związane z konfliktem zbrojnym. Co istotne, mandat EADRCC obejmuje

⁴²⁴ L. Speranza, Six reasons NATO's Euro-Atlantic Disaster Response Coordination Centre is important for our future security, Atlantic Council, New Atlanticist, 2020.

także sytuacje kryzysowe w warunkach operacji wojskowych i obrony kolektywnej – Centrum może koordynować pomoc cywilną również w trakcie konfliktu lub ataku na państwo sojusznicze⁴²⁵. Takiej roli nie pełni unijny mechanizm, co czyni narzędzia NATO unikatowymi na wypadek wojny. W ostatnich latach EADRCC odegrało ważną rolę w szeregu znaczących kryzysów. Podczas pandemii COVID-19 (2020-2021) Centrum kilkadziesiąt razy uruchamiało procedury pomocy – wspomogło m.in. transport pilnie potrzebnych materiałów medycznych (masek, rękawic, płynów dezynfekcyjnych, respiratorów) pomiędzy krajami sojuszniczymi. Przykładowo, wiosną 2020 r. na prośbę Hiszpanii i Włoch zmagających się z eksplozją zachorowań, EADRCC skoordynowało dostarczenie samolotami NATO setek tysięcy maseczek i dziesiątek respiratorów z Turcji, Niemiec i Czech. Ułatwiono także procedury celne, tranzytowe i przekraczanie granic dla konwojów z pomocą. Innym przykładem była reakcja NATO na katastrofalne trzęsienie ziemi w Turcji w lutym 2023 r. – największy kataklizm naturalny na obszarze Sojuszu w jego historii. EADRCC uruchomiło wówczas zarówno komponent cywilny (m.in. koordynując wysyłanie przez państwa członkowskie namiotów, koców, generatorów i ekip ratowniczych), jak i wsparcie wojskowe (oddano do dyspozycji tureckich władz okręty i samoloty do transportu, a nawet zaangażowano inżynierów wojskowych do usuwania gruzów). Wsparcie objęło też organizację tymczasowych schronień dla ocalałych – NATO rozstawiło dla Turcji namiotowe miasteczka zdolne pomieścić tysiące ludzi. Równie intensywnie EADRCC jest wykorzystywane od 2022 r. w związku z wojną rosyjsko-ukraińską – Sojusz za pośrednictwem Centrum koordynuje pomoc dla ludności Ukrainy (np. przekazywanie ambulansów, zaopatrzenia medycznego, szkolenie ukraińskich ratowników) oraz wsparcie dla państw przyjmujących uchodźców. NATO uruchomiło również specjalny fundusz pomocy dla Ukrainy, a EADRCC ściśle współdziała z polskimi i słowackimi władzami przy logistycznej obsłudze transportu pomocy przez granicę. Poza tym głośnymi przykładami, EADRCC ma na swoim koncie dziesiątki mniej znanych operacji na przestrzeni lat. Centrum koordynowało m.in. międzynarodową pomoc po huraganie Katrina w USA (2005 r.), organizowało

⁴²⁵ Traktat Północnoatlantycki, sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r. Nr 87, poz. 970, art. 5).

wsparcie przeciwpowodziowe dla Albanii i Czarnogóry, pomagało w gaszeniu pożarów lasów na Łotwie i w Izraelu, a także reagowało na klęski zimowe na Bałkanach. Zakres geograficzny i tematyczny tych misji jest bardzo szeroki – sięga poza obszar traktatowy NATO, obejmując także partnerów (np. Izrael) oraz działania humanitarne na prośbę ONZ. Do zadań EADRCC należy ponadto koordynacja odpowiedzi na potencjalne ataki terrorystyczne czy incydenty z użyciem broni masowego rażenia (CBRN). W razie takich zagrożeń Centrum może szybko uruchomić procedury udzielenia wsparcia poszkodowanemu państwu poprzez zmobilizowanie specjalistycznych zespołów (np. grup dekontaminacyjnych, medycznych) z innych krajów. Ta wszechstronność sprawia, że EADRCC jest ważnym elementem zdolności adaptacyjnych NATO w obliczu współczesnych wyzwań bezpieczeństwa.

Działalność EADRCC to nie tylko reagowanie po fakcie, ale też szeroko zakrojone działania prewencyjne i szkoleniowe, które wpisują się w wysiłki NATO na rzecz wzmacniania odporności cywilnej swoich członków. Centrum regularnie organizuje wielostronne ćwiczenia reagowania na sytuacje kryzysowe z udziałem państw sojuszniczych i partnerskich. Od początku istnienia zrealizowano łącznie 19 dużych ćwiczeń ochrony ludności – ostatnie odbyło się w 2021 r. w Macedonii Północnej, kolejne planowane jest na wrzesień 2025 r. w Bułgarii. Scenariusze tych manewrów obejmują m.in. reagowanie na trzęsienia ziemi, powodzie, zamachy terrorystyczne czy ataki chemiczne. Ćwiczenia EADRCC służą doskonaleniu interoperacyjności – umożliwiają służbom ratowniczym z różnych krajów wspólne trenowanie procedur i komunikacji, tak, aby w realnej akcji móc działać sprawnie ramię w ramię. Przy okazji testowane są nowatorskie technologie wspierające reagowanie kryzysowe. Przykładowo, w trakcie ćwiczeń w Ukrainie i Bośni testowano transgraniczny system telemedycyny, wirtualną rzeczywistość do symulacji akcji ratunkowych oraz wykorzystanie mediów społecznościowych w zarządzaniu kryzysowym. Takie inicjatywy podnoszą zdolności państw do radzenia sobie z zagrożeniami i wpisują się w szerszy wysiłek NATO na rzecz budowania odporności.

NATO traktuje odporność cywilną jako kluczowy element kolektywnej obrony i bezpieczeństwa. Zgodnie z Traktatem Waszyngtońskim każdy sojusznik jest zobowiązany do utrzymania i rozwijania zdolności

indywidualnej oraz zbiorowej odporności na atak⁴²⁶. Przez odporność rozumie się zdolność państwa i społeczeństwa do absorpcji i szybkiego odtworzenia kluczowych funkcji w razie poważnych zakłóceń – od katastrof naturalnych, przez agresję hybrydową, po konflikt zbrojny. W czasach zimnej wojny kwestie te były oczywiste (istniały rozbudowane struktury Obrony Cywilnej na wypadek wojny), jednak po 1990 r. uległy zaniedbaniu. Dopiero pogorszenie środowiska bezpieczeństwa po 2014 r. (agresja Rosji na Ukrainę) sprawiło, że NATO ponownie położyło nacisk na gotowość cywilną. Na szczytach w Newport (2014 r.) i Warszawie (2016 r.) przywódcy państw sojuszniczych uznali potrzebę wzmocnienia odporności i uzgodnili zestaw konkretnych kryteriów. Ustalono tzw. siedem bazowych wymogów odporności (ang. Seven Baseline Resilience Requirements) – dotyczą one kluczowych sektorów i funkcji cywilnych, których sprawność należy zapewnić w każdym państwie NATO. Są to m.in.: ciągłość działania władz i podstawowych usług publicznych, bezpieczeństwo dostaw energii, wody i żywności, odporność systemów łączności i transportu, a także zdolność do radzenia sobie z masowym napływem ludności i dużą liczbą poszkodowanych. Realizacja tych wymogów ma gwarantować, że nawet w sytuacji kryzysowej państwo będzie w stanie utrzymać funkcjonowanie infrastruktury krytycznej, zaopatrzyć ludność w niezbędne dobra, a także wesprzeć siły zbrojne w ich działaniach (np. zapewniając im transport, paliwo, opiekę medyczną). Co ważne, odpowiedzialność za spełnienie tych standardów spoczywa na władzach krajowych – NATO pełni tu rolę doradczą i koordynującą, monitorując postępy i ułatwiając wymianę dobrych praktyk między sojusznikami. Od 2016 r. w NATO funkcjonuje mechanizm regularnej oceny odporności – co pewien czas przygotowywany jest raport zbiorczy o stanie gotowości cywilnej całego Sojuszu, a państwa członkowskie zobowiązane są raportować realizację siedmiu wymogów⁴²⁷. Uzupełnieniem tego procesu są dobrowolne przeglądy narodowe – kraje mogą zapraszać ekspertów NATO do oceny ich przygotowań i rekomendowania ulepszeń.

⁴²⁶ Traktat Północnoatlantycki, sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r. Nr 87, poz. 970, art. 3).

⁴²⁷ Ł. Maślanka, P. Szymański, Odporność Unii Europejskiej i NATO w dobie multikryzysu, Komentarze OSW, nr 646, Warszawa, Ośrodek Studiów Wschodnich im. Marka Karpia, 2025.

Polska aktywnie wspiera te wysiłki NATO na rzecz odporności. W strukturach Sojuszu za planowanie cywilne i gotowość odpowiada Komitet Planowania Cywilnego (ang. Civil Emergency Planning Committee, CEPC) – najwyższy organ doradczy NAC w tej dziedzinie. Polskę na corocznych sesjach plenarnych CEPC reprezentuje Dyrektor Rządowego Centrum Bezpieczeństwa lub upoważniony przez niego przedstawiciel. RCB jest główną instytucją koordynującą kwestie zarządzania kryzysowego i ochrony infrastruktury krytycznej w kraju, stąd jego rola w kontaktach z NATO. Polski przedstawiciel bierze udział w pracach CEPC, w tym w wymianie informacji o stanie realizacji wymogów odporności przez nasz kraj. Co więcej, eksperci RCB działają w jednej z sześciu grup planistycznych NATO – Grupie ds. Ochrony Ludności (ang. Civil Protection Group), która zajmuje się m.in. przygotowaniem planów reagowania na klęski żywiołowe, awarie techniczne czy ataki CBRN. Poprzez udział w tej grupie Polska współtworzy polityki i wytyczne dotyczące współpracy cywilno-wojskowej i wzmacniania odporności w obszarach takich jak ciągłość administracji i świadczenie usług publicznych. Wymiana doświadczeń na forum CEPC i jego grup roboczych jest dla Polski bardzo cenna – pozwala porównać nasze przygotowania z innymi i czerpać z najlepszych praktyk sojuszników. NATO poprzez EADRCC oraz program zwiększania odporności cywilnej wnosi istotny wkład w system zarządzania kryzysowego, z którego korzysta również Polska. EADRCC zapewnia mechanizm szybkiej pomocy międzynarodowej w razie katastrof, także w sytuacjach wykraczających poza możliwości UE (np. w scenariuszu konfliktu zbrojnego), zaś sojusznicze programy planowania cywilnego mobilizują państwa do podnoszenia wewnętrznej gotowości na różne zagrożenia. Polska, uczestnicząc w tych inicjatywach, wzmacnia swoją własną odporność oraz przyczynia się do kolektywnego bezpieczeństwa NATO.

Polski system zarządzania kryzysowego jest silnie powiązany ze strukturami międzynarodowymi – członkostwo w UE i NATO obliguje nas do stałej współpracy, wymiany informacji i wspólnych ćwiczeń w obszarze reagowania kryzysowego. W praktyce oznacza to, że odpowiednie instytucje krajowe (m.in. Rządowe Centrum Bezpieczeństwa, Komenda Główna PSP, resorty siłowe i infrastrukturalne) pozostają w bieżącym kontakcie z centrami koordynacyjnymi UE i NATO, jak również z analogicznymi instytucjami

innych państw. Szybki przepływ wiarygodnych informacji jest fundamentem skutecznego zarządzania kryzysowego. Polska korzysta z dedykowanych systemów wymiany informacji zarówno w ramach UE, jak i NATO. Na szczeblu unijnym odbywa się to poprzez ERCC i platformę CECIS, gdzie zgłaszane są zagrożenia i potrzeby oraz składane oferty pomocy. Każde zdarzenie (np. powódź, pożar, epidemia), które może wymagać wsparcia zewnętrznego, jest raportowane przez krajowe centrum (KG PSP/RCB) do ERCC, skąd przekazywane jest partnerom. Analogicznie, Polska otrzymuje ostrzeżenia i prośby o pomoc od innych – np. informacja o wspomnianych pożarach w Szwecji w 2018 r. dotarła do MSWiA właśnie tą drogą i pozwoliła na szybkie przygotowanie oferty pomocy. Również w ramach NATO istnieją proceduralne kanały wymiany informacji o zagrożeniach. RCB regularnie informuje sojuszników (poprzez EADRCC i CEPCC) o poważnych zdarzeniach na terytorium Polski oraz o naszych zdolnościach wsparcia, jeśli gdzieś indziej wydarzy się katastrofa. Taka regularna wymiana danych, raportów i analiz między państwami sprzyja lepszemu zrozumieniu ryzyka i zwiększa gotowość. Jak podkreśla Rządowe Centrum Bezpieczeństwa, stała komunikacja i dzielenie się doświadczeniami na forum międzynarodowym owocuje ujednoliceniem standardów i procedur działania, co w efekcie ułatwia współdziałanie służb różnych państw podczas realnych kryzysów. Przykładem może być polsko-niemiecki projekt „Scenariusz Powódź” z 2013 r., gdzie wspólnie opracowano transgraniczną analizę ryzyka powodziowego dla Odry. W ramach tego przedsięwzięcia eksperci RCB i niemieckiego BBK wypracowali mechanizmy bieżącej wymiany informacji między centrami kryzysowymi obu krajów, co okazało się niezwykle ważne podczas realnych powodzi dotyczących region przygranicznego. Takie inicjatywy pokazują, że informacja jest najcenniejszym zasobem – jej sprawny przepływ może zapobiec eskalacji kryzysu lub przynajmniej ograniczyć jego skutki.

Kolejnym filarem współdziałania są międzynarodowe ćwiczenia kryzysowe, w których Polska aktywnie uczestniczy. Nasze służby ratunkowe, wojsko i administracja regularnie biorą udział w ćwiczeniach organizowanych pod egidą UE (np. ćwiczenia modułów rescEU, manewry w ramach programu MODEX) oraz NATO (ćwiczenia EADRCC, ćwiczenia z zakresu planowania cywilnego). Ćwiczenia te często symulują duże katastrofy, wymagające zaangażowania zasobów z wielu państw. Dla przykładu, Polska

gościła w 2019 r. unijne ćwiczenia modułów ratownictwa chemicznego, w których uczestniczyły ekipy z kilku krajów. Z kolei w ćwiczeniu NATO “Northern Macedonia 2021” polscy obserwatorzy uczyli się współdziałania przy akcjach poszukiwawczo-ratowniczych po trzęsieniu ziemi. Dzięki takim przedsięwzięciom polskie struktury kryzysowe zyskują bezcenne doświadczenie w międzynarodowym środowisku, poznają procedury partnerów i doskonalą własne plany. Równie ważne są ćwiczenia sztabowe i symulacje strategiczne – np. Polacy uczestniczą w cyklicznych ćwiczeniach zarządzania kryzysowego NATO (CMX), gdzie trenuje się reagowanie administracji rządowej na wielowymiarowe kryzysy polityczno-wojskowe. Podobnie na forum UE odbywają się gry decyzyjne dotyczące np. zamachów terrorystycznych czy pandemii, z udziałem przedstawicieli państw członkowskich. Wszystko to sprawia, że w momencie prawdziwego zagrożenia ludzie znają się i wiedzą, jak współpracować. Według RCB regularne ćwiczenia międzynarodowe przekładają się na wymierne korzyści – budują zaufanie i interoperacyjność instytucji odpowiedzialnych za bezpieczeństwo, co zwiększa skuteczność wspólnych operacji.

Najważniejszym testem współdziałania są oczywiście realne wydarzenia – duże katastrofy, w obliczu których aktywowane są mechanizmy pomocy międzynarodowej. Doświadczenia ostatnich lat (powódź w 2010 r., pandemia w 2020 r., kryzys uchodźczy w 2022 r., katastrofy za granicą) pokazały, że Polska może liczyć na wsparcie partnerów i sama potrafi nieść pomoc, gdy zajdzie taka potrzeba. Procedury wypracowane w ramach UE i NATO zadziałały sprawnie np. podczas wspomnianej powodzi 2010 r., kiedy to oferty pomocy dla Polski spłynęły w ciągu godzin z kilku krajów. Również w trakcie pandemii COVID-19 Polska korzystała ze współpracy europejskiej – mechanizmy unijne pomogły w dystrybucji sprzętu medycznego i szczepionek, a system NATO EADRCC ułatwiał wymianę informacji o potrzebach i nadwyżkach zaopatrzenia medycznego między sojusznikami. Gdy z kolei w lutym 2023 r. doszło do katastrofalnego trzęsienia ziemi w Turcji, polscy ratownicy ruszyli na pomoc w ramach misji zarówno unijnej, jak i natowskiej – nasza ciężka grupa poszukiwawczo-ratownicza (HUSAR Poland) działała na gruzowiskach w Adiyaman jako część unijnej operacji UCPM, a jednocześnie Wojsko Polskie wysłało samolot z pomocą

humanitarną koordynowany przez NATO. Te przykłady dowodzą, że synergia krajowych i międzynarodowych struktur kryzysowych przynosi realne efekty.

Należy też wspomnieć o formalnych porozumieniach i procedurach regulujących współdziałanie. Polska ratyfikowała szereg umów dwustronnych i wielostronnych o współpracy w zakresie ochrony ludności (m.in. z sąsiadami – Niemcami, Czechami, Ukrainą, Litwą), które uzupełniają mechanizmy UE/NATO. Istnieją również koordynatorzy ds. zarządzania kryzysowego akredytowani przy instytucjach międzynarodowych – np. oficer łącznikowy PSP przy ERCC w Brukseli – ułatwiający kontakt na poziomie operacyjnym. Na poziomie krajowym Rządowe Centrum Bezpieczeństwa pełni funkcję węzła łącznikowego, zapewniając przepływ informacji między polskim rządem a odpowiednimi strukturami unijnymi i sojuszniczymi. W razie potrzeby, do Centrum Zarządzania Kryzysowego Rządu mogą zostać oddelegowani przedstawiciele UE lub NATO jako obserwatorzy i doradcy (np. w czasie dużych ćwiczeń lub podczas zabezpieczania szczytów międzynarodowych w Polsce). Współdziałanie polskich struktur z organizacjami międzynarodowymi w obszarze bezpieczeństwa cywilnego stało się obecnie codzienną praktyką i koniecznością. Żaden kraj samodzielnie nie poradzi sobie z konsekwencjami największych katastrof czy złożonych kryzysów, dlatego tak istotne jest funkcjonowanie mechanizmów solidarnościowych UE i NATO. Polska – korzystając z tych mechanizmów – wzmacnia bezpieczeństwo swoich obywateli, a równocześnie przyczynia się do zwiększenia odporności całego regionu. Wymiana informacji, wspólne ćwiczenia i wzajemne wsparcie w potrzebie tworzą swoisty system naczyń połączonych, dzięki któremu zarządzanie kryzysowe przekracza granice państw i staje się wspólną odpowiedzialnością. Jest to szczególnie ważne w dobie tzw. multikryzysu (nakładania się wielu zagrożeń jednocześnie), z którym mierzy się współczesny świat⁴²⁸. Integracja wysiłków na forum UE i NATO daje szansę, by skuteczniej zapobiegać kryzysom i reagować na nie, co bezpośrednio przekłada się na poziom bezpieczeństwa Polski.

⁴²⁸ Ł. Maślanka, P. Szymański, Odporność Unii Europejskiej i NATO w dobie multikryzysu, Komentarze OSW, nr 646, Warszawa, Ośrodek Studiów Wschodnich im. Marka Karpią, 2025.

5.4. Współpraca transgraniczna i regionalna w reagowaniu kryzysowym

W obliczu katastrof naturalnych, awarii technicznych czy innych sytuacji kryzysowych, skuteczne reagowanie często wymaga współpracy transgranicznej – przekraczającej granice państw – oraz regionalnej, angażującej sąsiadujące kraje czy regiony. Żywieoty i zagrożenia nie respektują granic administracyjnych, dlatego państwa rozwijają mechanizmy umożliwiające wzajemną pomoc i koordynację działań ratunkowych ponad granicami⁴²⁹. Dotyczy to szczególnie krajów takich jak Polska, które graniczą z wieloma państwami i są członkiem szerszych struktur bezpieczeństwa europejskiego. Współpraca ta obejmuje umowy bilateralne, wspólne planowanie na wypadek ewakuacji czy katastrof, tworzenie euroregionów usprawniających lokalną kooperację, a także udział w makroregionalnych inicjatywach (np. region Morza Bałtyckiego, region karpacki). Podstawą transgranicznej kooperacji kryzysowej są porozumienia dwustronne między rządami sąsiadujących państw. Polska zawarła szereg umów międzyrządowych o współpracy i wzajemnej pomocy w przypadku katastrof, klęsk żywiołowych i innych poważnych wypadków praktycznie ze wszystkimi swoimi sąsiadami już na przełomie lat 90. i 2000. Były to m.in. umowy z Czechami, Słowacją, Litwą, Ukrainą, Białorusią, a także wcześniej z Rosją (dot. obwodu kaliningradzkiego). Na ich mocy strony uzgodniły zasady dobrowolnego udzielania pomocy na wniosek drugiej strony, ułatwienia w przekraczaniu granicy przez służby ratownicze, wzajemne uznawanie pewnych kwalifikacji ratowników, a nierzadko także zwolnienie z opłat – państwo udzielające pomocy nie domaga się zwrotu kosztów akcji. Takie porozumienia stanowią prawny fundament szybkiego reagowania, gdy własne zasoby kraju dotkniętego kryzysem są niewystarczające i potrzebne jest wsparcie z zagranicy.

Na mocy polsko-czeskiej umowy z 2000 r. oraz analogicznych umów z Litwą czy Słowacją, możliwe jest np. skierowanie zastępów straży pożarnej lub ekip ratownictwa technicznego z sąsiedniego kraju do pomocy przy dużym pożarze lub katastrofie na terenach przygranicznych. W 2011 r.

⁴²⁹ K. Świderski, *Współpraca formacji mundurowych w utrzymaniu bezpieczeństwa transgranicznego Polski*, *Wschodnioznawstwo*, 12, 2018, s. 127-142.

Polska i Niemcy podpisały odrębną umowę ramową o współpracy transgranicznej w ratownictwie medycznym. Dotyczy ona pasa przygranicznego (30-50 km od granicy) i zakłada, że w nagłych wypadkach medycznych karetka pogotowia z drugiej strony granicy może szybciej dotrzeć na miejsce – wtedy to ona udziela pomocy niezależnie od państwowej przynależności, byle jak najszybciej ratować życie. Umowa ta określa m.in. zasady wzajemnego uznawania uprawnień ratowników, priorytetowego przekraczania granicy przez ambulans, przewozu pacjentów, a także ochrony danych medycznych. Co ważne, koszty takich akcji w strefie przygranicznej nie są wzajemnie rozliczane – pomoc jest udzielana solidarnie bez obciążania strony proszącej. W praktyce umowy bilateralne usprawniły transgraniczne reagowanie już w wielu sytuacjach. Historycznym przykładem była powódź tysiąclecia w lipcu 1997 r., która dotknęła Polskę oraz Czechy i Niemcy jednocześnie. Już pierwszego dnia kryzysu strona polska zwróciła się o pomoc międzynarodową – pierwszym krajem, który odpowiedział, były Niemcy, wysyłając sprzęt i ratowników. Łącznie Polsce pomogły wtedy ekipy z dwunastu państw, w tym z krajów sąsiednich: Czech, Słowacji, Ukrainy, Litwy, a także m.in. z Węgier, Austrii czy Szwecji. Przybyło prawie 500 zagranicznych ratowników z pompami wysokiej wydajności, agregatami i amfibiami, którzy wspólnie z polskimi służbami walczyli z żywiołem. To wydarzenie uwidocznilo znaczenie uprzednio zawartych porozumień – dzięki nim możliwe było szybkie przyjęcie pomocy (np. uproszczenie procedur granicznych dla konwojów ratunkowych). Doświadczenia z 1997 r. i kolejnych powodzi (m.in. 2010 r.) przyczyniły się do udoskonalenia współpracy: m.in. poprawiono łączność między służbami różnych krajów i ustalono wspólne kanały alarmowe, gdyż początkowo brak takiej łączności utrudniał koordynację.

Rządowe Centrum Bezpieczeństwa podkreśla, że zgranie procedur i ludzi po obu stronach granicy jest kluczowe dla skutecznego reagowania⁴³⁰. W 2012 r. ustalono np., że Polska i Niemcy opracują wspólną analizę ryzyka dla wybranych zagrożeń transgranicznych (takich jak powódzie), aby lepiej przygotować plany reagowania. Uzgodniono również regularną wymianę informacji i doświadczeń – np. organizację wspólnych sztabowych ćwiczeń

⁴³⁰ Rządowe Centrum Bezpieczeństwa, Wymiana polskich i niemieckich doświadczeń w zakresie zarządzania kryzysowego, RCB – Archiwum, 2012.

kryzysowych czy dzielenie się wiedzą o systemach wczesnego ostrzegania. Podobnie Polska i Czechy zadeklarowały w ostatnich latach zacieśnienie współdziałania w reagowaniu na zagrożenia na pograniczu sudeckim, czego wyrazem są nowe porozumienia między województwami a czeskimi krajami⁴³¹.

Zawarcie porozumień instytucjonalnych nie jest wystarczające. Niezbędne pozostaje równoległe prowadzenie praktycznego planowania operacyjnego z partnerami po stronie sąsiedniej. Na obszarach przygranicznych opracowuje się wspólne plany działań na wypadek zidentyfikowanych zagrożeń, w szczególności powodzi, pożarów lasów oraz awarii przemysłowych, których skutki mogą oddziaływać po obu stronach granicy. W rejonie Sudetów (pogranicze polsko-czeskie) jednostki samorządu terytorialnego oraz służby ratownicze przygotowały transgraniczne plany ewakuacji ludności z dolin górskich na wypadek powodzi błyskawicznych, uwzględniając charakterystykę rzek górskich (m.in. Nysy Kłodzkiej i Kamiennej) oraz możliwość gwałtownych wezbrań na terytorium jednego państwa skutkujących zagrożeniem po stronie drugiego⁴³². W ramach projektu realizowanego przez gminy Szklarska Poręba (PL) i Harrachov (CZ) utworzono Transgraniczne Centrum Ewakuacji i Pomocy Ludności w Piechowicach (Dolny Śląsk), pełniące funkcję punktu koordynacji działań ratowniczych oraz miejsca czasowego schronienia dla osób ewakuowanych w razie zdarzeń o charakterze klęsk żywiołowych. Przedsięwzięcie obejmowało również doposażenie partnerów w specjalistyczny sprzęt ratowniczy przeznaczony do wykorzystania w działaniach wspólnych i szkoleniach⁴³³. Kluczowym rezultatem było opracowanie uzgodnionych procedur postępowania i scenariuszy działania oraz włączenie do współpracy lokalnych jednostek straży pożarnej, Państwowego Ratownictwa Medycznego, Policji i Straży Granicznej, co sprzyja

⁴³¹ J. Ziobro, Ratownictwo transgraniczne jako forma współpracy i integracji międzynarodowej oraz środek w procesie zapewniania bezpieczeństwa powszechnego – wybrane aspekty organizacji transgranicznych działań ratowniczych, *Scientific Reports of Fire University (ZN SGSP)*, 73(1), 2020, s. 165-191. <https://doi.org/10.5604/01.3001.0014.0781>

⁴³² Ł. Skoczylas, Aktualna współpraca transgraniczna Polski z wybranymi sąsiadami, *Białostockie Studia Prawnicze*, 12, 2012, s. 123-136. <https://doi.org/10.15290/bsp.2012.12.06>

⁴³³ K. Świderski, Współpraca formacji mundurowych w utrzymaniu bezpieczeństwa transgranicznego Polski, *Wschodnioznawstwo, Zakład Badań Wschodnich, Instytut Studiów Międzynarodowych, Uniwersytet Wrocławski*, 12, 2018, s. 133-134.

jednoznacznemu podziałowi kompetencji oraz ujednoliceniu standardów operacyjnych.

Istotnym obszarem współdziałania pozostaje ochrona środowiska oraz reagowanie na zagrożenia ekologiczne. Dla transgranicznych obszarów chronionych (np. Puszczy Białowieskiej oraz Karpat Wschodnich) uzgadnia się zasady koordynacji na wypadek pożarów lasów, wystąpienia chorób zwierząt oraz innych zdarzeń mogących oddziaływać na ekosystemy po obu stronach granicy. W praktyce obejmuje to wymianę informacji o zagrożeniach, uzgodnione mechanizmy wzajemnego alarmowania oraz rozwiązania umożliwiające podjęcie działań gaśniczych lub interwencyjnych w rejonie przygranicznym z zapewnieniem sprawności formalno-organizacyjnej. Na rzekach granicznych wdraża się ponadto wspólne plany reagowania na zanieczyszczenia, obejmujące monitoring stanu wód oraz procedury postępowania w przypadku wykrycia skażenia, w tym pochodzenia przemysłowego. Przykładem jest współpraca na Odrze, wzmacniana porozumieniami dotyczącymi utrzymania rzeki i współdziałania w sytuacjach zagrożeń powodziowych oraz ekologicznych.

Stałym elementem planowania operacyjnego są regularne ćwiczenia transgraniczne, które umożliwiają weryfikację procedur, kanałów łączności oraz mechanizmów podejmowania decyzji w warunkach zbliżonych do realnych zdarzeń. Przykładowo, w czerwcu 2008 r. przeprowadzono międzynarodowe ćwiczenie „Terryści na tamie” z udziałem służb Polski, Czech i Słowacji, ukierunkowane na sprawdzenie współdziałania przy ochronie infrastruktury krytycznej, prowadzeniu pościgu transgranicznego oraz organizacji ewakuacji ludności⁴³⁴. Równolegle realizowane są manewry ratownicze w formule projektów euroregionalnych, w tym warsztaty i ćwiczenia ukierunkowane na reagowanie na powodzie lub skażenia wód, które sprzyjają porównaniu stosowanych rozwiązań, ujednoliceniu praktyk i wypracowaniu rekomendacji usprawniających współpracę. Podobne cele realizują projekty szkoleniowe służb ratownictwa górskiego, prowadzące do wypracowania wspólnych standardów działań w terenie przygranicznym. Uzupełnieniem powyższych instrumentów są wspólne centra współpracy oraz zintegrowane

⁴³⁴ J. Maciejewski, A. Sokołowska, M. Stochmal (red.), Grupy dyspozycyjne w systemie współpracy transgranicznej na rzecz bezpieczeństwa, Wrocław, Wydawnictwo Uniwersytetu Wrocławskiego, 2015.

systemy monitorowania i wczesnego ostrzegania. W wybranych regionach funkcjonują centra, w których współpracują oficerowie łącznikowi różnych formacji, co usprawnia wymianę informacji i koordynację działań w strefie przygranicznej. Równocześnie, przy wsparciu środków unijnych, rozwijane są transgraniczne systemy wczesnego ostrzegania, w tym rozwiązania oparte na zintegrowanych danych hydrologicznych i meteorologicznych (np. w obszarze Euroregionu Nysa), umożliwiające generowanie ostrzeżeń dla społeczności po obu stronach granicy z odpowiednim wyprzedzeniem.

Euroregiony to struktury współpracy zrzeszające przygraniczne samorządy z dwóch lub więcej państw, mające ułatwiać rozwój lokalny i rozwiązywanie wspólnych problemów. W Polsce od lat 90. powstało kilkanaście euroregionów na granicach – m.in. Euroregion Nysa (PL-CZ-DE), Pomerania (PL-DE), Pro Europa Viadrina (PL-DE), Bug (PL-UA-BY), Karpacki (PL-SK-UA-HU-RO) i inne. Choć zajmują się one głównie sprawami społeczno-gospodarczymi, odgrywają też ważną rolę we współpracy w zakresie bezpieczeństwa. Euroregiony dysponują Funduszami Małych Projektów z UE, z których finansowane są np. szkolenia służb, zakup wyposażenia ratunkowego czy kampanie edukacyjne dla mieszkańców pogranicza. Samorządy lokalne w ramach euroregionów inicjują projekty zwiększające bezpieczeństwo – np. doposażenie straży pożarnych po obu stronach granicy, wspólne mapy ryzyka czy transgraniczne systemy łączności radiowej⁴³⁵.

Euroregion Karpacki zrealizował w latach 2014-2020 blisko 100 mikroprojektów, z których wiele dotyczyło bezpieczeństwa – np. wspólne szkolenia GOPR i HZS w Beskidach (jak wspomniano powyżej) czy poprawa wyposażenia jednostek OSP na pograniczu podkarpackim i obwodu lwowskiego. W Euroregionie Pomerania (pogranicze zachodniopomorskie – Meklemburgia) funkcjonują polsko-niemieckie posterunki straży pożarnej i pogotowia, które obsługują wezwania po obu stronach granicy tam, gdzie odległości do najbliższej jednostki w drugim kraju są mniejsze. Przykładem jest niemiecko-polska jednostka strażacka w Garz na Uznamie, wspólnie chroniąca kurorty po stronie polskiej (Świnoujście-Przytór) i niemieckiej

⁴³⁵ Ł. Skoczylas, Aktualna współpraca transgraniczna Polski z wybranymi sąsiadami, Białostockie Studia Prawnicze, 12, 2012, s. 123-136. <https://doi.org/10.15290/bsp.2012.12.06>

(Garz i okolice). Takie rozwiązania są możliwe dzięki porozumieniom komunalnym zawieranim pod auspicjami euroregionu.

Euroregiony organizują też transgraniczne ćwiczenia dla społeczności lokalnych, np. symulacje ewakuacji w razie wycieku chemicznego w strefie przygranicznej czy pokazy ratownictwa podczas powodzi. Działania te zwiększają świadomość mieszkańców i poziom zaufania między służbami sąsiednich krajów⁴³⁶. Jak wskazują analizy, właśnie na poziomie lokalnym współpraca bywa najściślejsza – wspólne codzienne patrole służb, kontakty strażaków ochotników, czy choćby bliźniacze miasta (np. Cieszyn-Český Těšín, Zgorzelec-Görlitz) mające wspólne plany reagowania kryzysowego dla swoich aglomeracji⁴³⁷. To wszystko sprawia, że granica państwa przestaje być barierą w sytuacji zagrożenia – liczy się sprawne dotarcie pomocy do poszkodowanych, niezależnie od jurysdykcji. Na rysunku 16 przedstawiono mapę Polski z naniesionymi długościami granic z państwami sąsiednimi (w kilometrach) oraz z wyróżnieniem odcinka granicy morskiej na Morzu Bałtyckim.

⁴³⁶ Ł. Skoczylas, Aktualna współpraca transgraniczna Polski z wybranymi sąsiadami, *Białostockie Studia Prawnicze*, 12, 2012, s. 123-136. <https://doi.org/10.15290/bsp.2012.12.06>

⁴³⁷ J. Maciejewski, A. Sokołowska, M. Stochmal (red.), *Grupy dyspozycyjne w systemie współpracy transgranicznej na rzecz bezpieczeństwa*, Wrocław, Wydawnictwo Uniwersytetu Wrocławskiego, 2015.



Rysunek 16. Długości granic Polski z państwami sąsiednimi oraz granica morska (km)

Źródło: AnonMoos, Poland borders, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Poland_borders.svg, [dostęp: 10.10.2025].

Zestawienie wskazuje, że najdłuższy odcinek granicy lądowej Polska utrzymuje z Republiką Czeską (ok. 790-796 km), natomiast najkrótszy – z Republiką Litewską (ok. 103-104 km). Granica morska (Bałtyk) została wskazana na poziomie ok. 440 km, przy jednoczesnym rozróżnieniu długości linii brzegowej Polski (ok. 770 km) od długości granic na morzu. W tym ujęciu (geograficznym i operacyjnym) działania euroregionów stanowią istotne uzupełnienie współpracy transgranicznej w zakresie zarządzania kryzysowego. Euroregiony organizują ćwiczenia dla społeczności lokalnych, w tym symulacje ewakuacji w przypadku awarii chemicznej w strefie przygranicznej oraz pokazy działań ratowniczych podczas epizodów powodziowych. Aktywności te wzmacniają świadomość ryzyk, poprawiają przygotowanie mieszkańców oraz budują zaufanie i kompatybilność współdziałania pomiędzy służbami sąsiadujących państw. Analizy praktyki współpracy wskazują, że to właśnie na poziomie lokalnym kooperacja bywa najbardziej

intensywna, m.in. poprzez wspólne patrole, stałe kontakty jednostek ochotniczych straży pożarnych oraz funkcjonowanie miast partnerskich po obu stronach granicy, które rozwijają uzgodnione rozwiązania reagowania kryzysowego dla obszarów funkcjonalnie powiązanych. W konsekwencji granica państwowa w sytuacji zagrożenia traci charakter bariery operacyjnej, a priorytetem staje się sprawne udzielenie pomocy poszkodowanym, niezależnie od właściwości jurysdykcyjnej.

Na poziomie makroregionalnym w Europie rozwinięto wielostronne platformy współpracy w zakresie przygotowania i reagowania kryzysowego. Polska uczestniczy w inicjatywach związanych z regionem Morza Bałtyckiego oraz w mechanizmach współpracy karpackiej, które wzmacniają zdolność koordynacji działań w sytuacjach zagrożeń o charakterze ponadgranicznym, wykraczających skalą poza możliwości pojedynczego państwa.

W regionie Morza Bałtyckiego kluczową rolę odgrywa Komisja Helsińska (HELCOM), działająca od lat 70. XX w. jako organizacja koordynująca ochronę środowiska morskiego. Do jej zadań należy również rozwijanie gotowości państw nadbałtyckich na wypadek awarii ekologicznych, w szczególności rozlewów substancji ropopochodnych w wyniku incydentów z udziałem jednostek pływających. Elementem praktycznego przygotowania pozostają cykliczne międzynarodowe ćwiczenia BALEX DELTA, traktowane jako największe manewry ratownicze w basenie Morza Bałtyckiego. W sierpniu 2025 r. gospodarzem ćwiczeń była Polska; działania szkoleniowe zrealizowano w rejonie Świnoujścia, z udziałem personelu i zasobów z siedmiu państw nadbałtyckich. Scenariusz obejmował symulację rozległego rozlewu olejowego oraz zintegrowane działania na morzu, w strefie brzegowej i w porcie, z udziałem wyspecjalizowanych jednostek ratownictwa morskiego. Część lądowa angażowała również podmioty krajowego systemu bezpieczeństwa, w tym służby ratownicze, formacje odpowiedzialne za ochronę granicy, komponenty wojskowe oraz instytucje właściwe w zakresie ochrony środowiska i nadzoru weterynaryjnego, a także wybrane organizacje pozarządowe. Zakres ćwiczeń obejmował nie tylko techniki zbierania substancji z powierzchni wody, lecz także procedury ochrony fauny (w tym ratowania ptaków) oraz koordynację logistyczną wielopunktowej operacji realizowanej równolegle w kilku lokalizacjach. Doświadczenia BALEX DELTA potwierdzają, że w przypadku katastrof ekologicznych o dużej

skali efektywna ochrona środowiska morskiego wymaga spójnego, międzynarodowego systemu współdziałania, obejmującego interoperacyjność zasobów, jednolite procedury oraz sprawną wymianę informacji. Uzupełnieniem ćwiczeń pozostaje stały mechanizm zgłaszania incydentów morskich i dystrybucji informacji o zagrożeniach, a także utrzymywanie zapasów i zdolności sprzętowych w różnych państwach regionu, umożliwiających szybkie wsparcie w miejscu zdarzenia.

Równolegle istotnym obszarem współpracy ponadnarodowej jest region karpacki, obejmujący terytoria kilku państw (m.in. Polski, Słowacji, Ukrainy, Rumunii i Węgier). W tym układzie geograficznym szczególnego znaczenia nabiera spójne podejście do zagrożeń naturalnych charakterystycznych dla obszarów górskich, w tym lawin, osuwisk oraz powodzi górskich. Ramy współpracy wyznacza Konwencja Karpacka (2003) dotycząca ochrony i zrównoważonego rozwoju Karpat, w ramach której rozwijane są także działania odnoszące się do zarządzania ryzykiem i odporności. Choć region karpacki nie dysponuje jeszcze formalnie ustanowioną strategią makroregionalną Unii Europejskiej, prowadzone są prace koncepcyjne nad Strategią Karpacką, w której uwzględniane mają być również komponenty bezpieczeństwa. W praktyce współdziałanie jest rozwijane m.in. poprzez wymianę dobrych praktyk pomiędzy służbami ratownictwa górskiego oraz inicjatywy sieciowe, ukierunkowane na usprawnienie działań poszukiwawczych i ratowniczych w rejonach przygranicznych. Doświadczenia regionu zostały dodatkowo wzmocnione w następstwie kryzysów o charakterze społecznym i geopolitycznym, w tym masowego napływu uchodźców z Ukrainy w 2022 r., kiedy podmioty samorządowe oraz służby w państwach sąsiadujących koordynowały działania humanitarne, organizując punkty recepcyjne, wsparcie logistyczne i korytarze transportowe. Praktyka ta może stanowić podstawę do dalszej instytucjonalizacji rozwiązań reagowania kryzysowego w układzie makroregionalnym.

Na tym tle szczególne znaczenie mają instrumenty Unii Europejskiej, w tym Unijny Mechanizm Ochrony Ludności, który stanowi paneuropejski system koordynacji pomocy w sytuacjach klęsk żywiołowych i katastrof. Mechanizm ten nie zastępuje współpracy bilateralnej z państwami sąsiednimi, lecz ją uzupełnia, umożliwiając uruchomienie wsparcia z całej UE w przypadku zdarzeń przekraczających potencjał reagowania państwa

dotkniętego kryzysem. W praktyce mechanizm był wykorzystywany zarówno w kontekście udzielania Polsce wsparcia w sytuacjach nadzwyczajnych, jak i w ramach udziału polskich zasobów w działaniach ratowniczych na terytorium innych państw, w tym w operacjach związanych z pożarami lasów. Dodatkowym obszarem weryfikacji zdolności współpracy była pandemia COVID-19, która unaoczniała wrażliwość na ograniczenia transgranicznej mobilności oraz na zakłócenia łańcuchów dostaw. Jednocześnie kryzys potwierdził rolę rozwiązań koordynacyjnych i solidarnościowych, w tym współdziałania w zakresie transportu, dystrybucji środków medycznych oraz wzajemnego wsparcia systemów ochrony zdrowia w regionach najbardziej obciążonych. W konsekwencji współpraca transgraniczna i regionalna stanowi obecnie integralny komponent systemu zarządzania kryzysowego. Umowy bilateralne i uzgodnione plany operacyjne z państwami sąsiednimi tworzą podstawy prawno-organizacyjne umożliwiające uruchomienie działań bez zbędnej zwłoki proceduralnej. Inicjatywy euroregionalne i lokalne wzmacniają zaufanie oraz sprawność współdziałania poprzez stałe relacje robocze, wspólne szkolenia i praktyczne ćwiczenia. Struktury makroregionalne, w szczególności w regionie Morza Bałtyckiego, zwiększają zdolność reagowania na zdarzenia o skali przekraczającej potencjał jednego państwa, zwłaszcza w obszarze bezpieczeństwa ekologicznego. Całość tych rozwiązań tworzy wielopoziomowy układ bezpieczeństwa – od poziomu lokalnego po mechanizmy UE – który zwiększa odporność oraz skuteczność reagowania na kryzysy. W warunkach narastania zagrożeń klimatycznych, technologicznych i geopolitycznych współpraca ponad granicami pozostaje warunkiem koniecznym zapewnienia bezpieczeństwa ludności oraz ochrony zasobów krytycznych.

5.5. Przykłady dobrych praktyk i doświadczenia z wybranych państw

W praktyce ochrony ludności i zarządzania kryzysowego obserwuje się znaczące zróżnicowanie modeli instytucjonalnych, sposobów finansowania, a także doboru narzędzi operacyjnych i technologicznych. Różnice te wynikają zarówno z uwarunkowań prawnych i ustrojowych, jak i z doświadczeń

historycznych oraz dominujących typów zagrożeń. Z tego względu analiza rozwiązań stosowanych w innych państwach stanowi istotne źródło wiedzy o mechanizmach podnoszenia odporności, organizacji reagowania oraz zapewniania ciągłości działania instytucji publicznych.

Pierwszym analizowanym przykładem jest system ochrony ludności i zarządzania kryzysowego funkcjonujący w Stanach Zjednoczonych, uznawany za jeden z najbardziej rozwiniętych modeli koordynacji działań w warunkach zdarzeń nadzwyczajnych. System ten ma charakter wyraźnie zdecentralizowany, przy jednoczesnym zapewnieniu spójnej koordynacji na poziomie federalnym. Kluczową rolę w tym układzie pełni Federalna Agencja Zarządzania Kryzysowego (Federal Emergency Management Agency – FEMA), powołana w 1979 r., a od 2003 r. działająca w strukturze Departamentu Bezpieczeństwa Krajowego. Jej utworzenie pozwoliło na uporządkowanie i scalenie kompetencji, które wcześniej były rozproszone pomiędzy liczne instytucje federalne odpowiedzialne za reagowanie na katastrofy. FEMA realizuje zadania w pełnym cyklu zarządzania kryzysowego, obejmującym identyfikację i ocenę ryzyk, planowanie, działania prewencyjne i edukacyjne, reagowanie oraz odbudowę i usuwanie skutków zdarzeń. W praktyce operacyjnej podstawowa odpowiedzialność za prowadzenie działań spoczywa na władzach stanowych i lokalnych (w tym na agencjach zarządzania kryzysowego stanów, hrabstw i miast), natomiast wsparcie federalne uruchamiane jest w sytuacjach przekraczających możliwości poziomu lokalnego, zgodnie z przyjętymi procedurami i mechanizmami finansowania. Istotnym wyróżnikiem amerykańskiego podejścia pozostaje standaryzacja zarządzania działaniami w terenie poprzez jednolity model dowodzenia incydem. W latach 70. XX w. opracowano Incident Command System (ICS), początkowo na potrzeby koordynacji działań podczas wielkoobszarowych pożarów lasów, a następnie sukcesywnie rozszerzany na inne typy zdarzeń i podmioty. Skuteczność ICS doprowadziła do jego upowszechnienia w skali kraju oraz do przyjęcia jako punktu odniesienia dla rozwiązań wdrażanych także w innych państwach. Po zamachach z 11 września 2001 r. wprowadzono Narodowy System Zarządzania Incydentami (National Incident Management System – NIMS), który zobowiązał organy administracji publicznej i służby do stosowania wspólnej struktury dowodzenia zgodnej z ICS. Rozwiązanie to zwiększyło interoperacyjność pomiędzy podmiotami

o różnych kompetencjach i podporządkowaniach, umożliwiając sprawniejsze współdziałanie straży pożarnej, policji, ratownictwa medycznego, Gwardii Narodowej oraz innych instytucji w ramach jednolitego schematu organizacyjnego. Na uwagę zasługuje również przyjęcie koncepcji all-hazards, zakładającej spójne przygotowanie instytucji do reagowania na pełne spektrum zagrożeń – od katastrof naturalnych, przez awarie technologiczne, po zagrożenia terrorystyczne – w oparciu o te same podstawowe zasady organizacji działań. Standardyzacja obejmuje wspólną terminologię, role dowódcze i planistyczne, jednolite narzędzia dokumentowania oraz procedury koordynacji międzyagencyjnej. Równolegle system akcentuje rozwijanie odporności społecznej poprzez edukację i przygotowanie obywateli, w tym programy informacyjne adresowane do gospodarstw domowych, szkół i instytucji publicznych, a także wzmacnianie gotowości poprzez działania o charakterze kampanii ogólnokrajowych. Charakterystyczne jest również szerokie włączanie potencjału organizacji pozarządowych i wolontariatu, w tym wyszkolonych zespołów wsparcia działań ratowniczych, co pozwala zwiększać zdolności reagowania przy zachowaniu klarownego podziału ról i odpowiedzialności. Wnioski dla praktyki polskiej odnoszą się przede wszystkim do potrzeby dalszej harmonizacji zasad dowodzenia, koordynacji oraz wymiany informacji pomiędzy służbami i instytucjami. Uporządkowanie i standaryzacja procedur na wzór ICS/NIMS mogłyby ograniczać ryzyko rozproszenia decyzyjnego w zdarzeniach złożonych oraz zwiększać interoperacyjność pomiędzy podmiotami systemu bezpieczeństwa. Istotne znaczenie mają także konsekwentnie rozwijane programy edukacji dla bezpieczeństwa oraz systemowe wykorzystanie zasobów społecznych, w tym organizacji ochotniczych i grup wsparcia, przy jednoczesnym zapewnieniu jednolitych standardów szkolenia, łączności i współdziałania.

Kolejnym przykładem jest niemiecki model ochrony ludności, ukształtowany w warunkach ustroju federalnego i oparty na wyraźnym podziale kompetencji pomiędzy poziom federacji a 16 krajów związkowych (Landów). W zakresie reagowania na klęski żywiołowe i katastrofy w czasie pokoju zasadnicza odpowiedzialność spoczywa na krajach związkowych, które posiadają własne regulacje prawne i struktury wykonawcze związane z ochroną przed katastrofami (Katastrophenschutz). Kompetencje federalne koncentrują się natomiast na obszarze ochrony cywilnej na wypadek

konfliktu zbrojnego (Zivilschutz) oraz na utrzymaniu instrumentów wsparcia i koordynacji, które mogą zostać uruchomione w sytuacjach zdarzeń o ponadregionalnym zasięgu. Centralną instytucją na szczeblu federalnym jest Federalny Urząd Ochrony Ludności i Pomocy w Przypadku Katastrof (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK), powołany w 2004 r., pełniący funkcje analityczne, planistyczne, szkoleniowe i koordynacyjne. BBK przygotowuje m.in. analizy ryzyka, opracowuje wytyczne i dokumenty planistyczne, prowadzi federalne centrum sytuacyjne monitorujące zdarzenia oraz rozwija systemy szkoleniowe i doskonalenia kadr. W przypadku zdarzeń przekraczających możliwości landu możliwe jest uruchomienie wsparcia federalnego, obejmującego zasoby BBK, Federalnej Agencji Pomocy Technicznej (Technisches Hilfswerk – THW), Policji Federalnej oraz – w określonych sytuacjach – Bundeswehry. Praktyka operacyjna ma zatem charakter wielopoziomowy: podstawowe działania realizowane są lokalnie przez służby ratownicze i administrację terenową, następnie eskalowane na poziom landu, a w razie potrzeby uzupełniane komponentem federalnym. Najbardziej charakterystyczną cechą systemu niemieckiego pozostaje bardzo szerokie wykorzystanie zasobów ochotniczych, ujętych w trwałe ramy organizacyjne państwa. Szczególną rolę odgrywa THW – formacja podległa federalnemu resortowi spraw wewnętrznych, wyspecjalizowana w technicznej pomocy ratowniczej (m.in. prace inżynierskie i logistyczne, usuwanie skutków katastrof budowlanych, zapewnianie awaryjnego zasilania, budowa przepraw tymczasowych, ratownictwo techniczne i wodne). Pomimo federalnego umocowania instytucjonalnego trzon THW stanowią wolontariusze, których liczebność w ostatnich latach sięgała około 88 tys., działających w rozbudowanej sieci jednostek lokalnych na terenie całych Niemiec. Zbliżoną funkcję w obszarze bezpieczeństwa lokalnego pełnią ochotnicze straże pożarne (Freiwillige Feuerwehr), które w wielu gminach stanowią podstawowy element systemu ratowniczego i zapewniają szybki czas reakcji, znajomość lokalnych uwarunkowań oraz trwałe powiązanie służb z mieszkańcami. Wysoki poziom uczestnictwa społeczeństwa w formacjach ochotniczych przekłada się na znaczącą rezerwę operacyjną państwa i wzmacnia odporność społeczności lokalnych na zdarzenia kryzysowe. Za szczególnie wartościowe w niemieckim modelu uznaje się konsekwentne powiązanie struktur publicznych z zasobami społecznymi w sposób

sformalizowany, oparty na jednolitych standardach szkolenia, wyposażenia i gotowości. THW stanowi przykład rozwiązania, które pozwala utrzymywać znaczący potencjał techniczny i logistyczny przy relatywnie korzystnej relacji koszt-efekt, a jednocześnie umożliwia uruchamianie zasobów zarówno w działaniach krajowych, jak i w misjach zagranicznych w ramach pomocy humanitarnej. Równolegle istotną zaletą jest przejrzysty podział zadań i odpowiedzialności pomiędzy szczeble administracji oraz rozwinięte planowanie, w którym każdy poziom – od gminy po federację – posiada określone narzędzia organizacyjne, procedury i organy decyzyjne. W praktyce dużych zdarzeń istotne znaczenie ma równoległe funkcjonowanie struktur dowodzenia operacyjnego w terenie oraz mechanizmów kierownictwa administracyjno-politycznego, odpowiadających za alokację zasobów, komunikację publiczną i decyzje o charakterze organizacyjnym. Rozdzielenie tych ról sprzyja sprawności działania i redukuje ryzyko przeciążenia dowodzenia operacyjnego zadaniami administracyjnymi. Niemcy rozwijają ponadto systemy ostrzegania i alarmowania ludności, łącząc tradycyjne narzędzia (syreny) z rozwiązaniami cyfrowymi, w tym aplikacjami powiadomień oraz technologią Cell Broadcast, a także prowadząc regularne testy systemu w ramach ogólnokrajowych ćwiczeń alarmowych (Warntag). Wymiar strategiczny wzmacnia fakt, że państwo prowadzi systematyczną aktualizację dokumentów planistycznych i koncepcyjnych, w tym podejmuje działania na rzecz podnoszenia odporności ludności poprzez rekomendacje dotyczące przygotowania gospodarstw domowych na okresowe zakłócenia dostaw podstawowych dóbr. W kontekście polskim szczególnie istotne są doświadczenia niemieckie dotyczące instytucjonalizacji wolontariatu oraz budowy rezerw zdolności ratowniczych w oparciu o standardy państwowe. Polska dysponuje rozbudowaną siecią Ochotniczych Straży Pożarnych, jednak skala systemowego włączania innych formacji i organizacji pozarządowych bywa nierównomierna, a mechanizmy koordynacji, szkolenia i wyposażenia wymagają dalszego wzmacniania. Wdrażane rozwiązania prawno-organizacyjne, w tym rozwój instrumentów ochrony ludności i struktur rezerw, powinny uwzględniać elementy modelu THW: przewidywalne finansowanie, jednolite standardy szkoleniowe, klarowną strukturę dowodzenia i sprawne mechanizmy mobilizacji. Równolegle zasadne jest dalsze doskonalenie krajowego systemu ostrzegania i alarmowania, w tym rozwijanie i regularne

testowanie kanałów masowych powiadomień oraz wzmacnianie zdolności komunikacji kryzysowej na poziomie centralnym i regionalnym. Wreszcie, niemiecki model wieloszczeblowej koordynacji wskazuje na wagę silnych, kompetentnych struktur analityczno-koordynacyjnych na poziomie krajowym, które mogłyby skuteczniej wspierać administrację terenową w zadaniach o charakterze ponadregionalnym poprzez standaryzację procedur, szkolenia i rozwój zdolności współdziałania międzysektorowego.

Kolejnym przykładem jest francuski model ochrony ludności, który wyróżnia się wysokim stopniem centralizacji oraz silną standaryzacją działań ratowniczych w skali całego państwa. Odpowiedzialność za organizację ochrony ludności i reagowanie kryzysowe została w dużej mierze skoncentrowana w strukturach administracji rządowej podporządkowanej Ministerstwu Spraw Wewnętrznych, w ramach rozbudowanego systemu *Sécurité Civile*. Kluczową rolę pełni Dyrekcja Generalna Bezpieczeństwa Cywilnego i Zarządzania Kryzysowego (*Direction générale de la sécurité civile et de la gestion des crises – DGSCGC*), która odpowiada za spójność rozwiązań planistycznych, nadzór nad gotowością operacyjną, utrzymywanie zasobów krajowych oraz koordynację działań w sytuacjach o charakterze ponadlokalnym. Istotnym filarem tego modelu jest terenowa administracja rządowa kierowana przez prefektów, którzy jako przedstawiciele rządu w terenie odpowiadają za koordynację działań służb podczas zdarzeń poważnych. Francja obejmuje łącznie 101 departamentów, a prefekci departamentalni dysponują kompetencjami umożliwiającymi kierowanie i synchronizowanie działań ratowniczych w granicach administracyjnych departamentu. Dodatkowo państwo zostało podzielone na większe strefy obrony i bezpieczeństwa, w ramach których prefekt strefy może przejąć koordynację, gdy zdarzenie przekracza możliwości jednego departamentu, korzystając z dedykowanych struktur sztabowych i centrów operacyjnych. W efekcie funkcjonuje model eskalacji oparty na zasadzie subsydiarności: zdarzenia o ograniczonym zasięgu obsługiwane są na poziomie lokalnym, natomiast w sytuacjach o większej skali uruchamiane są narzędzia koordynacyjne szczebla strefowego i centralnego. Struktura służb ratowniczych we Francji opiera się na współdziałaniu straży pożarnej, Policji i Żandarmerii oraz systemu ratownictwa medycznego (*SAMU*). Warto odnotować częściową militaryzację komponentu pożarniczego w największych aglomeracjach, gdzie formacje straży

pożarnej posiadają status wojskowy i podlegają odpowiednio armii lub marynarce, co stanowi rozwiązanie specyficzne na tle europejskim. Jednocześnie w skali kraju system w znacznym stopniu opiera się na wolontariacie – zdecydowaną większość personelu pożarniczego stanowią strażacy ochotnicy, co wzmacnia zdolność reagowania w oparciu o zasoby lokalne, przy zachowaniu jednolitych standardów organizacyjnych. Na poziomie gminy szczególną rolę pełni mer (burmistrz), który posiada ustawowe obowiązki w zakresie przygotowania planów ochrony ludności, w tym opracowania gminnego planu ratunkowego (Plan Communal de Sauvegarde) oraz możliwości tworzenia lokalnych rezerw bezpieczeństwa cywilnego, przewidzianych do wsparcia działań w sytuacjach kryzysowych. Jednym z kluczowych elementów francuskiego modelu jest prowadzenie działań według zestandaryzowanych planów i procedur w ramach systemu ORSEC (Organisation de la Réponse de Sécurité Civile). ORSEC stanowi ramę organizacyjną planowania operacyjnego, rozwijaną historycznie i zreformowaną ustawowo w 2004 r., obejmującą scenariusze zagrożeń, przypisanie ról podmiotom zaangażowanym w reagowanie oraz mechanizmy koordynacji międzyinstytucjonalnej. Plany ORSEC funkcjonują na poziomie departamentów i stref, zapewniając spójność działań w różnych konfiguracjach zdarzeń. Szczególnie istotny jest obowiązek regularnego ćwiczenia planów oraz utrzymywania wysokiej dyscypliny szkoleniowej, obejmującej zarówno administrację terenową, jak i służby, a także podmioty infrastruktury krytycznej i zakłady stwarzające podwyższone ryzyko, które zobowiązane są do cyklicznych prób alarmów i ewakuacji. Komplementarną funkcję pełni system bieżącego monitorowania sytuacji kryzysowej na poziomie centralnym, realizowany przez centra operacyjne DGSCGC, a spójność planowania w skali państwa jest wzmacniana przez struktury odpowiedzialne za kwestie obrony i bezpieczeństwa narodowego przy organach centralnych. Za szczególnie wartościowe w praktyce francuskiej uznaje się konsekwentną standaryzację ról, procedur i planów oraz jednoznaczne umocowanie administracji rządowej w koordynacji działań. Precyzyjnie zdefiniowane kompetencje prefektów i merów zwiększają przewidywalność decyzji w sytuacji zagrożenia i ograniczają ryzyko rozproszenia odpowiedzialności. System ORSEC stanowi narzędzie integrujące szerokie spektrum uczestników reagowania, obejmujące nie tylko formacje ratownicze i porządkowe, lecz także podmioty ochrony

zdrowia, wojsko, organizacje pozarządowe oraz operatorów infrastruktury, dzięki czemu w fazie reakcji możliwe jest uruchomienie współdziałania w oparciu o wcześniej uzgodnione role i kanały komunikacji. Znaczącym atutem pozostaje również obowiązkowość i regularność ćwiczeń, co sprzyja utrzymaniu realnej gotowości operacyjnej oraz identyfikacji luk organizacyjnych w warunkach kontrolowanych. Uzupełnieniem tych rozwiązań są scentralizowane zasoby ratownicze na szczeblu krajowym, przeznaczone do wsparcia terenowych struktur w sytuacjach nadzwyczajnych, w tym wyspecjalizowane komponenty lotnicze wykorzystywane m.in. w działaniach gaśniczych. W obszarze ostrzegania ludności Francja wdrożyła nowoczesny system FR-Alert oparty na technologii cell broadcast, który umożliwia szybkie przekazanie komunikatu alarmowego do wszystkich urządzeń mobilnych znajdujących się w strefie zagrożenia, niezależnie od stopnia obciążenia sieci. Rozwiązanie to uzupełnia tradycyjną sieć syren alarmowych, wzmacniając zasięg i niezawodność informowania oraz pozwalając na przekazanie instrukcji postępowania w sposób bezpośredni i jednoznaczny. Z perspektywy polskiej szczególnie istotne są doświadczenia Francji związane z centralną koordynacją działań przy zachowaniu odpowiedzialności i inicjatywy na poziomie lokalnym. W polskich realiach analogiczną funkcję do prefektów pełnią wojewodowie, dlatego zasadne pozostaje dalsze wzmacnianie ich zaplecza analitycznego i operacyjnego, w tym zdolności wojewódzkich struktur zarządzania kryzysowego do realnego kierowania koordynacją w zdarzeniach o szerszym zasięgu. Istotnym kierunkiem jest również rozwój planowania operacyjnego opartego na standardowych scenariuszach zagrożeń oraz systematyczne, cykliczne ćwiczenia międzyresortowe obejmujące administrację, służby i – w odpowiednim zakresie – podmioty infrastruktury krytycznej oraz społeczność lokalną. W obszarze ostrzegania ludności zasadne jest konsekwentne rozwijanie rozwiązań zbliżonych do cell broadcast, jako uzupełnienia klasycznych kanałów powiadomień, przy jednoczesnym prowadzeniu działań informacyjnych budujących zrozumienie komunikatów alarmowych. Wreszcie, rozwiązania francuskie wskazują na użyteczność lokalnych rezerw bezpieczeństwa cywilnego, które w warunkach polskich mogłyby przyjąć postać gminnych zespołów wsparcia operacyjnego współpracujących z samorządem, OSP i organizacjami ratowniczymi, realizujących zadania pomocnicze w ewakuacji, organizacji

punktów tymczasowego schronienia oraz dystrybucji podstawowych świadczeń w sytuacjach kryzysowych.

Na tle państw nordyckich Szwecja jest często wskazywana jako przykład konsekwentnie rozwijanego modelu odporności państwa, w którym bezpieczeństwo ujmowane jest w sposób całościowy, obejmujący równorzędnie komponent militarny i cywilny. Fundamentem tego podejścia pozostaje koncepcja obrony totalnej (Totalförsvaret), zakładająca, że w sytuacji poważnego kryzysu lub konfliktu każda instytucja publiczna, podmioty sektora prywatnego oraz obywatele mają określone role i obowiązki w podtrzymaniu podstawowych funkcji państwa. Ramy prawne obrony powszechnej opierają się na rozwiązaniach, w których obowiązki obronne obejmują szeroki przedział wieku (w praktyce 16-70 lat) i mogą być realizowane w różnych formach: od służby wojskowej, przez zadania w strukturach cywilnych, po wsparcie organizacyjne i logistyczne na rzecz utrzymania ciągłości działania państwa. W okresie pokoju system opiera się na standardowych strukturach administracji rządowej i samorządowej, natomiast w warunkach zagrożenia przewidziane są mechanizmy stopniowego przechodzenia w tryb funkcjonowania odpowiadający wymaganiom obrony totalnej, w tym uruchamiania procedur związanych z mobilizacją zasobów, priorytetyzacją usług publicznych oraz zapewnieniem dostaw dóbr krytycznych. Kluczową instytucją w cywilnej części systemu jest Szwedzka Agencja ds. Sytuacji Nadzwyczajnych (Myndigheten för samhällsskydd och beredskap – MSB), odpowiedzialna za koordynację przygotowań, rozwój standardów i wytycznych dla administracji i podmiotów prywatnych, wspieranie planowania ciągłości działania oraz prowadzenie działań informacyjnych i edukacyjnych. Szczególne znaczenie przypisuje się poziomowi lokalnemu: gminy mają obowiązek utrzymywania zdolności do realizacji podstawowych usług i funkcji publicznych również w warunkach zakłóceń, izolacji lub ograniczonej dostępności zasobów, obejmując w szczególności ochronę przeciwpożarową, opiekę medyczną, zaopatrzenie w wodę, wsparcie socjalne oraz organizację pomocy dla ludności. Istotnym elementem infrastrukturalnym pozostaje rozbudowany system schronów cywilnych, w dużej mierze odziedziczony po okresie zimnej wojny, utrzymywany jako zasób możliwy do uruchomienia w krótkim czasie w razie eskalacji zagrożeń. W praktyce utrzymywanie schronów jest uzupełniane przez system informacji publicznej umożliwiający lokalizowanie

dostępnych obiektów oraz weryfikację ich przeznaczenia w kontekście ochrony ludności. Szwedzki model kładzie nacisk na przygotowanie społeczeństwa do funkcjonowania w warunkach ograniczonej dostępności pomocy zewnętrznej. W rekomendacjach rządowych oraz w komunikacji publicznej przyjmuje się, że gospodarstwa domowe powinny być zdolne do samodzielnego przetrwania co najmniej przez siedem dni, w tym w zakresie zapasów wody, żywności, podstawowych środków higienicznych i elementarnego zabezpieczenia energetycznego. Podejście to stanowi rozwinięcie wcześniejszych zaleceń krótszego okresu samowystarczalności i wynika z doświadczeń związanych z przerwami w dostawach energii, zakłóceniami pogodowymi oraz ryzykami o charakterze systemowym. Wymiar edukacyjny jest realizowany w sposób konsekwentny i masowy, czego przykładem była dystrybucja do gospodarstw domowych materiałów informacyjnych przygotowanych przez MSB, zawierających praktyczne instrukcje postępowania w sytuacjach kryzysowych, zarówno o charakterze naturalnym, technologicznym, jak i związanym z zagrożeniami bezpieczeństwa państwa. W komunikacji publicznej utrwalono przekonanie, że odporność państwa jest współodpowiedzialnością instytucji i obywateli, a przygotowania społeczne stanowią element infrastruktury bezpieczeństwa porównywalny z zasobami technicznymi i organizacyjnymi. W ostatnich latach Szwecja podjęła również działania odtworzeniowe w zakresie zdolności obrony cywilnej, które po zakończeniu zimnej wojny zostały w istotnym stopniu ograniczone. Zmiana środowiska bezpieczeństwa po 2014 r. przyspieszyła proces odbudowy instrumentów odporności, w tym rozwijania rezerw strategicznych, modernizacji łączności kryzysowej, wzmacniania logistyki i zdolności ratowniczych oraz pogłębiania integracji planowania wojskowego i cywilnego. Charakterystyczne jest przy tym podejście długoterminowe, oparte na katalogowaniu scenariuszy skrajnych (np. długotrwałe przerwy w dostawach energii, zakłócenia łańcuchów dostaw, zagrożenia hybrydowe) i budowaniu mechanizmów utrzymania funkcji krytycznych w warunkach presji systemowej. Rozwiązania te są wspierane cyklicznymi ćwiczeniami, w tym grami decyzyjnymi na poziomie centralnym oraz szkoleniami i ćwiczeniami angażującymi administrację lokalną i podmioty infrastruktury krytycznej, co sprzyja utrwalaniu nawyków współdziałania międzysektorowego. W kontekście polskim doświadczenia szwedzkie wzmacniają argumenty na rzecz

rozwoju filozofii odporności powszechnej, rozumianej jako trwałe powiązanie planowania cywilnego z systemem bezpieczeństwa narodowego oraz jako praktyczne włączenie administracji, sektora prywatnego i obywateli w przygotowanie do sytuacji nadzwyczajnych. Szczególnie istotne są trzy elementy: systemowe budowanie kompetencji i gotowości gospodarstw domowych, rozwój infrastruktury ochronnej i rezerw oraz konsekwentna koordynacja działań międzyresortowych i międzysektorowych, obejmująca także operatorów usług kluczowych. Szwedzki model pokazuje również znaczenie przejrzystej, regularnej komunikacji publicznej o zagrożeniach i standardach postępowania, która wzmacnia zaufanie społeczne i ogranicza ryzyko dezinformacji w sytuacjach kryzysowych. W praktyce oznacza to potrzebę utrzymywania stałych programów edukacyjnych, klarownych instrukcji dla ludności oraz mechanizmów ćwiczeń, które traktują społeczeństwo nie jako biernego odbiorcę pomocy, lecz jako aktywnego uczestnika systemu ochrony ludności.

W warunkach stałej ekspozycji na zagrożenia naturalne, takie jak trzęsienia ziemi, tsunami, erupcje wulkanów, tajfuny czy osuwiska, system ochrony ludności Japonii został ukształtowany jako rozwiązanie wysoko sformalizowane, wielopoziomowe i silnie oparte na technologiach oraz utrwalonej kulturze przygotowań. Doświadczenia wielkoskalowych katastrof – w tym trzęsienia ziemi w regionie Kantō (1923 r.) oraz trzęsienia ziemi w Kobe (1995 r.) – stanowiły istotne impulsy do rozwoju ram prawnych, modernizacji standardów infrastrukturalnych oraz doskonalenia procedur reagowania, co w konsekwencji lokuje Japonię wśród najbardziej zaawansowanych państw w obszarze redukcji ryzyka katastrof. Podstawy organizacyjne wyznacza Podstawowa Ustawa o Przeciwdziałaniu Katastrofom z 1961 r., wielokrotnie nowelizowana w oparciu o wnioski wyciągane z kolejnych zdarzeń. W ramach tego systemu funkcjonuje Centralna Rada ds. Zarządzania Kryzysowego, koordynująca politykę państwa w zakresie zapobiegania, przygotowania i reagowania. Utrzymywany jest rozwinięty model planowania, w którym opracowywany jest plan krajowy, a jego operacjonalizacja następuje poprzez plany sektorowe oraz plany lokalne na poziomie prefektur i gmin, umożliwiające uwzględnianie specyfiki zagrożeń oraz warunków terenowych. Za rozwiązania szczególnie istotne uznawane są zaawansowane systemy wczesnego ostrzegania i alarmowania. Od 2007

r. eksploatowany jest system wczesnego ostrzegania o trzęsieniach ziemi, umożliwiający przekazanie alarmu do ludności w ciągu sekund od wykrycia wstrząsów, jeszcze przed dotarciem fal sejsmicznych do obszarów zabudowanych. Mechanizm ten, mimo ograniczonego czasu reakcji, pozwala na wykonanie podstawowych czynności ochronnych (np. przerwanie pracy urządzeń, zajęcie bezpiecznej pozycji, ograniczenie ryzyka pożaru), co w skali populacyjnej przekłada się na redukcję strat. W obszarze ostrzegania przed tsunami rozwinięto procedury oparte na zasadzie ostrożności, w których w przypadku niepewności parametrów zjawiska komunikowany jest wysoki poziom zagrożenia, aby uniknąć zaniżenia ryzyka. Funkcjonuje również ogólnokrajowy system alarmowania J-Alert, wykorzystujący łączność satelitarną i kanały masowego przekazu do szybkiej dystrybucji komunikatów, w tym w odniesieniu do zagrożeń o charakterze bezpieczeństwa państwa (np. ostrzeżeń przed incydentami rakietowymi). Drugim filarem japońskiego modelu pozostaje prewencja infrastrukturalna oraz konsekwentne podnoszenie standardów technicznych, zwłaszcza w zakresie budownictwa i zabezpieczeń przeciwpowodziowych. Systematycznie rozwijane są rozwiązania inżynierskie ograniczające skutki ekstremalnych zjawisk, w tym urządzenia retencyjne i systemy sterowania przepływem wód, zabezpieczenia przeciwoświsiskowe oraz technologie podnoszące odporność obiektów na wstrząsy sejsmiczne. Znaczącą rolę odgrywają normy budowlane oraz mechanizmy kontroli ich realizacji, modyfikowane po kolejnych katastrofach. Przykładowo, po trzęsieniu ziemi w 1978 r. wzmocniono kodeks budowlany w zakresie odporności sejsmicznej, a analiza skutków trzęsienia ziemi w Kobe (1995 r.) potwierdziła, że budynki wzniesione według nowszych standardów wykazywały znacząco większą odporność w porównaniu z zabudową starszą. Utrwalone zostało podejście traktujące zdarzenia nadzwyczajne jako źródło danych do doskonalenia przepisów, procedur i rozwiązań technicznych, co jest wspierane przez praktykę raportowania i wdrażania rekomendacji po zdarzeniach. Obok technologii i infrastruktury szczególne znaczenie ma kultura przygotowań, budowana poprzez stałą edukację i regularne ćwiczenia. Utrzymywana jest wysoka częstotliwość treningów ewakuacyjnych i alarmowych w szkołach, zakładach pracy oraz przestrzeni publicznej, a działania edukacyjne obejmują kształtowanie właściwych nawyków od najwcześniejszych etapów kształcenia. W praktyce operacyjnej

znaczącą rolę odgrywa ponadto aktywizacja społeczności lokalnych w ramach planowania wspólnotowego i struktur samopomocowych, wspierających działania formalnych służb w fazie reagowania i wczesnej odbudowy. Wzrost zaangażowania wolontariatu po katastrofach (w szczególności po 2011 r.) został włączony do rozwiązań systemowych, co wzmacnia zdolności logistyczne i organizacyjne w skali lokalnej. W ujęciu implikacji dla Polski doświadczenia japońskie akcentują potrzebę równoległego rozwoju komponentu technologicznego i społecznego w ochronie ludności. W warunkach krajowych, przy odmiennym profilu zagrożeń (m.in. nawałnice, powodzie błyskawiczne, incydenty przemysłowe), szczególne znaczenie uzyskuje rozbudowa systemów wczesnego ostrzegania i automatycznego alarmowania, w tym integracja danych hydrometeorologicznych oraz rozwój mechanizmów dystrybucji komunikatów o wysokiej niezawodności. W obszarze infrastruktury zasadne pozostaje wzmacnianie odporności obiektów i systemów krytycznych na zjawiska ekstremalne, w tym modernizacja zabezpieczeń przeciwpowodziowych, ograniczanie ryzyk osuwiskowych oraz podnoszenie standardów odporności sieci energetycznych i teleinformatycznych na oddziaływanie czynników pogodowych. Wymiar kulturowy wskazuje na użyteczność systematycznych ćwiczeń i praktycznej edukacji z zakresu reagowania kryzysowego, obejmującej scenariusze szersze niż ewakuacje pożarowe, a także na wartość wspólnotowego planowania działań w skali osiedli i gmin jako instrumentu wzmacniania odporności lokalnej. Istotnym elementem pozostaje również wdrażanie rutynowej analizy ex post zdarzeń o znaczącej skali, prowadzącej do formalnych wniosków i korekt systemowych, tak, aby każdy kolejny kryzys generował mniejsze straty dzięki kumulacji doświadczeń i udoskonaleniom organizacyjnym.

Dla syntetycznego zestawienia wniosków z analizy porównawczej przygotowano ujęcie tabelaryczne. W tabeli 4 zaprezentowano wybrane rozwiązania z zakresu ochrony ludności i zarządzania kryzysowego stosowane w Stanach Zjednoczonych, Niemczech, Francji, Szwecji oraz Japonii, ze wskazaniem elementów uznawanych za dobre praktyki. Zestawienie uzupełniono oceną potencjału adaptacji tych rozwiązań w warunkach polskich, w szczególności w odniesieniu do standaryzacji dowodzenia i planowania, roli wolontariatu i zasobów społecznych, systemów ostrzegania i alarmowania oraz budowania odporności infrastrukturalnej i społecznej.

Tabela 4. Wybrane zagraniczne rozwiązania w ochronie ludności i ich potencjał transferu do Polski

Państwo	Przykładowe rozwiązania (dobre praktyki)	Możliwość adaptacji w Polsce (wnioski)
USA	<ul style="list-style-type: none"> – Standaryzowany Incident Command System (ICS) i Narodowy System Zarządzania Incydentami (ujednolicone struktury dowodzenia). – Podejście all-hazards: jeden zintegrowany system planowania na wszystkie rodzaje zagrożeń. – Współpraca z NGO: partnerstwo FEMA z Czerwonym Krzyżem i wolontariuszami, programy edukacyjne dla ludności. 	<ul style="list-style-type: none"> – Wdrożenie elementów ICS między służbami (uspójnienie dowodzenia podczas kryzysów). – Kompleksowe podejście wszystkie zagrożenia: aktualizacja planów kryzysowych, aby obejmowały pełne spektrum ryzyk (np. cyberzagrożenia obok klęsk żywiołowych). – Budowa partnerstw z NGO: formalne włączenie organizacji pozarządowych i OSP w krajowy system reagowania kryzysowego.
Niemcy	<ul style="list-style-type: none"> – Federalna Agencja THW z ~88 tys. przeszkolonych wolontariuszy technicznych (wsparcie służb zawodowych). – Ochotnicze straże pożarne jako podstawa systemu na prowincji (wysoki wskaźnik ochotników na 1000 mieszk.). – Wielo-poziomowa koordynacja: lokalne sztaby operacyjne + polityczne komitety kryzysowe na wyższych szczeblach. – Nowoczesne ostrzeganie (syreny + aplikacja NINA + komunikaty CB) i coroczne testy alarmowe. 	<ul style="list-style-type: none"> – Rozwój wolontariatu ratowniczego: utworzenie Korpusu OC (zgodnie z ustawą z 2024 r.) na wzór THW, z zapewnieniem szkoleń i sprzętu dla ochotników. – Utrzymanie i wzmocnienie OSP jako kluczowego elementu systemu (dofinansowanie, integracja w planach kryzysowych). – Ćwiczenie koordynacji wieloszczeblowej: regularne duże ćwiczenia od gminy po szczebel centralny, zgrywające działania sztabów. – Ulepszenie systemu alarmowego: rozwój zintegrowanej aplikacji/CB do ostrzegania oraz Warntag – ogólnokrajowych testów syren i komunikatów.

Państwo	Przykładowe rozwiązania (dobre praktyki)	Możliwość adaptacji w Polsce (wnioski)
Francja	<ul style="list-style-type: none"> Centralny nadzór prefektów: silna rola przedstawiciela rządu (prefekta) w kierowaniu akcją na poziomie departamentu/strefy. Plany ORSEC: standardowe plany reagowania dla każdego regionu, określające role służb i władz. Powszechne ćwiczenia: obowiązkowe coroczne ćwiczenia ratownicze dla administracji i zakładów przemysłowych. FR-Alert: nowoczesny system ostrzegania ludności przez komunikaty na telefony (cell broadcast)(frfrancja.fr/frfrancja.fr). 	<ul style="list-style-type: none"> Wzmocnienie roli wojewodów w sytuacjach kryzysowych (usprawnienie łączności, procedur przekazywania decyzji od centrum do terenu). Opracowanie uniwersalnych planów reagowania na wzór ORSEC – gotowe scenariusze działań dla typowych zagrożeń w każdym województwie. Instytucjonalizacja regularnych ćwiczeń: zobowiązanie urzędów i obiektów infrastruktury do okresowych treningów kryzysowych. Wdrożenie systemu CB: pełne uruchomienie i popularyzacja w Polsce technologii broadcast SMS dla alarmów (zgodnie z wymogiem UE).
Szwecja	<ul style="list-style-type: none"> Obrona powszechna: zintegrowanie obrony cywilnej z wojskową, obowiązek przygotowania obywateli do działania w warunkach kryzysu/wojny. Szeroka sieć schronów: ~65 tys. schronów cywilnych utrzymywanych na bieżąco, publiczny rejestr i plany szybkiego uruchomienia. Autonomia obywatelska: zalecenie posiadania zapasów na 7 dni, ogólnokrajowa kampania informacyjna (brozury „If Crisis or War Comes”). Całościowa strategia odporności: państwo identyfikuje „najgorsze przypadki” i zawczasu planuje sposoby utrzymania ciągłości działania (żywność, energia, łączność). 	<ul style="list-style-type: none"> Integracja planowania cywilno-wojskowego: włączenie komponentu OC do strategii bezpieczeństwa narodowego RP, rozwijanie Rządowego Zespołu OC z udziałem MON. Program budowy schronów publicznych i osiedlowych (już zapoczątkowany w 2025 r.) – kontynuacja tak, by zwiększyć pokrycie schronami głównych miast. Edukacja i komunikacja: dalsze akcje uświadamiające obywateli (np. doroczna aktualizacja poradnika „Bezpieczna Polska”, kampanie w mediach o gotowości na blackout itp.). Rezerwy i ciągłość dostaw: rozbudowa państwowych rezerw strategicznych (żywność, paliwo) oraz planów awaryjnego zaopatrzenia ludności na poziomie lokalnym.

Państwo	Przykładowe rozwiązania (dobre praktyki)	Możliwość adaptacji w Polsce (wnioski)
Japonia	<ul style="list-style-type: none">– Zaawansowane systemy wczesnego ostrzegania: automatyczne alarmy o trzęsieniu ziemi (kilkanaście sekund wyprzedzenia), skuteczny system ostrzegania tsunami.– Surowe normy budowlane: budynki projektowane na wysoką odporność sejsmiczną, ciągle ulepszanie przepisów po każdej katastrofie (np. kodeks z 1981 r. ograniczył szkody w 1995 r. – tylko 3% nowych budynków uległo zawaleniu).– Narodowa kultura ćwiczeń: co roku 1 września ogólnokrajowe ćwiczenia na wypadek katastrofy, liczne treningi lokalne, Dni Pamięci (edukacja o lekcyjach z katastrof).– Wsparcie społeczności: promowanie lokalnych planów kryzysowych i grup sądeckich, silny ruch wolontariuszy (Dzień Wolontariatu 17 stycznia).	<ul style="list-style-type: none">– Modernizacja technologiczna: rozwój systemów prognozy stycznych IMGW, rozbudowa czujników hydrologicznych i sejsmicznych, integracja danych w RCB, aby szybciej przekazywać ostrzeżenia ludności (np. SMS o zbliżającej się trąbie powietrznej).– Wzmocnienie standardów odporności infrastruktury: audyty budynków użyteczności publicznej pod kątem odporności na ekstremalne zjawiska (wiatry, śnieżyce), promowanie budownictwa spełniającego wyższe normy bezpieczeństwa.– Ćwiczenia społeczne: ustanowienie stałego kalendarza ogólnokrajowych i lokalnych ćwiczeń zarządzania kryzysowego z udziałem mieszkańców (np. symulacja ewakuacji dzielnic podczas powodzi).– Aktywizacja społeczna: wspieranie inicjatyw oddolnych – dotacje dla gmin organizujących szkolenia pierwszej pomocy, tworzenie osiedlowych magazynów sprzętu kryzysowego (np. pompy, agregaty) zarządzanych przez mieszkańców.

Źródło: opracowanie własne na podstawie: A. Olech, Przygotowani na wojnę, czyli szwedzka obrona powszechna, <https://infosecurity24.pl/za-granica/przygotowani-na-wojne-czyli-szwedzka-obrona-powszechna>, 2025, [dostęp: 10.10.2025]; European Parliamentary Research Service (EPRS), Japan’s disaster risk reduction and preparedness – selected solutions, European Parliament, 2025, [dostęp: 10.10.2025].

Rozdział VI.

Wyzwania, trendy i kierunki rozwoju zarządzania kryzysowego

6.1. Nowe typy zagrożeń: cyber, hybrydowe i środowiskowe

We współczesnym środowisku bezpieczeństwa pojawiły się nowe typy zagrożeń, które znacząco wpływają na podejście do zarządzania kryzysowego. Do najważniejszych z nich należą zagrożenia cybernetyczne (w cyberprzestrzeni), zagrożenia hybrydowe oraz zagrożenia środowiskowe. Stanowią one wyzwanie zarówno dla Polski, jak i społeczności międzynarodowej, wymagając dostosowania systemów reagowania i budowy odporności państwa⁴³⁸. Niniejszy rozdział przedstawia typologię i charakterystykę tych zagrożeń, mechanizmy ich identyfikacji, aktualne trendy i wyzwania, a także rozwiązania systemowe w zakresie zarządzania kryzysowego. Analiza koncentruje się na Polsce, uwzględniając jednak tło międzynarodowe – działania podejmowane w ramach Unii Europejskiej, NATO oraz przez państwa partnerskie – w ujęciu porównawczym.

Zagrożenia cybernetyczne (cyberzagrożenia) dotyczą wszelkich działań wymierzonych w systemy teleinformatyczne, sieci komputerowe oraz przetwarzane w nich informacje, które mogą skutkować zakłóceniem ich

⁴³⁸ S. Wojciechowska-Filipek, Z. Ciekankowski, Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa, wyd. 2, Wydawnictwo CeDeWu, 2019.

funkcjonowania, kradzieżą danych lub innymi szkodami. Typologia cyberzagrożeń obejmuje między innymi:

- cyberprzestępczość, atakująca systemy w celach finansowych lub kryminalnych,
- cyberterroryzm, czyli działania mające wywołać strach lub destabilizację przez grupy terrorystyczne,
- cyberszpiegostwo, czyli wykradanie informacji przez obce służby lub grupy hakerskie,
- cyberwojnę i cyberataki sponsorowane przez państwa, wykorzystujące wyspecjalizowane techniki przeciw infrastrukturze krytycznej i administracji.

Charakterystyczną cechą cyberzagrożeń jest ich globalny zasięg i wysoka dynamika – ataki mogą pochodzić z dowolnego miejsca na świecie, przebiegają w ułamkach sekund, a metody działania np. złośliwe oprogramowanie, phishing, ransomware są stale rozwijane. Znaczącym trendem ostatnich lat jest wzrost skali i skoordynowania ataków na infrastrukturę krytyczną jak energetyczną, transportową, finansową, czy służbę zdrowia, często z udziałem grup powiązanych z obcymi państwami. Przykładowo, według analiz firmy Check Point w 2023 r. Polska doświadczyła około 80 tysięcy cyberataków – dwukrotnie więcej niż rok wcześniej – a prognozy wskazują, że w 2024 r. liczba ta może przekroczyć 100 tysięcy⁴³⁹. Ataki te coraz częściej wymierzone są w administrację rządową, systemy wojskowe, szpitale czy sieci energetyczne, czemu sprzyja napięta sytuacja geopolityczna (konflikt rosyjsko-ukraiński) i zaangażowanie hackerów sponsorowanych przez państwa. Wojna cybernetyczna to już nie tylko proste włamania czy zakłócanie usług (np. ataki DDoS), ale operacje mogące sparaliżować całe miasta lub państwa – jak ataki na systemy energetyczne i transportowe odnotowane podczas działań Rosji przeciw Ukrainie (lata 2015-2022), powodujące m.in. przerwy w dostawach prądu.

Mechanizmy identyfikacji zagrożeń cybernetycznych opierają się na stałym monitorowaniu sieci i systemów przez wyspecjalizowane jednostki.

⁴³⁹ M. Jaślan, W 2024 r. liczba cyberataków na Polskę może przekroczyć 100 tys. TELKO, 2024, <https://www.telko.in/w-2024-r-liczba-cyberatakow-na-polske-moze-przekroczyc-100-tys-2>, [dostęp: 10.10.2025].

W Polsce funkcjonuje rozbudowany system zespołów reagowania na incydenty komputerowe (CSIRT), tworzonych m.in. przez CERT Polska w NASK oraz zespoły resortowe np. CSIRT MON dla wojska, czy CSIRT GOV dla administracji. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, operatorzy usług kluczowych (np. w sektorze energii, transportu, bankowości) mają obowiązek wdrażać środki ochrony i zgłaszać poważne incydenty, co umożliwia ich szybką identyfikację i analizę⁴⁴⁰. Wykorzystuje się zaawansowane techniki, jak systemy detekcji włamań, sztuczną inteligencję do analizy anomalii w ruchu sieciowym oraz wymianę informacji o zagrożeniach na poziomie krajowym i międzynarodowym. Ważną rolę odgrywa współpraca międzynarodowa – państwa UE uzgodniły wspólne ramy reagowania na incydenty o dużej skali tzw. EU Cybersecurity Blueprint⁴⁴¹ oraz implementują dyrektywę NIS2, która zaostrza wymagania bezpieczeństwa i współpracy w zakresie cyberincydentów⁴⁴². Identyfikację ułatwia też aktywność służb wywiadowczych i kontrwywiadowczych, które śledzą kampanie wrogich grup APT. Niemniej, wyzwania pozostają: ataki często cechują się wysokim stopniem utajenia i nowatorstwa, co utrudnia ich wczesne wykrycie; brakuje też specjalistów w dziedzinie cyberbezpieczeństwa, a rosnąca liczba urządzeń (IoT) tworzy nowe wektory ataku.

Zagrożenia hybrydowe stanowią złożoną kategorię, która łączy różnorodne formy wrogich działań – zarówno konwencjonalnych, jak i niekonwencjonalnych – poniżej progu otwartej wojny. Nie istnieje jedna, sztywna definicja, termin pozostaje elastyczny, aby obejmować zmieniający się charakter tych zagrożeń⁴⁴³. Ogólnie, działania hybrydowe to skoordynowane, celowe operacje prowadzone przez podmioty państwowe lub niepaństwowe, mające na celu zaszkodzenie państwu lub instytucji poprzez użycie różnych środków jednocześnie. Arsenal hybrydowy obejmuje m.in. manipulacje informacyjne i dezinformację, cyberataki, presję ekonomiczną, szantaż

⁴⁴⁰ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).

⁴⁴¹ EU-Cybersecurity-Blueprint: European Commission, EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises – Blueprint, Brussels, 2017.

⁴⁴² NIS2-Directive: Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (Dz. Urz. UE L 333 z 27.12.2022).

⁴⁴³ Rada Unii Europejskiej, Zagrożenia hybrydowe, Bruksela, 2024, <https://www.consilium.europa.eu/pl/policies/hybrid-threats/>, [dostęp: 10.10.2025].

energetyczny, działania wywiadowcze, sabotaż, tajne operacje polityczne, a nawet groźbę użycia siły zbrojnej – przy czym poszczególne elementy są tak dobrane, by wzajemnie się wzmacniać. Celem bywa nie tylko osłabienie bezpieczeństwa, ale również podważenie stabilności demokratycznej – takie działania wymierzone są w podstawowe wartości demokratyczne, dążąc do podzielenia społeczeństwa, siania chaosu informacyjnego i utrudnienia podejmowania decyzji politycznych. Kluczową cechą zagrożeń hybrydowych jest ich trudna identyfikacja i atrybucja – są one konstruowane w taki sposób, aby nie przekraczały progu otwartej agresji zbrojnej, co utrudnia zastosowanie klasycznych mechanizmów obronnych oraz uniemożliwia jednoznaczne wskazanie sprawców. Działania te często mają charakter wielowymiarowy i skryty mogą obejmować równocześnie sferę polityczną, dyplomatyczną, informacyjno-propagandową, gospodarczą, społeczną czy nawet kulturową⁴⁴⁴. Sprawcy korzystają z lokalnych pośredników i „przykrywek” – np. wspierając wybrane organizacje społeczne, partie polityczne, firmy czy medialnych influencerów – co zacierza ślady prowadzące do inicjatora ataku. Jak zauważa Najwyższa Izba Kontroli, właśnie charakter działań hybrydowych – ich kamuflowanie i rozproszenie – powoduje trudności w początkowym rozpoznaniu i kwalifikacji incydentów jako elementów szerszej kampanii wrogiej.

W ostatnich latach zagrożenia hybrydowe stały się palącym wyzwaniem dla bezpieczeństwa narodowego Polski i innych krajów regionu, zwłaszcza w kontekście agresywnej polityki Rosji. Przykładem emblematycznym jest kryzys na granicy polsko-białoruskiej w 2021 r., kiedy reżim w Mińsku celowo wywołał napływ tysięcy migrantów na granice Polski, Litwy i Łotwy jako formę presji politycznej. Działania te, wsparte przez Rosję, przekształciły się w wieloaspektową operację hybrydową – połączono elementy wojny informacyjnej – propaganda oskarżająca Polskę o nieludzkie traktowanie migrantów, presji migracyjnej, jak instrumentalne wykorzystanie migrantów do destabilizacji granicy oraz groźby eskalacji militarnej w tle⁴⁴⁵. Operacja ta miała na celu m.in. zdestabilizowanie sytuacji

⁴⁴⁴ Najwyższa Izba Kontroli (NIK), *Hybrydowe zagrożenie – przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*, (wyniki kontroli), Warszawa, NIK, 2023.

⁴⁴⁵ A. M. Dyner, *The Border Crisis as an Example of Hybrid Warfare*, Polski Instytut Spraw Międzynarodowych (PISM), 02.02.2022, 2022.

wewnętrznej i międzynarodowej pozycji Polski oraz wymuszenie ustępstw od UE w sprawie sankcji na reżim Łukaszenki. Jest to klasyczny przykład, jak działania poniżej progu wojny angażują znaczne siły i środki państwa-ofiary, wywołując sytuację kryzysową o charakterze bezpieczeństwa narodowego. Innym przykładem zagrożenia hybrydowego jest kampania dezinformacyjna wokół pandemii COVID-19 – rozpowszechnianie w Internecie fałszywych informacji o szczepionkach, obostrzeniach czy rzekomych spiskach miało na celu wywołanie nieufności wobec instytucji publicznych i pogłębienie podziałów społecznych, co pośrednio zagrażało skutecznemu zarządzaniu kryzysem zdrowotnym. Służby wielu państw (w tym Polski) wskazywały na udział podmiotów powiązanych z Rosją w szerzeniu antyzachodniej narracji w czasie pandemii, traktując to jako element wojny informacyjnej.

Mechanizmy identyfikacji zagrożeń hybrydowych są z natury trudniejsze niż w przypadku jednoznacznych incydentów (jak atak terrorystyczny czy klęska żywiołowa). Wymagają one ciągłego monitoringu przestrzeni informacyjnej, politycznej i ekonomicznej oraz sprawnej analizy danych wywiadowczych. Kluczowe jest wczesne rozpoznanie wzorców świadczących o skoordynowanej kampanii: np. skumulowania dezinformacji na określony temat, nietypowych ruchów kapitałowych, nagłych zdarzeń o pozornie niepowiązanym charakterze, które mogą stanowić elementy jednego scenariusza. W Polsce powołano specjalne struktury – m.in. Rządowy Zespół Roboczy ds. wczesnej identyfikacji zagrożeń hybrydowych, działający przy Rządowym Zespole Zarządzania Kryzysowego. Zespół ten analizuje potencjalne przejawy działań hybrydowych w obszarach kluczowych dla bezpieczeństwa państwa, wykorzystując metodologię analizy stosowaną przez NATO. Istotna jest także współpraca międzynarodowa: NATO utworzyło specjalne centra doskonalenia, np. Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach (tzw. Hybrid CoE) oraz wdrożyło mechanizmy wymiany ostrzeżeń o hybrydowych działaniach przeciwnika. Unia Europejska z kolei rozwija tzw. pakiet narzędzi antyhybrydowych – zbiór instrumentów koordynowania reakcji na kampanie hybrydowe, przyjęty po raz pierwszy w 2022 r. W jego ramach usprawniana jest identyfikacja złożonych, wielowymiarowych kampanii (m.in. poprzez lepsze łączenie sygnałów z różnych sektorów), a także przygotowanie zespołów szybkiego reagowania na zagrożenia hybrydowe. Niemniej, wyzwania pozostają poważne:

zagrożenia hybrydowe ewoluują wraz z rozwojem technologii i zmianami geopolitycznymi, przez co identyfikacja musi opierać się na scenariuszowym myśleniu o potencjalnych nowych formach ataku. Ponadto, wymaga to ścisłej koordynacji między służbami różnych resortów (wojskowymi, cywilnymi, specjalnymi) oraz współpracy z sektorem prywatnym (np. firmami medialnymi i telekomunikacyjnymi w przypadku walki z dezinformacją). Brak jednoznacznych ram prawnych może utrudniać reagowanie – NIK zauważa, że w polskich dokumentach strategicznych do niedawna brakowało jasnej definicji i przypisania zadań dotyczących zagrożeń hybrydowych. To luka, którą dopiero zaczyna się wypełniać poprzez nowe strategie i nowelizacje ustaw.

Zagrożenia środowiskowe obejmują szeroki zakres zjawisk związanych ze środowiskiem naturalnym, które mogą prowadzić do sytuacji kryzysowych. Zaliczamy tu przede wszystkim klęski żywiołowe (powodzie, susze, wichury, ekstremalne zjawiska pogodowe), a także katastrofy spowodowane przez człowieka, wpływające na środowisko i ludność (awarie przemysłowe, skażenia chemiczne, awarie infrastruktury). W ostatnich dekadach zauważalny jest wzrost częstotliwości i intensywności takich zdarzeń, co wiąże się m.in. z postępującymi zmianami klimatu⁴⁴⁶. Globalne ocieplenie powoduje występowanie groźnych, wcześniej rzadko notowanych anomalii pogodowych na terenie Polski, takich jak długotrwałe susze obejmujące rozległe obszary kraju, rekordowe fale upałów czy nawalne opady prowadzące do błyskawicznych powodzi. Raport Międzynarodowego Zespołu ds. Zmian Klimatu (IPCC) wskazuje, że każde dodatkowe ocieplenie o 0,5°C wyraźnie zwiększa intensywność i częstotliwość ekstremalnych zjawisk pogodowych⁴⁴⁷. Dla oznacza to m.in. większe ryzyko powtarzających się fal upałów (i towarzyszących im zjawisk, jak pożary lasów czy problemy energetyczne), powodzi roztopowych i opadowych, a także huraganowych wiatrów czy trąb powietrznych na obszarach, gdzie dotąd były rzadkością. Równocześnie, zagrożeniem środowiskowym stają się zanieczyszczenia i degradacja środowiska – np. smog w dużych aglomeracjach, zanieczyszczenie wód (co pokazała

⁴⁴⁶ Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, Biuro Bezpieczeństwa Narodowego, 2020.

⁴⁴⁷ IPCC, Zmiana klimatu 2021: Podstawy fizyczne, Wkład Grupy Roboczej I do Szóstego Raportu Oceniającego, Geneva, IPCC, 2021.

katastrofa ekologiczna na Odrze w 2022 r., gdy masowe wymieranie ryb nastąpiło wskutek kombinacji zanieczyszczeń i czynników naturalnych), czy niekontrolowane składowiska odpadów grożące pożarami toksycznymi. Do kategorii tej można zaliczyć również potencjalne skutki awarii przemysłowych i technologicznych, które mają środowiskowo-społeczny wymiar kryzysowy – np. poważne wycieki chemikaliów, eksplozje w zakładach chemicznych lub rafineriach, awarie elektrowni (jak awaria jądrowa w Czarnobylu w 1986 r. czy Fukushima w 2011 r., których skutki przekroczyły granice państw). Choć w Polsce nie doszło dotąd do katastrofy jądrowej, kraj odczuł pośrednio skutki Czarnobyla (skażenie radioaktywne w 1986 r.), co uwiódociło potrzebę planów na wypadek zdarzeń radiacyjnych. Ponadto, Polska doświadczała poważnych katastrof górniczych i awarii przemysłowych np. wybuch w zakładach Nitroerg w 2020 r., które również są przedmiotem zarządzania kryzysowego.

Typowym zagrożeniem środowiskowym o dramatycznych skutkach są powodzie. Polska pamięta szczególnie powódź tysiąclecia z lipca 1997 r., która objęła dorzecze Odry i częściowo Wisły – zginęło wtedy 56 osób, a straty materialne oszacowano na ponad 12 mld zł. Kolejne duże powodzie w 2010 r. (na Wiśle i jej dopływach) potwierdziły utrzymujące się wysokie ryzyko tego rodzaju klęsk. W ostatnich latach pojawiają się również gwałtowne powodzie błyskawiczne na mniejszych ciekach i obszarach miejskich, spowodowane krótkotrwałymi ulewami o ogromnej intensywności (często efekt tzw. stacjonarnych burz nawałnych). Innym przejawem ekstremalnych zjawisk są huragany i trąby powietrzne – np. w 2017 r. niszczycielskie wiatry w Borach Tucholskich powaliły ogromne połacie lasów i spowodowały śmierć kilku osób biwakujących, co ukazało, że nawet w Polsce, tradycyjnie omijanej przez huragany, ryzyko takich zdarzeń rośnie. Susze hydrologiczne z kolei zagrażają rolnictwu i zasobom wody – od 2015 r. niemal co roku notuje się niedobory opadów wpływające na plony i sytuację hydrologiczną rzek. Długotrwała susza zwiększa też zagrożenie pożarowe – np. w 2020 r. rozległy pożar strawił znaczne obszary Biebrzańskiego Parku Narodowego podczas wiosennej suszy. Do zagrożeń środowiskowych zalicza się również tzw. blackoutu energetyczne spowodowane ekstremalnymi warunkami pogodowymi lub przeciążeniem systemu. W Polsce nie doszło dotąd do pełnoskalowego blackoutu, jednak w sierpniu 2015 r. system elektroenergetyczny

znalazł się pod silną presją wskutek rekordowych upałów i suszy, które obniżyły sprawność elektrowni przy jednoczesnym wzroście zapotrzebowania na energię elektryczną. W odpowiedzi na tę sytuację 10 sierpnia 2015 r. wprowadzono ograniczenia w poborze energii elektrycznej dla przemysłu (tzw. 20. stopień zasilania), po raz pierwszy od dziesięcioleci. Działanie to miało na celu ograniczenie ryzyka destabilizacji systemu i uniknięcie niekontrolowanego wyłączenia zasilania na dużą skalę. Eksperci wskazują, że od tego czasu polska energetyka wciąż balansuje na granicy wydolności w okresach szczytowego zapotrzebowania, a groźba blackoutu jest realna zwłaszcza podczas skrajnych zjawisk pogodowych. Przykładem było zdarzenie z maja 2021 r., gdy awaria stacji przesyłowej Rogowiec przy Elektrowni Bełchatów wyłączyła na krótko większość bloków największej elektrowni w kraju – przed masowym wyłączeniem prądu uchronił system jedynie awaryjny import energii z sąsiednich krajów. To pokazuje, że infrastruktura krytyczna jest podatna na zarówno czynniki naturalne (upały, wichury uszkadzające linie przesyłowe), jak i techniczne, a jej awarie mają wymiar kryzysu narodowego.

Identyfikacja zagrożeń środowiskowych opiera się w dużej mierze na systemach wczesnego ostrzegania i monitoringu środowiska. Polska dysponuje rozwiniętym systemem obserwacji meteorologicznych i hydrologicznych – IMGW-PIB (Instytut Meteorologii i Gospodarki Wodnej) prowadzi sieć stacji pomiarowych, radarów meteorologicznych i satelitarnych analiz, które pozwalają wykrywać nadchodzące groźne zjawiska (intensywne opady, silne wiatry, gwałtowne burze) z pewnym wyprzedzeniem. Dzięki temu możliwe jest wydawanie alertów pogodowych (trzystopniowa skala ostrzeżeń IMGW) oraz prognoz hydrologicznych, np. ostrzegających przed przekroczeniem stanów alarmowych na rzekach. Od 2018 r. funkcjonuje też państwowy system Alert RCB – rozsyłania ostrzegawczych komunikatów SMS do ludności na zagrożonych obszarach, dotyczących np. nadciągającej nawałnicy, ekstremalnego upału czy skażenia wody. System ten zwiększa szanse dotarcia z ostrzeżeniem do mieszkańców w celu podjęcia działań ochronnych (ewakuacja z terenów zalewowych, zabezpieczenie dobytku, unikanie przebywania na dworze itp.). Identyfikacja ryzyka środowiskowego dokonuje się także poprzez okresowe oceny i mapy zagrożeń – np. mapy zagrożenia powodziowego opracowane zgodnie z dyrektywą powodziową

UE, mapy osuwisk, monitoring jakości powietrza (pyły PM10/2.5, alerty smogowe) czy inspekcje obiektów przemysłowych pod kątem ryzyka awarii (instalacje objęte tzw. dyrektywą Seveso muszą identyfikować potencjalne scenariusze awaryjne). Na poziomie międzynarodowym istnieją systemy wczesnego ostrzegania, z których Polska korzysta, np. European Flood Awareness System (EFAS) dla wczesnego sygnalizowania ryzyka powodzi w Europie czy Copernicus Emergency Management Service, który dostarcza zobrazowania satelitarne np. na potrzeby reagowania na pożary i powódzie. Pomimo tych narzędzi, wyzwania w identyfikacji zagrożeń środowiskowych rosną ze względu na nieprzewidywalność zmiany klimatu – dotychczasowe wzorce mogą ulec zaburzeniu, co utrudnia prognozowanie. Pojawiają się zagrożenia nakładające się, np. susza zwiększająca ryzyko pożaru, który dodatkowo pogarsza jakość powietrza. Istotnym wyzwaniem jest też świadomość społeczna – społeczeństwo musi rozumieć komunikaty ostrzegawcze i traktować je poważnie; w tym celu prowadzone są kampanie edukacyjne dotyczące zachowania w razie alarmu (np. jak przygotować dom na powódź, co robić podczas upału itp.).

W obliczu opisanych nowych typów zagrożeń – cyber, hybrydowych i środowiskowych – system zarządzania kryzysowego w Polsce oraz w innych krajach podlega intensywnym przeobrażeniom. Aktualne trendy wskazują na dążenie do kompleksowego, zintegrowanego podejścia do bezpieczeństwa. Tradycyjny podział na bezpieczeństwo zewnętrzne (militarne) i wewnętrzne zaciera się: cyberataki czy kampanie dezinformacyjne mogą towarzyszyć konwencjonalnym agresjom, a klęski żywiołowe mogą być wykorzystywane przez przeciwników jako okazja do wrogich działań (np. rozsiewanie paniki). Dlatego strategiczne dokumenty – w tym Strategia Bezpieczeństwa Narodowego RP z 2020 r. – podkreślają potrzebę podniesienia odporności państwa i społeczeństwa na szerokie spektrum zagrożeń. Odporność oznacza zdolność do przetrwania i szybkiego odzyskania sprawności mimo uderzenia kryzysu. Budowanie odporności stało się kluczowym kierunkiem zarówno w Polsce, jak i w politykach NATO oraz UE. Polska w ostatnich latach wprowadza lub aktualizuje szereg strategii i planów w odpowiedzi na nowe zagrożenia. Strategia Cyberbezpieczeństwa RP na lata 2019-2024 stawia za cel podniesienie odporności na cyberzagrożenia wszystkich kluczowych sektorów poprzez wzmocnienie ochrony informacji

i zdolności do wykrywania incydentów. Nowelizacja ustawy o zarządzaniu kryzysowym z 2020 r. przewidywała dodanie narzędzi prawnych do walki z nowymi zagrożeniami: wprost wskazano takie zjawiska jak zmiany klimatu, dezinformacja i cyberprzestępczość jako wyzwania dla służb i administracji. Odpowiedzią ma być między innymi rozbudowa systemów monitorowania ryzyka, lepsza koordynacja działań i – ponownie – wzmacnianie odporności społeczeństwa.

Systemowe rozwiązania w zakresie zarządzania kryzysowego ewoluują w kierunku większej integracji wysiłków różnych podmiotów oraz wielopoziomowej współpracy. W Polsce system zarządzania kryzysowego jest wieloszczeblowy (od gmin przez powiaty i województwa po poziom centralny), co pozostaje fundamentem reagowania na klasyczne zagrożenia (np. powódź lokalna jest najpierw zarządzana przez gminne i powiatowe centra kryzysowe). Jednak nowe zagrożenia wymagają często reakcji skoordynowanej centralnie i międzynarodowo. Dlatego rośnie rola Rządowego Centrum Bezpieczeństwa (RCB) jako instytucji koordynującej wymianę informacji o zagrożeniach cyber i hybrydowych między służbami. Jak wykazała kontrola NIK, RCB – mimo ograniczeń kadrowych i finansowych – jest oceniane pozytywnie jako element systemu, który dysponuje doświadczeniem i współpracą międzynarodową pozwalającą na identyfikację nowych zagrożeń. W celu usprawnienia reagowania, w Krajowym Planie Zarządzania Kryzysowego uwzględniono już scenariusze związane z atakami cybernetycznymi czy przerwami dostaw energii na dużą skalę. Ćwiczenia kryzysowe coraz częściej obejmują symulacje ataków hybrydowych – np. gry decyzyjne przeprowadzone przez NIK w 2023 r. w czterech województwach sprawdzały, jak lokalne organy zareagują na informacje o niespodziewanym zagrożeniu hybrydowym⁴⁴⁸. Wnioski były niepokojące: żaden z badanych zespołów zarządzania kryzysowego nie zajmował się na swoich posiedzeniach problematyką zagrożeń hybrydowych, co sugeruje potrzebę pilnego doskonalenia procedur i świadomości. NIK zarekomendowała m.in. określenie wymogów dotyczących przygotowania osób realizujących zadania z zakresu ochrony

⁴⁴⁸ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi (Informacja o wynikach kontroli; nr ewid. 16/2023/P/22/029/KPB; KPB.430.002.2023), 2023.

ludności w kontekście nowych zagrożeń oraz zwiększenie częstotliwości szkoleń i ćwiczeń uwzględniających scenariusze hybrydowe⁴⁴⁹.

Na szczeblu międzynarodowym, NATO adaptuje swój system zarządzania kryzysowego, aby sprostać zagrożeniom hybrydowym i cybernetycznym. Po doświadczeniach agresji Rosji (hybrydowej w Ukrainie 2014-2015 i pełnoskalowej 2022) Sojusz przyjął szereg inicjatyw: uznał cyberprzestrzeń za osobną domenę operacyjną (2016), stworzył zespoły doradcze do spraw przeciwdziałania zagrożeniom hybrydowym, które mogą wspierać państwa członkowskie, a także zacieśnił współpracę z UE na polu wymiany informacji o tych zagrożeniach. NATO kładzie nacisk na odstraszanie – komunikując potencjalnym agresorom, że działania hybrydowe również spotkają się ze skoordynowaną odpowiedzią Sojuszu. Ponadto, każdy kraj NATO zobowiązał się spełniać 7 podstawowych wymogów odporności (przyjętych w 2016 r.), dotyczących m.in. ciągłości działania władz, zabezpieczenia dostaw energii, funkcjonowania transportu, zaopatrzenia w żywność i wodę, ochrony infrastruktury telekomunikacyjnej, zdolności do reagowania na masowe ofiary oraz funkcjonowania systemów finansowych. Te wymagania dotyczą w równym stopniu zagrożeń wynikających z klęsk żywiołowych, jak i z ataków wrogich (hybrydowych lub cybernetycznych). W ten sposób następuje zbliżenie sfery cywilnej i wojskowej w postrzeganiu odpowiedzialności za bezpieczeństwo⁴⁵⁰. Podobnie Unia Europejska, poprzez Mechanizm Ochrony Ludności UE, wspiera państwa członkowskie w reagowaniu na katastrofy naturalne i przemysłowe – np. umożliwiając szybkie uzyskanie pomocy międzynarodowej przy gaszeniu wielkich pożarów czy powodzi. Po serii katastrofalnych pożarów i powodzi w Europie Komisja utworzyła inicjatywę rescEU – wspólną europejską rezerwę zasobów ratunkowych (samoloty gaśnicze, pomp wysokiej wydajności, szpitale polowe itp.), by szybciej i solidarnie reagować na katastrofy przekraczające możliwości pojedynczego kraju. To element budowania odporności zbiorowej na zagrożenia środowiskowe. Równolegle UE rozwija zdolności przeciwdziałania zagrożeniom hybrydowym: powołano m.in. fusion cell ds. hybrydowych

⁴⁴⁹ Najwyższa Izba Kontroli (NIK), *Hybrydowe zagrożenie – przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*, (wyniki kontroli), Warszawa, NIK, 2023.

⁴⁵⁰ J. Ł. Keplin, *Budowanie odporności państwa na działania hybrydowe*, *Przegląd Bezpieczeństwa Wewnętrznego*, 15(29), 2023. <https://doi.org/10.4467/20801335PBW.23.018.18760>

przy Europejskiej Służbie Działań Zewnętrznych, a także uruchomiono system wczesnego ostrzegania o dezinformacji (platformę wymiany informacji o kampaniach dezinformacyjnych między państwami członkowskimi).

Aktualne badania naukowe akcentują potrzebę holistycznego ujęcia zarządzania kryzysowego wobec tych nowych typów zagrożeń. Podkreśla się, że zdarzenia kryzysowe mogą przybierać charakter kaskadowy – np. poważny cyberatak na system energetyczny może wywołać przerwę w dostawach prądu (blackout), co z kolei rodzi konsekwencje społeczne i ekonomiczne. Dlatego modele analizy ryzyka muszą uwzględniać współzależności infrastruktury i zagrożeń⁴⁵¹. Pojawia się także postulat szerszego wykorzystania scenariuszy stres-testów dla państwa: tak jak testuje się odporność banków, powinno się testować odporność systemu państwowego na jednocześnie wystąpienie np. ataku cybernetycznego, kampanii dezinformacyjnej i klęski żywiołowej. Literatura z zakresu bezpieczeństwa zauważa, że same definicje „zagrożeń hybrydowych” i „odporności” bywają nieprecyzyjne – co może utrudniać tworzenie polityk – jednak panuje zgoda co do kierunku działań: wzmacniać kooperację między instytucjami i państwami, podnosić świadomość społeczną, inwestować w odporność infrastruktury oraz rozwijać nowoczesne technologie monitoringu i obrony⁴⁵². Przykładowo, badania nad wpływem zmian klimatu na bezpieczeństwo narodowe Polski rekomendują poprawę zdolności analitycznych i przepływu informacji między służbami hydrometeorologicznymi a centrami kryzysowymi, tak, aby wcześniej rozpoznawać zagrożenia i skuteczniej ostrzegać ludność. Inne analizy wskazują na potrzebę doskonalenia publicznej komunikacji kryzysowej – w dobie dezinformacji władze muszą szybko i wiarygodnie informować społeczeństwo o zagrożeniach i działaniach zaradczych, aby nie pozostawiać pola plotkom i panice.

Nowe typy zagrożeń – cybernetyczne, hybrydowe i środowiskowe – wymuszają zmianę paradygmatu zarządzania kryzysowego. Kryzysy mogą wynikać zarówno z ataku niewidzialnego wirusa komputerowego, skrytych manipulacji informacją, jak i z gwałtownej siły natury. Polska, podobnie jak

⁴⁵¹ Z. Ciekanski, B. Błaszczak, I. Malinowska, System zarządzania kryzysowego NATO a zagrożenia hybrydowe, *Prawo i Bezpieczeństwo – Law & Security*, 1(2), 2024, s. 7-19. <https://doi.org/10.4467/29567610PIB.24.001.19837>

⁴⁵² J. Ł. Keplin, Budowanie odporności państwa na działania hybrydowe, *Przegląd Bezpieczeństwa Wewnętrznego*, 15(29), 2023. <https://doi.org/10.4467/20801335PBW.23.018.18760>

inne państwa, stoi przed koniecznością rozwijania zintegrowanego systemu bezpieczeństwa narodowego, który łączy elementy ochrony cywilnej, obronności, cyberbezpieczeństwa i ochrony infrastruktury krytycznej. Wymaga to kompleksowych rozwiązań organizacyjno-prawnych – jak postulowana ustawa o ochronie ludności – oraz ciągłego doskonalenia planów i procedur. Kluczowym elementem jest świadomość i zaangażowanie społeczeństwa: obywatel odporny na dezinformację, przygotowany na sytuacje awaryjne i współpracujący z władzami stanowi istotny zasób w systemie odporności państwa. Na szczeblu międzynarodowym zaś, pogłębiona współpraca w ramach UE i NATO wzmacnia wspólną zdolność do przeciwdziałania tym transgranicznym zagrożeniom. Nowe typy zagrożeń będą nadal ewoluować – wyzwaniem kolejnych lat może stać się chociażby wykorzystanie sztucznej inteligencji do generowania dezinformacji na masową skalę czy też konflikty o zasoby wodne spowodowane zmianą klimatu. Dlatego system zarządzania kryzysowego musi pozostać elastyczny, proaktywny i uczący się. Tylko w ten sposób można zapewnić skuteczną ochronę życia obywateli, mienia oraz podstaw funkcjonowania państwa w obliczu złożonych zagrożeń XXI wieku.

6.2. Zarządzanie ryzykiem i odporność społeczna

Tradycyjne podejście do bezpieczeństwa opierało się na reagowaniu post factum na zaistniałe zagrożenia – gaszeniu „pożarów” i usuwaniu skutków kryzysów. Współcześnie następuje jednak wyraźny zwrot w stronę proaktywnego zarządzania ryzykiem i budowania odporności (resilience) systemów społecznych. Doświadczenia ostatnich lat pokazały, że poleganie wyłącznie na przewidywaniu konkretnych zagrożeń i planowaniu reakcji może być niewystarczające. Paradoks nowoczesnych zagrożeń polega na ich coraz większej złożoności i nieprzewidywalności – od ekstremalnych zjawisk pogodowych, poprzez pandemiczne, po zagrożenia hybrydowe. Jak zauważa Ziarko, współczesne kryzysy często wymykają się prostemu prognozowaniu, a przygotowanie się do nich jest utrudnione lub wręcz niemożliwe⁴⁵³.

⁴⁵³ J. Ziarko, Uwarunkowania zarządczego podejścia do społecznej odporności na zagrożenia kryzysowe, *Bezpieczeństwo, Teoria i Praktyka*, 2024, 4(LVII). <https://doi.org/10.2478/2790292223511111>

Nie sposób dokładnie przewidzieć czasu, przebiegu ani skutków wielu zagrożeń, ani tego, jak ludzie i infrastruktura sobie z nimi poradzą. W sytuacji, gdy żadna społeczność nie jest wolna od ryzyka nieprzewidywalnych zagrożeń, strategie reagowania oparte na budowaniu odporności stają się bardziej adekwatne od tradycyjnego planowania opartego na konkretnych scenariuszach.

W skali międzynarodowej ta zmiana paradygmatu została przypieczętowana m.in. przez Ramowy Program Działań z Sendai na lata 2015-2030⁴⁵⁴. Dokument ten podkreśla konieczność przejścia od zarządzania skutkami katastrof do zarządzania ryzykiem katastrof, kładąc nacisk na prewencję, przygotowanie i zwiększanie odporności społeczeństw. Innymi słowy, zamiast koncentrować się wyłącznie na działaniach ratunkowych po katastrofie, państwa i społeczności powinny inwestować w działania przed kryzysem: redukcję ryzyka, edukację, planowanie oraz wzmacnianie zdolności adaptacyjnych. Taka filozofia proaktywnego bezpieczeństwa zakłada, że całe społeczeństwo – obok instytucji publicznych – jest zaangażowane we wspólne budowanie odporności. Seniorzy zarządzania ryzykiem w sektorze prywatnym również zwracają uwagę, że należy przejść od defensywnego reagowania do nastawienia „resilience-first”, traktując odporność jako element strategiczny, a nie wyłącznie operacyjny. Następuje odejście od kultury reaktywnej na rzecz kultury prewencji i odporności. Zarządzanie ryzykiem integruje identyfikację potencjalnych zagrożeń, ocenę ich prawdopodobieństwa i skutków oraz wdrażanie środków zapobiegawczych – zanim kryzys nastąpi. Dzięki temu możliwe jest ograniczenie strat oraz utrzymanie ciągłości działania kluczowych usług nawet w obliczu niespodziewanych zdarzeń⁴⁵⁵. Ważnym aspektem jest tu podejście holistyczne: wzmacnianie odporności nie w jednej sferze, lecz równolegle w infrastrukturze, instytucjach i społecznościach lokalnych. Poniżej omówiono te wymiary odporności oraz ich znaczenie dla bezpieczeństwa.

org/10.48269/2451-0718-btip-2024-4-009

⁴⁵⁴ United Nations Office for Disaster Risk Reduction (UNDRR), Sendai Framework for Disaster Risk Reduction 2015-2030, Geneva, United Nations, 2015.

⁴⁵⁵ A. Mitchell, Risk and Resilience: From Good Idea to Good Practice, OECD Development Co-operation Working Papers nr 13, Paris, OECD Publishing, 2013. <https://doi.org/10.1787/5k3ttg4cxcbbp-en>

Pojęcie resilience (tłumaczone na język polski najczęściej jako odporność, ewentualnie rezyliencja) wywodzi się z nauk przyrodniczych i technicznych, gdzie oznaczało sprężystość lub zdolność materiału do odzyskiwania pierwotnego kształtu. W naukach o bezpieczeństwie termin ten przyjął się dla opisanego zdolności systemów społecznych do przetrwania i rozwoju mimo przeciwności. W literaturze spotyka się różne ujęcia definicyjne. Przykładowo Europejski Trybunał Obrachunkowy definiuje odporność instytucji jako „umiejętność radzenia sobie z negatywnymi skutkami danej sytuacji bądź zdolność do odbudowy po wystąpieniu kataklizmu”, co przekłada się na zdolność administracji publicznej do nieprzerwanego funkcjonowania w kryzysie⁴⁵⁶. Z kolei w kontekście społecznym odporność społeczna bywa definiowana jako zdolność grup i społeczności do przetrwania, adaptacji i odbudowy po kryzysie, dzięki posiadanym zasobom oraz umiejętnościom efektywnego reagowania. Istotne jest, że odporność to nie tylko twarda infrastruktura, ale także ludzie, ich wiedza, kultura i relacje społeczne, które pozwalają działać wspólnie w obliczu zagrożeń⁴⁵⁷.

Badacze są zgodni, że resilience ma charakter wielowymiarowy. Wskazuje się, że odporność społeczności obejmuje komponenty: społeczne, ekonomiczne, instytucjonalne, infrastrukturalne, ekologiczne oraz związane z kapitałem społecznym. Można więc wyróżnić trzy główne płaszczyzny: odporność infrastruktury, odporność instytucji oraz odporność społeczności. Wszystkie one składają się na całościową zdolność społeczeństwa do przetrwania w kryzysie. Infrastruktura krytyczna obejmuje podstawowe systemy techniczne i sieci usług, których sprawne działanie warunkuje funkcjonowanie społeczeństwa i gospodarki. Należą do niej m.in. systemy energetyczne (prąd, ciepło), sieci wodociągowe, systemy łączności i teleinformatyczne, transport i logistyka czy infrastruktura ochrony zdrowia. Odporność infrastruktury oznacza zdolność tych systemów do zapobiegania przerwom, ochrony przed zakłóceniami, skutecznego reagowania na incydenty oraz

⁴⁵⁶ Europejski Trybunał Obrachunkowy, Instytucje UE a pandemia COVID-19. Reakcja była szybka, ale wciąż istnieją wyzwania, jak w optymalny sposób wykorzystać innowacje i elastyczność będące wynikiem kryzysu, Sprawozdanie specjalne nr 18/2022, Luksemburg, 2022. <https://doi.org/10.2865/116653>

⁴⁵⁷ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 10.10.2025].

szybkiego odbudowania funkcji po ewentualnych awariach lub atakach⁴⁵⁸. Według raportu grupy zadaniowej NATO-UE odporność infrastruktury krytycznej definiowana jest jako zdolność do zapobiegania incydentom, ochrony przed nimi, przeciwstawiania się im, a także łagodzenia i absorpcji ich skutków⁴⁵⁹. Innymi słowy, infrastruktura odporna to taka, która nawet jeśli zostanie dotknięta przez katastrofę lub atak, dalej funkcjonuje lub szybko powraca do działania na akceptowalnym poziomie.

Zapewnienie ciągłości działania infrastruktury ma kluczowe znaczenie zwłaszcza podczas kryzysów. Przerwy w dostawie prądu, wody czy paliw natychmiast przekładają się na bezpieczeństwo ludności i mogą potęgować chaos. Wyobraźmy sobie rozległy blackout – miasto pogrążone w ciemności: wstrzymany transport, brak łączności, zagrożenie dla szpitali i służb ratunkowych. Skutki społeczne i ekonomiczne byłyby natychmiastowe i poważne. Dlatego odporność infrastruktury stanowi fundament bezpieczeństwa – od niej zależy, czy w sytuacji nadzwyczajnej społeczność zachowa dostęp do podstawowych usług (energia, woda, komunikacja), czy też doświadczy kaskady awarii. Rosnące zagrożenia (zarówno naturalne, jak i celowe ataki – np. cyberataki na sieci energetyczne) sprawiają, że wzmacnianie infrastruktury jest priorytetem polityki bezpieczeństwa wielu państw. W Unii Europejskiej przyjęto ostatnio regulacje mające zwiększyć odporność podmiotów krytycznych (np. tzw. dyrektywa CER z 2022 r.)⁴⁶⁰, a NATO wspólnie z UE rekomenduje dodatkowe środki ochronne w kluczowych sektorach, takich jak energetyka, transport czy infrastruktura cyfrowa.

Budowanie odporności infrastrukturalnej obejmuje szereg działań technicznych i organizacyjnych. Analiza ryzyka pozwala zidentyfikować potencjalne zagrożenia dla sieci (np. powodzie, ataki hackerskie, przerwy w dostawach komponentów). Na tej podstawie wdraża się środki zwiększające odporność: redundancję (np. zapasowe źródła zasilania, alternatywne trasy przesyłu danych), dywersyfikację dostaw, hardening infrastruktury

⁴⁵⁸ M. Stachoń, Raport Grupy Zadaniowej NATO-UE ds. odporności infrastruktury krytycznej, NASK – Cyber Policy, <https://cyberpolicy.nask.pl/raport-grupy-zadaniowej-nato-ue-ds-odpornosci-infrastruktury-krytycznej>, [dostęp: 10.10.2025].

⁴⁵⁹ Tamże.

⁴⁶⁰ Parlament Europejski i Rada UE, Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych oraz uchylająca dyrektywę Rady 2008/114/WE (Dz.U. UE L 333 z 27.12.2022).

(fizyczne wzmocnienie obiektów, zabezpieczenia przeciwpowodziowe itp.), regularną konserwację i monitorowanie stanu technicznego. Istotnym elementem jest także posiadanie planów awaryjnych i procedur przywracania działania (tzw. plany ciągłości działania – Business Continuity Plans, BCP). Integracja planów ciągłości działania z systemem zarządzania kryzysowego zapewnia spójny, wielowarstwowy system reagowania, łączący bieżące działania ratunkowe z utrzymaniem podstawowych usług. Takie podejście wzmacnia odporność instytucji odpowiedzialnych za infrastrukturę i – co ważne – buduje zaufanie społeczne: gdy obywatele widzą, że nawet w trudnych warunkach prąd płynie, woda jest dostarczana, a telekomunikacja działa, czują się bezpieczniej i pewniej. Należy jednak pamiętać, że żaden system nie jest w 100% odporny. Dlatego równie ważna jak prewencja awarii jest zdolność zarządzania skutkami: posiadanie rezerwowych zasobów (np. agregatów prądotwórczych, zapasów paliwa i wody), sprawna logistyka naprawcza oraz procedury szybkiej odbudowy infrastruktury po zniszczeniu. Odporność infrastruktury jest wypadkową wysiłków technicznych, inwestycji finansowych oraz efektywnej współpracy między sektorem publicznym a prywatnym (większość obiektów krytycznych jest zarządzana przez firmy, które muszą dbać zarówno o bezpieczeństwo, jak i rentowność). Podsumowując, trwałość infrastruktury wobec wstrząsów to podstawowy filar odporności całej społeczności – bez niej trudno mówić o skutecznej reakcji na kryzys.

Drugim kluczowym wymiarem jest odporność instytucji, czyli zdolność organizacji – szczególnie publicznych – do funkcjonowania i wypełniania swoich zadań w warunkach zakłóceń. Instytucje odpowiedzialne za bezpieczeństwo (administracja rządowa i samorządowa, służby ratunkowe, wojsko, policja, szpitale itp.) stanowią kręgosłup systemu zarządzania kryzysowego. Jeśli same ulegną dezorganizacji w obliczu kryzysu, nie będą w stanie skutecznie pomagać społeczeństwu. Odporna instytucja to taka, która ma przygotowane plany na wypadek nadzwyczajny, potrafi szybko dostosować strukturę i sposób działania do nowych warunków oraz zachować ciągłość kluczowych procesów decyzyjnych. Przykładem testu odporności

instytucjonalnej była pandemia COVID-19⁴⁶¹. Z dnia na dzień wiele urzędów i organizacji musiało przejść na tryb pracy zdalnej i jednocześnie sprostać nowym zadaniom (np. wdrażanie obostrzeń sanitarnych, organizacja wsparcia medycznego). Jak odnotował Europejski Trybunał Obrachunkowy, zdolność administracji publicznej do nieprzerwanego funkcjonowania w kryzysie okazała się krytyczna – warunkowała ona możliwość podjęcia przez rządy skutecznych działań ratunkowych⁴⁶². Wysiłkiem instytucji UE było m.in. szybkie wdrożenie pracy zdalnej, zapewnienie bezpieczeństwa cyfrowego i nowych procedur decyzyjnych, tak, aby utrzymać ciągłość procesów nawet przy zamkniętych budynkach i rozproszonym personelu. Wnioski z tego okresu wskazują, że elastyczność organizacyjna, cyfryzacja usług oraz posiadanie kultur ciągłości działania są kluczowe dla odporności instytucji⁴⁶³.

W warunkach polskich również dostrzeżono konieczność wzmocnienia odporności administracji i służb. Przykładem takiego podejścia jest powiązanie planów ciągłości działania (BCP) z planami zarządzania kryzysowego opracowywanymi na poziomie lokalnym. Dzięki temu każda gmina czy powiat ma z wyprzedzeniem opracowane scenariusze postępowania, zabezpieczone zasoby oraz jasno określone kompetencje i procedury na czas sytuacji nadzwyczajnych. Struktura systemu zarządzania kryzysowego w Polsce, z podziałem na poziom centralny (Rządowe Centrum Bezpieczeństwa, Rządowy Zespół Zarządzania Kryzysowego) i terenowy (wojewódzkie, powiatowe i gminne centra zarządzania kryzysowego), zakłada ścisłą współpracę wielu instytucji dla osiągnięcia wspólnego celu. Ważne jest przy tym zachowanie zasady subsydiarności – działania podejmowane są na najniższym szczeblu możliwym, blisko obywateli, co zwiększa szybkość i trafność reakcji. Odporność instytucjonalna opiera się również na kapitale ludzkim i kulturze organizacyjnej wewnątrz instytucji. Jeśli pracownicy są

⁴⁶¹ B. Sawczuk-Golaszewska, M. Chodyka, T. Grudniewski, Z. Ciekanowski, Bezpieczeństwo placówek edukacyjnych szkolnictwa średniego w czasie pandemii COVID-19, Warszawa, Menedżerska Akademia Nauk Stosowanych w Warszawie (Wydawnictwo im. Prof. Leszka J. Krzyżanowskiego), 2024.

⁴⁶² Europejski Trybunał Obrachunkowy, Instytucje UE a pandemia COVID-19. Reakcja była szybka, ale wciąż istnieją wyzwania, jak w optymalny sposób wykorzystać innowacje i elastyczność będące wynikiem kryzysu, Sprawozdanie specjalne nr 18/2022, Luksemburg, 2022. <https://doi.org/10.2865/116653>

⁴⁶³ Tamże.

dobrze wyszkoleni, świadomi procedur kryzysowych i potrafią improwizować w niespotykanych sytuacjach – organizacja łatwiej przetrwa trudny czas. Liderzy instytucji odgrywają tu rolę kluczową: ich zdecydowanie, zdolność komunikacji i współpracy z innymi podmiotami mogą przesądzić o powodzeniu działań ratunkowych. Dlatego coraz częściej kładzie się nacisk na rozwój kultury bezpieczeństwa wewnątrz organizacji – regularne ćwiczenia sztabowe, szkolenia kryzysowe dla kadry kierowniczej, tworzenie zespołów zarządzania kryzysowego w firmach i urzędach. Istotnym aspektem odporności instytucji jest także zaufanie społeczne do instytucji. Jeżeli obywatele ufają władzom i służbom, są bardziej skłonni stosować się do ich zaleceń w sytuacji zagrożenia (np. do ewakuacji czy szczepień), co usprawnia wspólną reakcję. Zaufanie buduje się latami poprzez skuteczność i transparentność działań. Każdy kryzys jest weryfikacją: sprawnie działające instytucje umacniają swoją wiarygodność, natomiast opieszałość lub chaos mogą zaufanie podważyć. W polskim społeczeństwie ogólny poziom zaufania do instytucji i innych ludzi jest historycznie niski – co stanowi wyzwanie dla budowania odporności społecznej. W tabeli 5 zaprezentowano odsetek osób deklarujących ogólne zaufanie do innych ludzi w poszczególnych krajach.

Tabela 5. Klasyfikacja państw według poziomu analizowanego wskaźnika

Poziom wskaźnika	Zakres	Państwa
Bardzo wysoki	45% i więcej	Chiny (56%), Indie (56%), Niderlandy (48%), Arabia Saudyjska (48%), Szwecja (47%)
Wysoki	35-44%	Australia (41%), Wielka Brytania (43%), Włochy (39%), Irlandia (38%), Szwajcaria (35%)
Średni	25-34%	Kanada (33%), Stany Zjednoczone (33%), Niemcy (33%), Hiszpania (27%), Argentyna (25%), Belgia (25%)
Niski	15-24%	Rosja (24%), Meksyk (23%), Korea Południowa (23%), Kolumbia (22%), Japonia (21%), Chile (20%), Francja (20%), Węgry (19%), Peru (17%), Polska (16%), Republika Południowej Afryki (16%)
Bardzo niski	poniżej 15%	Turcja (14%), Maledzja (13%), Brazylia (11%)

Źródło: opracowanie własne na podstawie: Ipsos, Zaufanie do ludzi w Polsce i na świecie, Ipsos Global Advisor, 2022, <https://www.ipsos.com/pl-pl/zaufanie-do-ludzi-w-polsce-i-na-swiecie>, [dostęp: 10.10.2025].

Dane wskazują, że Polska lokuje się w grupie państw o najniższym poziomie zaufania społecznego, z wynikiem 16% odpowiedzi potwierdzających przekonanie, że większości ludzi można ufać. Niski kapitał zaufania społecznego może utrudniać reakcję kryzysową – społeczeństwo mniej ufające sobie i władzom gorzej się mobilizuje i częściej ulega panice⁴⁶⁴. Dlatego w budowaniu odporności ważne jest, aby instytucje podejmowały działania uwzględniające dialog i partycypację obywateli, co zwiększa poczucie współodpowiedzialności i zaufania. Przykładem może być angażowanie mieszkańców w opracowanie lokalnych planów zarządzania ryzykiem czy wspólne ćwiczenia ewakuacyjne – takie inicjatywy nie tylko poprawiają przygotowanie merytoryczne, ale również zacieśniają więź między społecznością a władzami lokalnymi. Podsumowując, odporność instytucji państwa i samorządu jest warunkiem skutecznej ochrony ludności, a jej wzmocnienie przekłada się zarówno na lepsze wyniki operacyjne w kryzysie, jak i na większe zaufanie społeczne, które samo w sobie jest czynnikiem zwiększającym odporność całego systemu.

Najbardziej złożonym, a zarazem fundamentalnym filarem jest odporność społeczna, odnosząca się do zdolności całych grup społecznych i wspólnot (od poziomu lokalnego po społeczeństwo narodowe) do radzenia sobie z kryzysami. Społeczna odporność wynika z cech i zasobów tkwiących w ludziach oraz relacjach między nimi – określa ją m.in. poziom wiedzy i świadomości zagrożeń, umiejętności praktyczne mieszkańców, stopień zintegrowania społeczności, normy wzajemnej pomocy, a także kultura zachowań w obliczu niebezpieczeństwa. Można wyróżnić tu kilka warstw: indywidualną (odporność jednostki), rodzinną i lokalnej społeczności oraz ogólnospołeczną (narodową). Jarosław Goraj obrazowo opisuje te trzy poziomy:

- jednostka – obywatel przygotowany, posiadający np. apteczkę, wiedzę o pierwszej pomocy i procedurach alarmowych,
- rodzina i sąsiedztwo – sieć wsparcia sąsiedzkiego, opieka nad słabszymi, dzielenie się informacją i zasobami,

⁴⁶⁴ D. P. Aldrich, *Building Resilience: Social Capital in Post-Disaster Recovery*, Chicago, University of Chicago Press, 2012. <https://doi.org/10.7208/chicago/9780226012896.001.0001>

- instytucje lokalne i państwowe – plany awaryjne, ćwiczenia, skuteczna komunikacja z ludnością⁴⁶⁵.

Wszystkie te poziomy muszą ze sobą współgrać, by społeczność jako całość była odporna. Kapitał społeczny – czyli sieci relacji, zaufanie i normy wzajemności – odgrywa tu kluczową rolę. Badania nad klęskami żywiołowymi dowodzą, że społeczności o silnych więzach wewnętrznych lepiej radzą sobie z katastrofami i szybciej wracają do równowagi. Daniel P. Aldrich wykazał, że to właśnie siła więzi międzyludzkich i zaangażowanie obywatelskie często stanowią czynnik decydujący o tempie odbudowy po kataklizmie – ważniejszy nieraz niż pomoc materialna z zewnątrz⁴⁶⁶. Dobre relacje sąsiedzkie sprawiają, że ludzie pomagają sobie nawzajem jeszcze zanim nadejdzie formalna pomoc państwowa. W polskich realiach widzieliśmy tego przykłady: podczas powodzi tysiąclecia 1997 r. czy powodzi 2010 r. mieszkańcy zagrożonych terenów spontanicznie organizowali akcje ratunkowe i zabezpieczali wały, w pierwszych miesiącach pandemii COVID-19 setki oddolnych inicjatyw (szycie maseczek, dostarczanie zakupów osobom starszym) uzupełniały działania rządowe, po wybuchu wojny na Ukrainie w 2022 r. społeczeństwo masowo zaangażowało się w pomoc uchodźcom, zapewniając schronienie i wsparcie. Te przykłady pokazują ogromny potencjał solidarności drzemący w polskim społeczeństwie. Jednocześnie jednak, jak zauważa Goraj, spontaniczne zrywy obywatelskie bywają niekoordinowane i krótkotrwałe⁴⁶⁷. Wyzwanie polega na tym, by przełożyć tę spontaniczną solidarność na trwałą zdolność – zorganizowaną, przemyślaną i podpartą wiedzą.

Kluczowym czynnikiem ograniczającym odporność społeczną jest brak wiedzy i przygotowania przeciętnego obywatela. Niestety, wciąż wielu ludzi nie zna podstawowych procedur bezpieczeństwa ani nie posiada planu działania na wypadek nagłego zagrożenia. Eksperci wskazują na poważne

⁴⁶⁵ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 10.10.2025].

⁴⁶⁶ D. P. Aldrich, *Building Resilience: Social Capital in Post-Disaster Recovery*, Chicago, University of Chicago Press, 2012. <https://doi.org/10.7208/chicago/9780226012896.001.0001>

⁴⁶⁷ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 10.10.2025].

luki w edukacji powszechnej w zakresie bezpieczeństwa. W Polsce po zakończeniu zimnej wojny zaniedbano edukację obronną – obecne pokolenie dorosłych nie przechodziło przeszkolenia OC, a edukacja dla bezpieczeństwa w szkołach bywa traktowana marginalnie. W rezultacie większość rodzin nie ma przygotowanego domowego planu awaryjnego (np. gdzie się spotkać w razie ewakuacji, jakie zapasy zgromadzić), nigdy nie uczestniczyła w żadnych ćwiczeniach kryzysowych, a w domu nie posiada nawet podstawowego zestawu przetrwania na 72 godziny (latarki, radio na baterie, woda, żywność długoterminowa itp.). Taki stan rzeczy oznacza, że w momencie kryzysu ludzie reagują chaotycznie, często popadając w panikę lub czekając bezradnie na pomoc z zewnątrz. Tymczasem im bardziej świadomy i samodzielny jest obywatel, tym skuteczniej cała społeczność przetrwa kryzys – dobrze przygotowani ludzie odciążają służby, które mogą skupić się na najcięższych przypadkach.

Kultura bezpieczeństwa społeczeństwa – rozumiana jako zbiór wartości, nawyków i postaw sprzyjających bezpiecznym zachowaniom – bezpośrednio przekłada się na odporność. Wojakowska i Gikiewicz podkreślają, że wysoki poziom kultury bezpieczeństwa jednostek i lokalnych wspólnot skutkuje większym bezpieczeństwem zbiorowym i narodowym. Jeśli od najmłodszych lat ludzie uczą się dbać o bezpieczeństwo (w domu, w szkole, w miejscu pracy), traktują je jako wspólną wartość i obowiązek, wówczas w obliczu zagrożenia reagują bardziej racjonalnie i solidarnie. Kultura bezpieczeństwa przejawia się np. w tym, że mieszkańcy znają sygnały alarmowe i wiedzą, jak się zachować po ich usłyszeniu, że w społeczności istnieje nawyk przygotowywania awaryjnych zapasów, że regularnie odbywają się lokalne ćwiczenia ratownicze z udziałem społeczności, że posiadanie gaśnicy czy apteczki jest standardem, a nie wyjątkiem. Wszystko to buduje świadomość ryzyka i zmniejsza podatność na panikę. Odporne społeczności, zdaniem Wojakowskiej i Gikiewicz, szybciej rozpoznają symptomy zagrożeń i sprawniej podejmują reakcję, wykazując wysoką gotowość adaptacyjną. W praktyce oznacza to np., że gdy nadchodzi huragan, ludzie wcześniej zabezpieczają dobytek i ostrzegają sąsiadów, zamiast bagatelizować sygnały, albo że w razie ewakuacji mieszkańcy wiedzą, dokąd się udać i co ze sobą zabrać, co usprawnia przebieg akcji.

Aby zwiększyć odporność społeczności, konieczne są celowe działania wzmacniające powyższe czynniki – przede wszystkim edukacja, budowanie kultury bezpieczeństwa oraz włączanie obywateli we współtworzenie systemu bezpieczeństwa (partycypacja). Eksperci zgodnie twierdzą, że budowanie odporności to proces długofalowy, wymagający inwestycji w świadomość społeczną. Poniżej zestawiono główne obszary takich działań wraz z przykładowymi inicjatywami:

1. Powszechna edukacja dla bezpieczeństwa – Wprowadzenie od najmłodszych lat programów edukacyjnych uczących praktycznych umiejętności radzenia sobie w sytuacjach kryzysowych. W szkołach powinny odbywać się obowiązkowe zajęcia z pierwszej pomocy, zasad ewakuacji, zachowania podczas pożaru, powodzi czy innego zagrożenia. Edukacja nie powinna ograniczać się do teorii – kluczowe są elementy praktyczne, ćwiczenia i drille. Również na poziomie osiedli czy zakładów pracy warto organizować szkolenia z zakresu bezpieczeństwa (np. obsługa gaśnic, udzielanie pomocy przedmedycznej). Wiedza i nawyki wyniesione z takich szkoleń pozostają z ludźmi na całe życie, zwiększając ich samodzielność w obliczu zagrożeń.
2. Kampanie społeczne i informacyjne – Budowanie kultury bezpieczeństwa wymaga dotarcia do szerokiego grona obywateli poprzez media i akcje informacyjne. Proste komunikaty – np. co powinno znaleźć się w domowej apteczce i „plecaku ewakuacyjnym”, jak przygotować zapas wody i jedzenia na 3 dni, jak zabezpieczyć mieszkanie przed wichurą – mogą znacząco podnieść poziom przygotowania rodzin⁴⁶⁸. Ważnym narzędziem są tu kampanie prowadzone przez służby (np. poradniki Rządowego Centrum Bezpieczeństwa), organizacje pozarządowe, a także lokalne inicjatywy (ulotki, spotkania informacyjne w gminach). W erze mediów społecznościowych przekaz można kierować precyzyjnie – np. zachęcać mieszkańców zagrożonych regionów do instalacji aplikacji alarmowych, informować rolników

⁴⁶⁸ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 10.10.2025].

- o zagrożeniach suszą itd. Celem jest zmiana mentalności: przekonanie ludzi, że przygotowanie się na kryzys jest normą, a nie przesadą.
3. Ćwiczenia i treningi lokalne – Same instrukcje to za mało – konieczne jest praktyczne przećwiczenie procedur z udziałem społeczności. Lokalne władze powinny regularnie (np. raz do roku) organizować treningi kryzysowe: symulacje ewakuacji szkoły, alarmu powodziowego, akcji poszukiwawczej, działania po blackoucie itp. Zaangażowanie mieszkańców w takie ćwiczenia daje im bezcenne doświadczenie – w momencie prawdziwego zagrożenia będą wiedzieć, jak się zachować. Dla władz to z kolei okazja do sprawdzenia planów w praktyce i ulepszenia ich na podstawie wniosków. Niestety, jak dotąd większość Polaków nigdy nie uczestniczyła w żadnych ćwiczeniach związanych z reagowaniem na zagrożenia. Zmiana tego stanu rzeczy powinna stać się priorytetem polityki lokalnej i centralnej.
 4. Wspieranie organizacji społecznych i wolontariatu – Bardzo ważnym ogniwem są organizacje pozarządowe oraz oddolne inicjatywy obywatelskie działające w obszarze bezpieczeństwa. Ochotnicze Straże Pożarne (OSP), grupy ratownictwa, harcerze, stowarzyszenia obrony cywilnej – wszystkie one mobilizują zasoby społeczności i podnoszą jej odporność. Należy je włączać w oficjalne struktury planowania kryzysowego, szkolić i dofinansowywać. Na przykład OSP w wielu wsiach stanowią pierwszą linię reagowania przy pożarach czy powodziach – ich dobra współpraca z PSP i samorządem jest bezcenna. W miastach można tworzyć zespoły pierwszej pomocy złożone z przeszkolonych wolontariuszy. Państwo powinno doceniać i promować takie inicjatywy, bo każdy przygotowany obywatel to mniejsze obciążenie dla służb w kryzysie.
 5. Budowanie zaufania i włączanie obywateli w system – Partycypacja to nie tylko uczestnictwo w ćwiczeniach, ale też realny wpływ mieszkańców na kwestie bezpieczeństwa. Ustawa przewiduje rozwój edukacji z zakresu ochrony ludności i obrony cywilnej w systemie oświaty oraz w formach pozaszkolnych organizowanych przez organy ochrony ludności, a także większe włączenie organizacji społecznych w realizację zadań na rzecz bezpieczeństwa. To podejście traktuje bezpieczeństwo

jako obowiązek wspólny, a nie wyłączną domenę państwa. Włączenie obywateli w planowanie (np. konsultacje planów zagospodarowania pod kątem zagrożeń), w proces decyzyjny (rady bezpieczeństwa przy samorządach) i w działania (programy typu Community Watch, lokalne systemy wczesnego ostrzegania) przekłada się na większą świadomość i odpowiedzialność społeczności za własne bezpieczeństwo. W rezultacie, w chwili próby ludzie nie są biernymi ofiarami oczekującymi wyłącznie na pomoc z zewnątrz, lecz aktywnymi uczestnikami reagowania kryzysowego.

Spółeczna odporność jest pochodną wielu czynników: wiedzy, więzi, zaufania, organizacji i kultury. Jej wzmocnienie wymaga konsekwentnej polityki – edukacyjnej, informacyjnej i integracyjnej. Społeczeństwo świadome zagrożeń i przygotowane do działania jest jak dobrze naoliwiony mechanizm: w obliczu kryzysu reaguje spokojniej, rozsądniej i skuteczniej. Jak trafnie ujęto to w analizie Stowarzyszenia Świadoma Obrona Cywilna, „społeczna odporność to najtańsza i najskuteczniejsza inwestycja w bezpieczeństwo państwa”, budowana z tysięcy małych cegiełek – indywidualnych kompetencji i zasobów każdego obywatela⁴⁶⁹. To właśnie z tych cegiełek powstaje mur ochronny, który może uchronić społeczeństwo przed skutkami przyszłych katastrof i wstrząsów.

6.3. Innowacje technologiczne w zarządzaniu kryzysowym

Współczesne zarządzanie kryzysowe coraz częściej sięga po najnowsze zdobycze technologii – sztuczną inteligencję (AI – Artificial Intelligence), Internet Rzeczy (IoT – Internet of Things) oraz analitykę dużych zbiorów danych (Big Data) – w celu poprawy efektywności reagowania na zagrożenia. Technologie te umożliwiają wcześniejsze prognozowanie i wykrywanie potencjalnych kryzysów, wszechstronną analizę scenariuszy rozwoju sytuacji

⁴⁶⁹ J. Goraj, Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, Stowarzyszenie Świadoma Obrona Cywilna, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 10.10.2025].

oraz optymalizację wykorzystania zasobów podczas reagowania na sytuacje nadzwyczajne. Jak wskazują badania, zastosowanie AI, IoT i analizy Big Data może znacząco usprawnić procesy decyzyjne i działania operacyjne służb kryzysowych. Poniżej omówiono rolę tych innowacji – ich możliwości zastosowań w zarządzaniu kryzysowym, a także związane z nimi wyzwania i ryzyka.

Sztuczna inteligencja (AI) znajduje coraz szersze zastosowanie w zarządzaniu kryzysowym, oferując narzędzia do zaawansowanej analizy danych i wspomagania decyzji. Dzięki algorytmom uczenia maszynowego możliwe jest automatyczne przetwarzanie ogromnych zbiorów informacji w celu wykrywania trendów i zależności, których człowiek nie byłby w stanie szybko zauważyć. AI potrafi wspierać prognozowanie zagrożeń – na przykład modele oparte na sieciach neuronowych mogą przewidywać prawdopodobieństwo wystąpienia klęsk żywiołowych na podstawie danych historycznych i bieżących (np. pogodowych czy sejsmicznych). Coraz częściej podkreśla się również zdolność AI do symulowania i analizowania różnych scenariuszy kryzysowych. Symulacje komputerowe pozwalają na modelowanie przebiegu zdarzeń w hipotetycznych sytuacjach awaryjnych, co wspiera planowanie awaryjne i trening służb. Przykładowo, dzięki sztucznej inteligencji można opracować najlepszy scenariusz działań ratunkowych dla nadchodzącej katastrofy, uwzględniający optymalną ewakuację ludności oraz rozlokowanie sił i środków. AI znacząco usprawnia także optymalizację alokacji zasobów w trakcie kryzysu. Algorytmy inteligentnego wspomagania decyzji są zdolne do proponowania najbardziej efektywnego rozdziału dostępnych jednostek ratowniczych, sprzętu i zaopatrzenia tam, gdzie są najbardziej potrzebne. Systemy oparte na AI mogą automatycznie wyznaczać trasy zaopatrzenia omijające zagrożone obszary oraz wskazywać, które lokalizacje powinny otrzymać pomoc w pierwszej kolejności. Sztuczna inteligencja wspiera również monitorowanie zagrożeń w czasie rzeczywistym – analizując strumienie danych z czujników, kamer czy mediów społecznościowych potrafi wychwycić anomalie mogące świadczyć o początku kryzysu (np. nagły wzrost stężenia dymu sugerujący pożar lub wzmożone dyskusje o objawach choroby mogące wskazywać na wybuch epidemii). Co więcej, AI przyczynia się do zwalczania dezinformacji w trakcie sytuacji kryzysowych: narzędzia analizy języka naturalnego mogą filtrować nieprawdziwe

informacje pojawiające się w Internecie i kontrolować plotki, dostarczając społeczeństwu rzetelnych komunikatów.

W literaturze podkreśla się szeroki wachlarz korzyści z zastosowania AI w całym cyklu zarządzania kryzysowego⁴⁷⁰. Należą do nich m.in. ulepszone systemy wczesnego ostrzegania, dzięki którym możliwe jest wcześniejsze alarmowanie o nadchodzących zagrożeniach, oraz automatyzacja powtarzalnych procesów, od inteligentnego alarmowania, przez rozpoznawanie mowy i automatyczną transkrypcję zgłoszeń alarmowych, po analizę obrazów satelitarnych czy zdjęć z dronów w celu oceny szkód. Sztuczna inteligencja ułatwia również komunikację i koordynację – platformy współpracy oparte na AI integrują wielu interesariuszy (służby ratownicze, administrację, organizacje pozarządowe, obywateli), umożliwiając im dzielenie się informacjami o potrzebach w czasie rzeczywistym oraz lepsze dopasowanie pomocy do sytuacji. Wszystko to przekłada się na szybsze i trafniejsze decyzje podejmowane pod presją czasu. Warto zauważyć, że również w Polsce prowadzone są badania nad zastosowaniem AI w zarządzaniu kryzysowym. Przykładem jest przegląd systematyczny K. Sienkiewicz-Małyjurek, który potwierdził rosnące zainteresowanie tą tematyką i zidentyfikował kluczowe obszary badań, m.in. wykorzystanie AI do analizy dużych zbiorów danych, predykcji zagrożeń czy wspomagania procesu decyzyjnego⁴⁷¹. Już teraz istnieją wdrożenia elementów AI w praktyce – np. podczas pandemii COVID-19 wykorzystano algorytmy uczenia maszynowego do prognozowania przebiegu pandemii, analiz skupisk zachorowań oraz dystrybucji zasobów medycznych. Te doświadczenia pokazują potencjał sztucznej inteligencji w radzeniu sobie ze złożonością współczesnych zagrożeń.

Internet Rzeczy (IoT), rozumiany jako sieć powiązanych ze sobą urządzeń i sensorów komunikujących się w czasie rzeczywistym, odgrywa coraz większą rolę w systemach bezpieczeństwa i reagowania kryzysowego. W miastach powstają rozwiązania typu smart city, w których tysiące czujników monitorują otoczenie – od jakości powietrza i poziomu wód, przez obciążenie konstrukcji budynków, po natężenie ruchu ulicznego – dostarczając ciągłego strumienia danych do centrów zarządzania kryzysowego.

⁴⁷⁰ T. Wiktorowski, Systemy ostrzegania i informowania ludności jako narzędzie zwiększania odporności społecznej, Bezpieczeństwo. Teoria i Praktyka, 2024.

⁴⁷¹ K. Sienkiewicz-Małyjurek, Skuteczne zarządzanie kryzysowe, Warszawa, Difin, 2015.

Inteligentne sensory rozmieszczone w środowisku umożliwiają bieżący monitoring zagrożeń i szybkie wykrywanie anomalii mogących świadczyć o nadchodzącym kryzysie. Przykładowo, sieć czujników poziomu wody na rzekach (połączona poprzez IoT) może wcześniej ostrzegać przed powodzią, gdy tylko odnotuje nietypowy przyrost stanu wód. Podobnie czujniki sejsmiczne włączone do Internetu mogą natychmiast alarmować o wstrząsach, co skraca czas reakcji przed nadejściem fal sejsmicznych. Z kolei w miastach czujniki jakości powietrza informują o zagrożeniach smogowych lub chemicznych, a systemy inteligentnego transportu na bieżąco zarządzają ruchem drogowym, ułatwiając przejazd pojazdów uprzywilejowanych w sytuacji alarmowej. IoT służy nie tylko detekcji zagrożeń, ale również usprawnieniu komunikacji i koordynacji działań ratunkowych. Urządzenia IoT mogą automatycznie powiadamiać odpowiednie służby, gdy zdarzy się wypadek – na przykład inteligentny czujnik dymu w budynku może wysłać sygnał do straży pożarnej, zanim ktokolwiek zadzwoni pod numer alarmowy. Inteligentne miasta integrują infrastrukturę krytyczną (sieci energetyczne, wodociągi, transport) z systemami IoT, co zapewnia ciągłość informacji o ich stanie. Dzięki temu zarządzanie kryzysowe dysponuje aktualnym obrazem sytuacji. Badania wskazują, że IoT staje się efektywną platformą integrującą usługi informacyjne dla potrzeb bezpieczeństwa – umożliwia ciągle zbieranie, aktualizowanie i udostępnianie danych w dynamicznie zmieniającym się środowisku⁴⁷². Szczególnego znaczenia nabiera tu monitorowanie środowiska pod kątem wystąpienia katastrof naturalnych i nietypowych zjawisk. Ogórek i Zaskórski podkreślają, że skuteczne monitorowanie takich zagrożeń (np. powodzi, suszy, pożarów, ale także nagłych zdarzeń społecznych) jest kluczowe dla sprawnego systemu reagowania. IoT dostarcza narzędzi do realizacji tego zadania – rozległe sieci czujników środowiskowych mogą śledzić parametry klimatyczne, hydrologiczne czy chemiczne niemal w czasie rzeczywistym. Platformy IoT ułatwiają również efektywne wykorzystanie sił i środków ratunkowych. Informacje zbierane przez sensory – np. o stanie dróg, natężeniu ruchu czy dostępności sprzętu – mogą być automatycznie analizowane w celu optymalizacji działań służb. Dzięki

⁴⁷² M. Ogórek, P. Zaskórski, Internet rzeczy w integracji procesów zarządzania kryzysowego, Zeszyty Naukowe Politechniki Poznańskiej. Organizacja i Zarządzanie, 76, 2018. <https://doi.org/10.21008/j.0239-9415.2018.076.15>

temu możliwe jest przyspieszenie akcji ratowniczych i usprawnienie procedur poprzez lepszą synchronizację różnych podsystemów (synergia m.in. systemów łączności, logistyki, monitoringu). Na przykład lokalizatory GPS w pojazdach ratowniczych (element IoT) pozwalają centrum dowodzenia na bieżąco śledzić położenie jednostek i kierować je tam, gdzie są najbardziej potrzebne. Równocześnie czujniki w infrastrukturze (mostach, tunelach, budynkach) informują o jej ewentualnych uszkodzeniach, co pomaga zdecydować o trasach dojazdu czy ewakuacji. W ten sposób Internet Rzeczy wspomaga optymalizację zasobów w kryzysie – zapewniając dokładne dane, pozwala podejmować trafniejsze decyzje dotyczące rozmieszczenia ludzi i sprzętu. Warto podkreślić rolę IoT w monitorowaniu infrastruktury krytycznej oraz środowiska miejskiego. Inteligentne sieci sensorów czuwają nad bezpieczeństwem obiektów takich jak systemy zaopatrzenia w wodę, sieci energetyczne, transport publiczny – wykrywając awarie, przerwy w działaniu czy próby sabotowania tych systemów. Jednocześnie monitorują parametry środowiskowe (np. poziom zanieczyszczeń powietrza, jakość wody) zarówno w miastach, jak i na obszarach wiejskich, co ma znaczenie np. przy zagrożeniach epidemiologicznych. Wszystkie te dane mogą zasilać hurtownie informacji kryzysowych, będące częścią infrastruktury Big Data. Jest to istotne, bo integracja danych z IoT z systemami analitycznymi (GIS, systemy informacji przestrzennej, platformy Big Data) umożliwia tworzenie kompleksowego obrazu sytuacji kryzysowej w skali kraju lub regionu. Na poziomie krajowym trwają prace nad coraz lepszym wykorzystaniem IoT w zarządzaniu kryzysowym. Wdrożono np. ogólnokrajowy System Alertu RCB, który wykorzystuje sieci telekomunikacyjne – SMS w telefonach komórkowych do masowego powiadamiania ludności o nadciągających zagrożeniach. Choć nie jest to klasyczny IoT, pokazuje trend ku automatyzacji powiadomień. W przyszłości można spodziewać się szerszego zastosowania IoT w polskich miastach – od inteligentnych systemów sterowania ruchem ulicznym ułatwiających przejazd służb ratowniczych po zaawansowane systemy monitoringu środowiska (np. sieć czujników Państwowej Straży Pożarnej do wykrywania pożarów lasów). Ciągły rozwój Internetu Rzeczy daje duże możliwości w poprawie bezpieczeństwa – sprawnie funkcjonujące systemy zarządzania kryzysowego z wykorzystaniem IoT mogą wcześniej

wykrywać symptomy zagrożeń, minimalizować ryzyko, a w razie wystąpienia kryzysu skuteczniej go opanować.

Big Data odnosi się do technik gromadzenia i analizowania ogromnych zbiorów danych – zarówno ustrukturyzowanych, jak i nieustrukturyzowanych – pochodzących z wielu źródeł. W kontekście zarządzania kryzysowego Big Data odgrywa kluczową rolę, ponieważ sytuacje nadzwyczajne generują ogromne ilości danych, które odpowiednio wykorzystane mogą znacząco usprawnić reagowanie. Analiza big data pozwala na monitorowanie sytuacji w czasie rzeczywistym oraz na predykcję rozwoju kryzysu, co przekłada się na szybsze i trafniejsze decyzje decydentów. Dzięki zaawansowanym algorytmom analitycznym możliwe jest natychmiastowe wykrywanie sygnałów ostrzegawczych: systemy big data mogą np. na bieżąco analizować tysiące komunikatów (zgłoszeń 112, wpisów w mediach społecznościowych, odczytów sensorów IoT) i wyłuskiwać z nich informacje wskazujące na zagrożenie. Źródła danych wykorzystywane w Big Data dla kryzysów są bardzo różnorodne. Należą do nich m.in. dane meteorologiczne (np. radarowe obrazy opadów, modele pogodowe), pozwalające przewidywać warunki atmosferyczne i potencjalne ekstremalne zjawiska (burze, huragany, susze). Ważnym źródłem są media społecznościowe, które stanowią dziś niezastąpione źródło informacji w czasie rzeczywistym, dostarczając bezpośrednich relacji świadków zdarzeń oraz umożliwiając monitorowanie nastrojów społecznych. Użytkownicy platform takich jak X czy Facebook pełnią rolę społecznych sensorów – publikując informacje o tym, co dzieje się wokół nich, często szybciej niż oficjalne kanały są w stanie zareagować. Analiza tych danych (tzw. social media mining) pozwala służbom na uzyskanie wiedzy o skali zjawiska, lokalizacji poszkodowanych czy pilnych potrzebach ludności⁴⁷³. Przykładowo, podczas powodzi czy nawałnych opadów, analiza geolokalizowanych postów na X może wskazać dzielnice najbardziej dotknięte zalaniem, co pomaga skierować tam pomoc. W ten sposób media społecznościowe stają się cennym narzędziem w zarządzaniu kryzysowym, wspierając procesy decyzyjne i alokację zasobów poprzez dostarczanie

⁴⁷³ M. Chodyka, Z. Ciekankowski, Analiza treści audiowizualnych jako element systemów bezpieczeństwa państwa, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2024.

aktualnych informacji zwrotnych od społeczeństwa⁴⁷⁴. Inne istotne strumienie danych big data to m.in. dane geolokalizacyjne z urządzeń mobilnych i GPS, które umożliwiają śledzenie przemieszczania się ludności w trakcie kryzysu. Operatorzy sieci komórkowych mogą anonimizować i udostępniać zbiorcze informacje o zagęszczeniu telefonów w danym obszarze, co pomaga oszacować liczbę osób wymagających ewakuacji lub ocenić, czy ludność stosuje się do zaleceń (np. strefy zamknięte). Również obrazy satelitarne i dane teledetekcyjne (np. zdjęcia z radarów SAR) to element Big Data – ich analiza (często z pomocą AI) pozwala ocenić zniszczenia po katastrofie (areę zalania, zasięg pożaru) niemal w czasie rzeczywistym. Wszystkie te dane z różnych źródeł są integrowane w ramach zaawansowanych systemów, często z wykorzystaniem technologii GIS do wizualizacji. Dzięki temu zarządzający kryzysem mają do dyspozycji kompleksowy obraz sytuacji przedstawiony na mapach cyfrowych (np. lokalizacja zdarzeń, rozkład dostępnych zasobów ratunkowych, zamknięte drogi). Analizy Big Data odgrywają również kluczową rolę w predykcji i modelowaniu przebiegu kryzysu. Analityka predykcyjna korzysta z historycznych danych o wcześniejszych zdarzeniach (np. baz danych o trzęsieniach ziemi, trajektoriach huraganów, statystykach awarii infrastruktury) aby prognozować przyszłe zdarzenia lub ich skutki. Na przykład modele big data mogą oszacować, jakie obszary miasta zostaną najbardziej dotknięte przez powódź na podstawie prognoz pogody i danych topograficznych – co daje czas na wzmocnienie wałów czy ewakuację mieszkańców z tych miejsc. Innym przykładem jest wykorzystanie Big Data do optymalizacji reakcji służb ratunkowych: łącząc dane z wielu źródeł (social media, sensory środowiskowe, obrazy z dronów), można szybko zidentyfikować najbardziej poszkodowane obszary i przewidzieć, gdzie braki w zasobach mogą być największe. Algorytmy mogą zasugerować rozmieszczenie punktów medycznych lub źródeł zaopatrzenia tak, aby maksymalnie skrócić czas dotarcia pomocy. Przykłady praktyczne zastosowania Big Data w zarządzaniu kryzysowym już istnieją. W skali globalnej m.in. analiza ruchu telefonii komórkowej była wykorzystywana podczas epidemii eboli w Afryce do śledzenia przemieszczania się ludności i przewidywania

⁴⁷⁴ H. Marjak, Potencjał i rola mediów społecznościowych w zarządzaniu kryzysowym, *Zeszyty Naukowe Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej*, 2, 2019.

dróg rozprzestrzeniania choroby. Również platformy analityczne korzystające z big data wspierały koordynację pomocy podczas katastrofy po trzęsieniu ziemi na Haiti (2010 r.) czy huraganu Sandy (2012 r.) – agregując informacje od wolontariuszy, organizacji i obywateli w czasie rzeczywistym. W Polsce koncepcja Big Data w sytuacjach kryzysowych dopiero zyskuje na znaczeniu, ale pojawiają się inicjatywy w tym zakresie. Przykładowo, Analiza Ruchu Big Data oferowana przez jednego z operatorów telekomunikacyjnych pozwala samorządom monitorować masowe imprezy i zgromadzenia pod kątem bezpieczeństwa (liczebność tłumu, kierunki przemieszczania się), co może być wykorzystane w planowaniu zabezpieczenia takich wydarzeń. Jest prawdopodobne, że w najbliższych latach również centra zarządzania kryzysowego w Polsce wdrożą dedykowane platformy Big Data integrujące dane z systemów 112, monitoringów miejskich, sensorów środowiskowych i mediów społecznościowych, aby usprawnić wymianę informacji i podejmowanie decyzji.

Choć AI, IoT i Big Data oferują ogromne możliwości usprawnienia zarządzania kryzysowego, ich wdrożenie wiąże się także z istotnymi wyzwaniami i ryzykami. Jednym z głównych problemów jest kwestia prywatności i bezpieczeństwa danych. Rozbudowane systemy IoT oraz analizy big data gromadzą wielkie ilości informacji, często o charakterze wrażliwym (np. dane o lokalizacji ludzi, ich aktywności, informacje medyczne zebrane podczas kryzysu). Należy zagwarantować, że dane te będą odpowiednio chronione przed nieuprawnionym dostępem. Niestety, obecnie nie ma pełnej gwarancji bezpieczeństwa i prywatności danych przetwarzanych przez takie systemy. Wyciek danych czy ich niewłaściwe wykorzystanie może skutkować naruszeniem prywatności poszkodowanych osób lub nawet całych społeczności. Ponadto, w dobie cyfryzacji pojawia się ryzyko cyfrowej inwigilacji – np. kamery i czujniki w przestrzeni publicznej, choć służą bezpieczeństwu, mogą budzić obawy co do nadmiernego śledzenia obywateli. Konieczne jest więc wypracowanie jasnych standardów i przepisów prawnych dotyczących wykorzystywania AI i IoT w sytuacjach nadzwyczajnych, tak, aby zrównoważyć korzyści z ochroną praw obywatelskich. Kolejnym wyzwaniem jest zależność od technologii – coraz większa integracja systemów kryzysowych z zaawansowanymi technologiami oznacza, że ewentualna awaria tych systemów może poważnie zakłócić prowadzenie akcji

ratunkowych. Nadmierna automatyzacja bez odpowiednich planów awaryjnych niesie ryzyko, że w przypadku niespodziewanego scenariusza ludzie nie będą dysponować niezbędnymi informacjami lub umiejętnościami, by przejąć kontrolę. Przykładowo, zawodność algorytmów AI w niestandardowych sytuacjach to realny problem – modele uczone na danych historycznych mogą sobie nie poradzić z zupełnie nowym typem zagrożenia, dając błędne rekomendacje. Może to prowadzić do „spirali błędnych ocen”, gdzie system podpowiada niewłaściwe działania, a decydenci zbyt ufający technologii opóźniają korektę tych decyzji. Ponadto, brak standardowych zbiorów danych do trenowania modeli AI w dziedzinie kryzysowej powoduje, że różne systemy mogą dawać rozbieżne wyniki. Zależność od technologii uwiódź się również, gdy infrastruktura krytyczna zostanie uszkodzona – np. brak zasilania, awaria sieci telekomunikacyjnych czy Internetu unieruchomi sporą część rozwiązań IoT/AI. Dlatego ważne jest zachowanie równowagi między automatyzacją a utrzymaniem zdolności do ręcznego, analogowego działania w sytuacjach skrajnych. Nie można też zapominać o nowych wektorach ataku związanych z tymi technologiami. Cyberbezpieczeństwo staje się nieodłącznym elementem zarządzania kryzysowego opartego na ICT. Systemy IoT mogą być narażone na ataki hakerskie – przykładowo włamanie do sieci sensorów może skutkować podaniem fałszywych odczytów (alarmowanie o zagrożeniu, którego nie ma, lub odwrotnie – ukrycie prawdziwego zagrożenia). Już teraz odnotowano incydenty, gdzie złośliwe oprogramowanie (malware) infekowało urządzenia IoT, tworząc tzw. botnety, które mogą zakłócić działanie sieci (np. atak Mirai). W kontekście kryzysowym taki atak mógłby sparaliżować system łączności lub dezinformować służby. Algorytmy AI również mogą być podatne na manipulacje – istnieje ryzyko tzw. ataków adversarialnych, gdy poprzez drobne zmiany w danych wejściowych można spowodować błędną ocenę sytuacji przez model AI. Na przykład fałszywe informacje masowo rozpowszechnione w mediach społecznościowych (boty internetowe) mogą wprowadzić w błąd systemy analityczne śledzące nastroje społeczne. Ekspert ostrzegają, że obecnie poziom podatności nowoczesnych systemów na cyberzagrożenia jest wysoki, a bezpieczeństwo tych rozwiązań nie nadąża za ich rozwojem. Stąd konieczne jest inwestowanie w zabezpieczenia (szyfrowanie komunikacji, autoryzacja dostępu do urządzeń, monitorowanie anomalii sieciowych) równolegle

z wdrażaniem IoT i AI. Wreszcie, wprowadzenie innowacji technologicznych wymaga odpowiednich kompetencji ludzkich. Czynniki ludzkie nadal pozostaje kluczowy – nawet najlepsze systemy nie spełnią swojej roli, jeśli personel zarządzający kryzysowo nie będzie umiał z nich korzystać lub nie będzie im ufał. Niestety, badania wskazują na niedostatek wyszkolenia i opór przed nowymi technologiami wśród części pracowników służb kryzysowych. Pokonanie tej bariery wymaga szkoleń, ćwiczeń i budowy zaufania do systemów. Istotne jest również opracowanie jasnych procedur współdziałania ludzi i AI/IoT – np. określenie, kto podejmuje ostateczną decyzję, gdy system rekomenduje określone działanie, oraz jak weryfikować wyniki dostarczane przez algorytmy⁴⁷⁵.

Technologiczne innowacje w postaci AI, IoT i Big Data otwierają nowy rozdział w zarządzaniu kryzysowym, oferując narzędzia do lepszego przewidywania zagrożeń, skuteczniejszej koordynacji i szybszego reagowania. Doświadczenia z ostatnich lat – od wykorzystania AI w pandemii, przez projekty smart city zwiększające bezpieczeństwo, po analizy Big Data wspomagające reakcję na klęski żywiołowe – pokazują, że potencjał tych technologii jest ogromny. Jednocześnie jednak należy świadomie zarządzać towarzyszącymi im ryzykami. Zapewnienie prywatności danych, odporności systemów na awarie i ataki, dostosowanie przepisów prawnych oraz przygotowanie ludzi do współpracy z inteligentnymi systemami – to warunki konieczne, aby innowacje te rzeczywiście przełożyły się na większe bezpieczeństwo społeczeństwa. Jeśli zostaną spełnione, AI, IoT i Big Data mogą stać się filarami nowoczesnego zarządzania kryzysowego, znacznie zwiększając jego skuteczność i odporność na wyzwania przyszłości.

6.4. Edukacja, szkolenia i kultura bezpieczeństwa

Bezpieczeństwo państwa i obywateli zależy nie tylko od sprzętu i procedur, ale także od ludzi: od poziomu ich wiedzy, wyszkolenia oraz utrwalonych nawyków i postaw. Kluczową rolę odgrywa tu edukacja w zakresie bezpieczeństwa oraz kształtowanie kultury bezpieczeństwa rozumianej jako

⁴⁷⁵ J. Wołęjszo (red.), *Innowacje i nowe technologie w bezpieczeństwie*, Kalisz, Wydawnictwo Naukowe Uniwersytetu Kaliskiego, 2025.

wspólny system wartości, przekonań i zachowań sprzyjających bezpiecznym działaniom. W literaturze podkreśla się, że bezpieczeństwo to nie tylko stan, ale i proces wymagający ciągłego uczenia się i adaptacji do zmiennych zagrożeń. Jak zauważa Wiśniewska-Paź, „to właśnie w pierwszej kolejności edukacja i kształtowana na jej podstawie kultura bezpieczeństwa stanowią trzon turbiny konstruktywnych zmian w zakresie bezpieczeństwa”⁴⁷⁶. W tym ujęciu kształcenie i doskonalenie kompetencji powinno obejmować zarówno kadry administracji publicznej, służby ratownicze i porządkowe, jak i ogół społeczeństwa, aby wzmacniać spójność oraz odporność systemu bezpieczeństwa narodowego. Szczególne znaczenie mają rozwiązania systemowe w postaci szkoleń, ćwiczeń i programów kształcenia specjalistycznego (w tym studiów podyplomowych), które wspierają profesjonalizację działań oraz ujednolicenie standardów postępowania. Równolegle kluczową rolę pełni kultura bezpieczeństwa rozumiana jako „miękkie spoiwo” systemu – obejmujące utrwalone nawyki i postawy, poziom zaufania do instytucji publicznych, a także oddziaływanie edukacji formalnej i nieformalnej oraz mediów na świadomość zagrożeń i gotowość do współdziałania.

Administracja publiczna wszystkich szczebli pełni funkcje kluczowe w systemie zarządzania kryzysowego i ochrony ludności, co uzasadnia konieczność systematycznego rozwijania kompetencji jej kadr w obszarze bezpieczeństwa, planowania oraz reagowania na zdarzenia nadzwyczajne^{477,478}. Przez długi okres przygotowanie urzędników i osób pełniących funkcje kierownicze w administracji miało charakter rozproszony, a ścieżki kształcenia opierały się głównie na formach fakultatywnych, takich jak studia podyplomowe, kursy specjalistyczne czy szkolenia organizowane przez wybrane ośrodki szkoleniowe. W literaturze wskazywano na deficyt spójnego, systemowego podejścia do kształcenia w zakresie ochrony ludności, obejmującego zarówno komponent kompetencyjny, jak i procedury decyzyjne oraz współdziałanie międzyinstytucjonalne.

⁴⁷⁶ B. Wiśniewska-Paź, *Kultura bezpieczeństwa a edukacja – wzajemne konteksty, relacje i wyzwania*, Pedagogika Społeczna, XIX, 3(77), 2020, s. 101-118. <https://doi.org/10.35464/1642-672X.PS.2020.3.07>

⁴⁷⁷ M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce, Wydawnictwo Akademii Podlaskiej, 2007.

⁴⁷⁸ A. Skrabacz, L. Kanarski, K. Loranty (red.), *Edukacja dla bezpieczeństwa: o kształtowaniu kultury bezpieczeństwa*, Warszawa, Wojskowe Centrum Edukacji Obywatelskiej im. płk. dypl. Mariana Porwita, 2015.

W ostatnich latach nastąpiło w Polsce wzmocnienie ram prawno-organizacyjnych odnoszących się do profesjonalizacji kadr administracji w obszarze bezpieczeństwa. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej wprowadziła obowiązek realizacji szkoleń dla przedstawicieli administracji rządowej i samorządowej w zakresie przygotowania i reagowania na sytuacje kryzysowe⁴⁷⁹. Na jej podstawie Minister Spraw Wewnętrznych i Administracji określił programy szkoleń właściwe dla poszczególnych szczebli administracji, w tym w rozporządzeniu z dnia 6 lutego 2025 r.⁴⁸⁰ Takie rozwiązania sprzyjają standaryzacji kompetencji, ujednoliceniu praktyk oraz budowaniu zdolności instytucjonalnej do podejmowania decyzji w warunkach presji czasu i niepewności informacyjnej.

W ramach nowego systemu OLiOC utworzono Wyższe Kursy Ochrony Ludności (WKOL) adresowane do różnych grup decydentów. Przykładowo, w lutym 2025 r. uruchomiono cykl szkoleń dla starostów i marszałków województw, a we wrześniu 2025 r. – kurs dla ministrów, wiceministrów i kierowników urzędów centralnych⁴⁸¹. Programy szkoleń obejmują moduły tematyczne, takie jak: środowisko bezpieczeństwa, kierowanie bezpieczeństwem, system ochrony ludności i obrony cywilnej oraz dobre praktyki. Kształcenie ma charakter praktyczny – uczestnicy biorą udział w warsztatach, analizują rzeczywiste scenariusze kryzysowe i wypracowują schematy działania. Przewidziano naukę m.in. krajowych i międzynarodowych ram prawnych, funkcjonowania państwa w sytuacjach zagrożeń, systemów ostrzegania i alarmowania, organizacji ewakuacji i akcji ratowniczych, współpracy cywilno-wojskowej czy koordynacji działań. Również na poziomie lokalnym, we współpracy z wojewodami i szkołkami resortowymi (np. ośrodkami PSP), prowadzone są szkolenia dla prezydentów miast, burmistrzów i wójtów. Przykładowo, w czerwcu 2025 r. w woj. opolskim zorganizowano trzydniowe

⁴⁷⁹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

⁴⁸⁰ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 6 lutego 2025 r. w sprawie programów szkoleń z zakresu ochrony ludności i obrony cywilnej oraz wymagań dla podmiotów prowadzących szkolenia (Dz.U. z 2025 r. poz. 162).

⁴⁸¹ KG PSP, Wyższy Kursu Ochrony Ludności dla osób pełniących funkcje ministrów, sekretarzy stanu, podsekretarzy stanu i kierowników urzędów centralnych (WKOL-C), <https://www.gov.pl/web/kgpsp/wyzszy-kursu-ochrony-ludnosci-dla-osob-pelniacych-funkcje-ministrow-sekretarzy-stanu-podsekretarzy-stanu-i-kierownikow-urzedow-centralnych-wkol-c>, [dostęp: 10.10.2025].

szkolenie dla władz gmin, kładąc szczególny nacisk na współpracę z różnymi służbami, koordynację działań lokalnych oraz zagadnienia takie jak ocena ryzyka, ostrzeganie ludności, prowadzenie ewakuacji czy udzielanie pierwszej pomocy⁴⁸². Szkolenia te mają być powtarzane cyklicznie co roku, aby stale podnosić kompetencje decydentów lokalnych.

Uzupełnieniem systemu kursów resortowych są liczne studia podyplomowe oraz kierunki akademickie w obszarze nauk o bezpieczeństwie. W Polsce od lat 2000. powstały kierunki takie jak bezpieczeństwo narodowe, zarządzanie kryzysowe, ochrona ludności czy administracja w systemie bezpieczeństwa, oferowane przez uczelnie cywilne i wojskowe. Wiele uczelni publicznych i niepublicznych prowadzi takie studia, kształcąc zarówno studentów, jak i doksztalając urzędników. Programy obejmują wiedzę teoretyczną z zakresu bezpieczeństwa wewnętrznego, prawa kryzysowego, obrony cywilnej, ale również praktyczne elementy zarządzania sytuacjami nadzwyczajnymi. Specjalistyczne szkolenia i studia dla samorządów są kluczowym elementem budowania lokalnej i krajowej odporności na sytuacje nadzwyczajne. Zajęcia prowadzą doświadczeni praktycy, a wykorzystuje się aktywizujące metody kształcenia – studia przypadków, treningi decyzyjne, symulacje – by przygotować administrację do efektywnego reagowania na potrzeby społeczeństwa w czasie kryzysu.

Warto podkreślić, że ustawa o ochronie ludności z 2024 r. nałożyła na administrację publiczną nie tylko obowiązek posiadania planów ochrony ludności czy organizacji systemu wczesnego ostrzegania, ale *explicite* wymaga prowadzenia szkoleń i ćwiczeń z tej tematyki oraz edukowania społeczeństwa⁴⁸³. Jest to pierwsze tak kompleksowe ujęcie obowiązków edukacyjnych administracji w sytuacjach kryzysowych – ustawodawca dostrzegł potrzebę ujednoliconego przygotowania kadr oraz stałego doskonalenia ich kompetencji. Pierwsze doświadczenia wdrażania nowego systemu są pozytywne: wzrasta świadomość roli administracji w systemie bezpieczeństwa oraz

⁴⁸² Opolski Urząd Wojewódzki, Rozpoczęły się kolejne szkolenia dla władz samorządowych z Opolszczyzny w zakresie ustawy o ochronie ludności i obronie cywilnej, <https://www.gov.pl/web/uw-opolski/rozpoczely-sie-kolejne-szkolenia-dla-wladz-samorzadowych-z-opolszczyzny-w-zakresie-ustawy-o-ochronie-ludnosci-i-obronie-cywilnej>, [dostęp: 10.10.2025].

⁴⁸³ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907, art. 17).

odpowiedzialność władz za przygotowanie społeczności na wypadek klęsk żywiołowych czy konfliktu zbrojnego. Można jednak przewidywać wyzwania – np. konieczność aktualizacji programów szkoleń co pewien czas, zmotywowania wszystkich adresatów do udziału (zwłaszcza przy dużej rotacji kadr), a także zapewnienia odpowiedniej liczby instruktorów-praktyków. Niemniej kierunek zmian jest zgodny z trendami międzynarodowymi, gdzie podkreśla się profesjonalizację służby cywilnej w obszarze bezpieczeństwa. Dobrze wyszkolona administracja stanowi fundament sprawnego zarządzania kryzysowego i kooperacji z pozostałymi podmiotami systemu bezpieczeństwa.

Kolejną grupę adresatów działań szkoleniowych stanowią służby ratownicze i formacje reagowania – Państwowa Straż Pożarna, Ochotnicza Straż Pożarna, system Państwowego Ratownictwa Medycznego, GOPR, WOPR oraz inne podmioty operacyjne – które dysponują rozbudowanymi, sformalizowanymi systemami kształcenia zawodowego i doskonalenia kompetencji. Na przykład PSP posiada hierarchiczny system kształcenia: od szkół aspirantów (kształcących techników pożarnictwa), przez Szkołę Główną Służby Pożarniczej (kształcącej oficerów – inżynierów pożarnictwa) po ośrodki szkolenia PSP prowadzące kursy specjalistyczne dla strażaków różnych specjalności. Każdy nowo przyjęty funkcjonariusz PSP przechodzi szkolenie podstawowe w komendach lub ośrodkach, a następnie może się specjalizować (np. kursy ratownictwa technicznego, chemicznego, wysokościowego, medycznego itd.). Ochotnicza Straż Pożarna – złożona z wolontariuszy – także prowadzi wewnętrzne szkolenia we współpracy z PSP, aby druhowie OSP zdobyli wymagane uprawnienia (np. kurs podstawowy strażaka OSP, kurs dowódców, naczelników itp.). System szkolenia służb ratowniczych jest stale doskonalony i zawiera elementy kształcenia ustawicznego – strażacy i ratownicy regularnie uczestniczą w ćwiczeniach, szkoleniach okresowych, seminariach doskonalących, by utrzymać i poszerzać swoje kompetencje⁴⁸⁴. Podobne mechanizmy dotyczą ratownictwa medycznego (system kursów dla ratowników i dyspozytorów medycznych, specjalizacje dla lekarzy medycyny ratunkowej) czy służb takich jak policja, której funkcjonariusze również odbywają szkolenia w szkołach policyjnych i centrum szkolenia antyterrorystycznego.

⁴⁸⁴ B. Wiśniewska-Paź, *Współczesne zagrożenia – bezpieczeństwo – edukacja, czyli jak uczyć społeczeństwo zasad bezpieczeństwa*, Wrocław, Wydawnictwo Uniwersytetu Wrocławskiego, 2018.

Równolegle do kształcenia indywidualnego kluczowe znaczenie przypisuje się doskonaleniu praktycznemu w formule ćwiczeń, symulacji i treningów koordynacyjnych, realizowanych na różnych szczeblach organizacyjnych – od lokalnego po ogólnokrajowy. Ćwiczenia te obejmują zarówno przedsięwzięcia branżowe, ukierunkowane na procedury właściwe danej formacji, jak i ćwiczenia zintegrowane, prowadzone w układzie wielosłużbowym oraz cywilno-wojskowym, w których weryfikowane są mechanizmy współdziałania, komunikacji i dowodzenia w scenariuszach złożonych zdarzeń. Nowa ustawa o ochronie ludności nałożyła obowiązek regularnego prowadzenia ćwiczeń z zakresu ochrony ludności^{485,486}. Ćwiczenia służą praktycznemu sprawdzeniu planów reagowania i doskonaleniu współdziałania różnych podmiotów: straży, policji, pogotowia, administracji cywilnej i jednostek wojskowych (np. WOT). Podczas ćwiczeń uczestnicy uczą się m.in. zasad komunikacji kryzysowej, procedur dowodzenia na miejscu zdarzenia, logistyki akcji ratunkowej czy zasad informowania ludności. Przykładowo, program szkoleń dla starostów przewiduje ćwiczenia z zakresu ochrony ludności i obrony cywilnej przygotowujące do działania w przypadku wystąpienia zagrożenia – w praktyce mogą to być np. powiatowe ćwiczenia reagowania na skażenie chemiczne czy trening systemu alarmowania ludności. Dzięki takim praktycznym formom szkolenia służby ratunkowe nie działają w izolacji, lecz uczą się wspólnego reagowania zgodnie z ideą zintegrowanego systemu ratowniczego, tj. Krajowy System Ratowniczo-Gaśniczy integruje PSP, OSP i inne służby w jednym układzie.

Zakres wyzwań szkoleniowych w służbach ratowniczych ulega systematycznemu rozszerzeniu wraz ze zmianą profilu współczesnych zagrożeń oraz oczekiwań wobec państwowych struktur reagowania. Państwowa Straż Pożarna, obok tradycyjnych zadań gaśniczych, realizuje obecnie także działania z zakresu ratownictwa technicznego, chemicznego, ekologicznego i medycznego, a w coraz większym stopniu również przedsięwzięcia przypisywane sferze ochrony ludności i obrony cywilnej, w tym dekontaminację oraz wsparcie organizacyjne w sytuacjach masowych zdarzeń.

⁴⁸⁵ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907, art. 53-54).

⁴⁸⁶ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 lutego 2025 r. w sprawie ćwiczeń z zakresu ochrony ludności i obrony cywilnej (Dz.U. z 2025 r. poz. 253).

Wprowadzone w 2024 r. rozwiązania prawne w obszarze ochrony ludności wzmocniły pozycję PSP jako podstawowego filaru systemu, co wynika z jej zasobów, infrastruktury oraz doświadczenia operacyjnego. Jednocześnie wśród nowych zadań wskazuje się m.in. popularyzowanie wiedzy w zakresie ochrony ludności i obrony cywilnej, współudział w organizacji systemu alarmowania oraz wsparcie koordynacji pomocy humanitarnej. W konsekwencji rośnie znaczenie przygotowania funkcjonariuszy nie tylko do działań stricte ratowniczych, lecz także do udzielania pomocy ludności w warunkach katastrof, długotrwałych zakłóceń oraz sytuacji o podwyższonym ryzyku, w tym zdarzeń CBRN. Doświadczenia ostatnich lat pokazały, że część aktywności o charakterze ochronnym i logistycznym była już realizowana praktycznie, przykładowo w okresie pandemii COVID-19, kiedy w działania angażowano również zasoby PSP i OSP w obszarach wykraczających poza klasyczne ratownictwo. Formalizacja i poszerzenie katalogu zadań implikuje konieczność aktualizacji programów szkoleniowych, w tym wprowadzania komponentów dotyczących zagrożeń hybrydowych, bezpieczeństwa teleinformatycznego oraz procedur reagowania w warunkach konfliktu zbrojnego, takich jak ewakuacja ludności cywilnej czy działania w rejonach objętych zniszczeniami infrastruktury krytycznej. Tendencje te znajdują odzwierciedlenie w praktyce dydaktycznej ośrodków szkolenia pożarniczego, gdzie stopniowo zwiększa się udział treści z zakresu ochrony ludności, a ćwiczenia poligonowe są uzupełniane o scenariusze uwzględniające zdarzenia o charakterze militarnym i ich konsekwencje dla bezpieczeństwa cywilnego. Podsumowując, polskie służby ratownicze cechuje rozbudowany, profesjonalny system kształcenia, który zapewnia im wysoki poziom przygotowania. Znajduje to odzwierciedlenie w ogromnym zaufaniu społecznym, jakim Polacy darzą strażaków oraz inne służby niosące pomoc – co omówiono w dalszej części rozdziału⁴⁸⁷. W miarę pojawiania się nowych zagrożeń (np. zwiększone ryzyko konfliktu zbrojnego w Europie) system szkolenia jest intensywnie rozwijany, aby ratownicy mogli skutecznie chronić ludność w każdej sytuacji.

⁴⁸⁷ IBRiS, Kryzys zaufania do instytucji. Kto zyskuje, a kto traci?, <https://ibris.pl/kryzys-zaufania-do-instytucji-kto-zyskuje-a-kto-traci/>, [dostęp: 10.10.2025].

Powszechna edukacja na rzecz bezpieczeństwa realizowana jest przede wszystkim poprzez system oświaty. Już od najmłodszych lat dzieci nabywają podstawowe nawyki – w przedszkolach uczą się numerów alarmowych poprzez zabawę, a w szkołach podstawowych w ramach zajęć zintegrowanych i techniki poznają elementy pierwszej pomocy i zasady ruchu drogowego. Kluczową rolę pełni przedmiot Edukacja dla bezpieczeństwa (EDB), który jest obowiązkowy w VIII klasie szkoły podstawowej oraz I klasie szkoły ponadpodstawowej (liceum, technikum) – wprowadzono go w 2009 r. w miejsce dawnego przysposobienia obronnego. Celem EDB (określonym w podstawie programowej) jest przygotowanie uczniów do właściwych zachowań w sytuacjach zagrażających życiu lub zdrowiu oraz wyrobienie podstawowych umiejętności reagowania kryzysowego (np. udzielania pierwszej pomocy, ewakuacji podczas pożaru czy alarmu bombowego, rozpoznawania alarmów). Podstawa programowa EDB obejmuje także edukację obronną – m.in. elementarne wiadomości o Siłach Zbrojnych RP, rodzajach alarmów i zasadach postępowania w czasie wojny. W ostatnich latach, w odpowiedzi na zmieniające się uwarunkowania geopolityczne, zwiększono nacisk na edukację proobronną. W 2022 r. Minister Edukacji i Nauki podpisał zmiany do podstawy programowej EDB, dodając szkolenie strzeleckie – docelowo od roku szkolnego 2024/2025 wszystkie szkoły ponadpodstawowe mają obowiązkowo prowadzić zajęcia z posługiwania się bronią (strzelanie na symulatorach: repliki ASG, strzelnice wirtualne lub laserowe, a tam gdzie to możliwe także z bronią palną). Przywraca to elementy nieobecne w szkołach od dekad, a ma na celu zwiększenie zdolności obronnych młodzieży. Równocześnie wiele szkół ponadpodstawowych oferuje dodatkowe zajęcia lub klasy profilowane o charakterze proobronnym i ratowniczym (np. klasy mundurowe, w których obok programu EDB prowadzone są zajęcia z musztry, terenoznawstwa, strzelectwa itp.). Na poziomie szkolnictwa wyższego oraz w ramach kursów dla dorosłych również dostępne są formy poszerzania wiedzy z zakresu bezpieczeństwa – na niektórych uczelniach funkcjonują Centra Szkolenia Obronnego oferujące kursy pierwszej pomocy dla społeczności akademickiej czy ćwiczenia ewakuacyjne na wypadek pożaru. Wiele uczelni organizuje też otwarte wykłady i warsztaty dla mieszkańców (np. cykl spotkań „Akademia Bezpieczeństwa” adresowany do seniorów w jednym z miast akademickich).

Poza systemem szkolnym istotną rolę w podnoszeniu świadomości społecznej o zagrożeniach odgrywają rozmaite szkolenia, kampanie informacyjne i inicjatywy prowadzone przez instytucje publiczne oraz organizacje pozarządowe. Państwo polskie (m.in. MSWiA, Rządowe Centrum Bezpieczeństwa, Komenda Główna PSP) realizuje kampanie uświadamiające i uczy właściwych zachowań w sytuacjach kryzysowych. Przykładem jest platforma edukacyjna ochronaludnosci.edu.pl⁴⁸⁸, uruchomiona przez Akademię Pożarniczą – zawiera ona „Niezbędnik Ochrony Ludności”, czyli praktyczne poradniki dla obywateli jak przygotować rodzinę i dom na różne zagrożenia (instrukcje tworzenia domowego zestawu ratunkowego, opracowania planu ewakuacji, zabezpieczenia domu, zasady alarmowania itp.). Platforma udostępnia również bezpłatne szkolenia e-learningowe dla różnych grup: administracji, organizacji społecznych oraz ogółu obywateli. W ostatnich latach realizowano kampanie społeczne promujące konkretne pożądane zachowania – np. „Bądź gotowy – ratuj życie” zachęcającą do nauki pierwszej pomocy czy „Zgaś ryzyko” dotyczącą zapobiegania pożarom domów. Media publiczne i prywatne włączają się w takie akcje, emitując spoty edukacyjne (o bezpieczeństwie nad wodą latem, o konieczności posiadania czujek czadu zimą itp.). Również organizacje pozarządowe prowadzą od lat szkolenia dla ludności – Polski Czerwony Krzyż regularnie organizuje masowe kursy pierwszej pomocy (często bezpłatne dla uczniów i studentów), a jednostki OSP w wielu gminach urządzają pokazy ratownictwa podczas festynów. Pojawiają się też oddolne inicjatywy, jak grupy preppersów czy stowarzyszenia na rzecz obrony cywilnej (np. „Świadoma Obrona Cywilna”), które poprzez Internet i warsztaty uczą obywateli, jak przygotować zapasy wody i żywności, podstaw survivalu itp.

Warto przytoczyć tutaj doświadczenia innych krajów, częściowo już wdrażane w Polsce. Na uwagę zasługuje amerykański program CERT (ang. Community Emergency Response Teams) – system wolontariackiego szkolenia obywateli do reagowania w katastrofach⁴⁸⁹. Od lat 80. XX w. przeszkolono w USA ponad 600 tys. osób, tworząc ponad 2700 lokalnych zespołów

⁴⁸⁸ <https://ochronaludnosci.edu.pl>, [dostęp: 10.10.2025].

⁴⁸⁹ Federal Emergency Management Agency, Community Emergency Response Team (CERT). Basic Training: Participant Manual, National CERT Program, 2011, https://www.fema.gov/sites/default/files/2020-07/fema-cert_basic-training-participant-manual_01-01-2011.pdf#page=1&zoom=auto,-263,798, [dostęp: 10.10.2025].

CERT gotowych wspierać zawodowe służby. Wolontariusze CERT uczą się m.in. gaszenia niewielkich pożarów, udzielania pierwszej pomocy, lekkich poszukiwań i ratownictwa oraz podstaw organizacji działań – a zdobyte umiejętności wykorzystują potem we własnych społecznościach podczas powodzi, huraganów czy innych klęsk. W Japonii z kolei istnieje wieloletnia tradycja powszechnego angażowania społeczeństwa w przygotowanie na klęski żywiołowe. Regularnie odbywają się tam treningi i drille – 1 września, w Dniu Zapobiegania Katastrofom, setki tysięcy Japończyków uczestniczą w ćwiczeniach ewakuacyjnych, gaszenia pożarów czy udzielania pomocy. W miastach corocznie organizuje się lokalne bosai kunren (treningi katastroficzne), gdzie mieszkańcy uczą się obsługi pomp pożarniczych czy wiązania staz taktycznych, a na osiedlach utrzymuje się magazyny sprzętu ratunkowego, do których dostęp mają przeszkoleni wolontariusze. W szkołach kilka razy do roku odbywają się próbne alarmy i ewakuacje, a dzieci od najmłodszych lat uczone są właściwych odruchów – czego efektem była słynna „cudowna ewakuacja” w mieście Kamaishi podczas tsunami 2011 r., gdzie dzięki edukacji żadna ze szkół nie poniosła dużych strat wśród uczniów. Rząd i społeczeństwo Japonii dbają również o pamięć o katastrofach – powstały liczne muzea i centra edukacyjne poświęcone tragicznym wydarzeniom (w samym regionie Tōhoku po tsunami w 2011 r. utworzono ponad 10 muzeów i ośrodków edukacyjnych). Mieszkańcy Japonii, mając świeżo w pamięci lekcje z przeszłości, poważnie podchodzą do kwestii bezpieczeństwa i nie popadają w rutynę. Innym przykładem jest Szwecja, która w 2018 r. – pierwszy raz od czasów zimnej wojny – rozesłała do wszystkich gospodarstw domowych broszurę „Om krisen eller kriget kommer” („Gdy nadejdzie kryzys lub wojna”). W listopadzie 2024 r. wydano jej zaktualizowaną edycję, wysyłając 5,2 mln egzemplarzy do mieszkańców (także w języku polskim). Broszura w prosty sposób instruuje obywateli, jak przygotować zapasy żywności i wody na co najmniej 72 godziny, jak postępować podczas alarmów, gdzie szukać schronienia i rzetelnych informacji. Rząd Szwecji poprzez tę kampanię pragnie wzmocnić „odporność społeczeństwa” i przygotować ludzi psychicznie na ewentualność konfliktu zbrojnego. Międzynarodowe przykłady pokazują, że kompleksowa edukacja całego społeczeństwa – od dzieci po seniorów – jest możliwa i przynosi wymierne efekty w postaci mniejszej paniki, sprawniejszej ewakuacji, a nawet uratowanych

istnień podczas realnego kryzysu. Polska również zmierza w tym kierunku, czemu sprzyjają zarówno oddolne inicjatywy obywatelskie, jak i odgórne programy państwowe będące efektem nowych regulacji. Skuteczność wszelkich działań edukacyjnych i szkoleniowych w obszarze ochrony ludności zależy od ukształtowania w społeczeństwie i instytucjach odpowiedniej kultury bezpieczeństwa. Termin ten, choć stosunkowo nowy, zyskuje na popularności w naukach o bezpieczeństwie. Klasycznie kulturę bezpieczeństwa definiowano w kontekście organizacji (np. przemysłu wysokiego ryzyka) jako „produkt indywidualnych i grupowych wartości, postaw, percepcji, kompetencji i wzorów zachowań określających zaangażowanie oraz styl zarządzania bezpieczeństwem w organizacji”⁴⁹⁰. Innymi słowy, jest to swoisty wewnętrzny „program operacyjny” kierujący zachowaniami ludzi w zakresie zapewnienia sobie bezpieczeństwa⁴⁹¹. Kultura bezpieczeństwa ma charakter psychospołeczny – przejawia się na zewnątrz poprzez konkretne działania i postawy jednostek oraz grup, a zarazem wynika z wewnętrznych przekonań, doświadczeń i wiedzy uczestników. W szerszym ujęciu państwa kulturę bezpieczeństwa można rozumieć jako wspólny mianownik świadomości społecznej i instytucjonalnej w zakresie radzenia sobie z zagrożeniami. Obejmuje ona m.in.: nawyki (utrwalone, automatyczne zachowania sprzyjające bezpieczeństwu, np. zapinanie pasów w aucie, posiadanie gaśnicy w domu), postawy (stosunek do kwestii bezpieczeństwa – czy traktujemy je priorytetowo, czy bagatelizujemy ryzyko), zaufanie do instytucji (przekonanie, że służby i władze działają dla naszego dobra i kompetentnie nas ostrzegą lub uratują) oraz gotowość do współpracy (skłonność obywateli do podporządkowania się zaleceniom i współdziałania w sytuacjach kryzysowych).

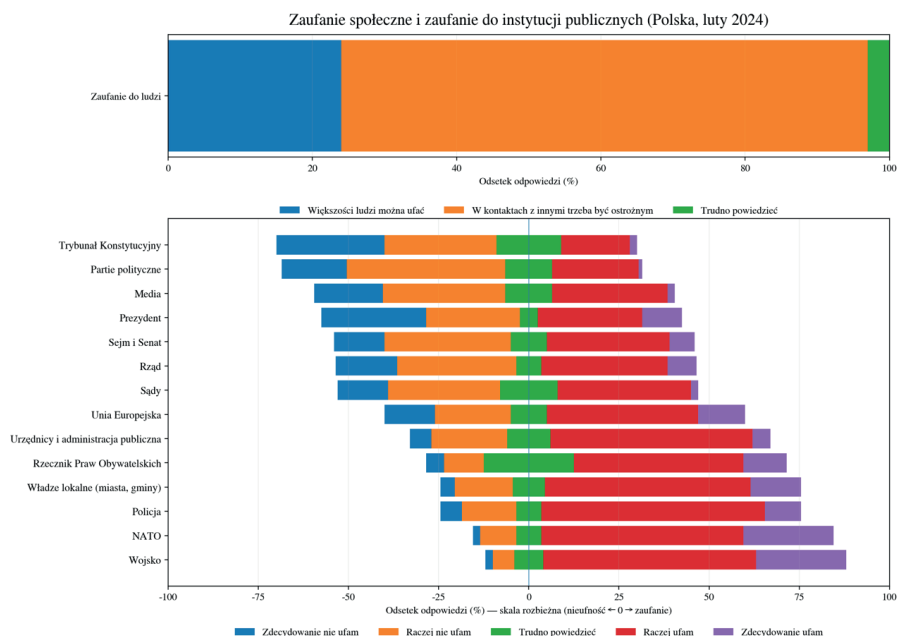
Jednym z kluczowych elementów kultury bezpieczeństwa jest zaufanie społeczne – zarówno ogólny poziom ufności między ludźmi, jak i konkretne zaufanie do służb ratowniczych i instytucji odpowiedzialnych za bezpieczeństwo. Badania socjologiczne pokazują, że Polacy tradycyjnie cechują się niskim kapitałem zaufania: aż ok. 3/4 obywateli uważa, że „w kontaktach z innymi trzeba zachować dużą ostrożność”, a tylko 1/4 deklaruje,

⁴⁹⁰ A. Filipek, C. Gałek, *Istota kultury bezpieczeństwa i jej znaczenie dla człowieka i grup społecznych*, Kultura Bezpieczeństwa, 2014, s. 17-57.

⁴⁹¹ Tamże.

że „większości ludzi można ufać”⁴⁹². Ten deficyt zaufania do innych może utrudniać oddolną współpracę i solidarność w czasach kryzysu. Jednak obraz ten nie jest jednorodny – o wiele wyższym zaufaniem Polacy darzą konkretne służby niosące pomoc. Sondaże wskazują, że Państwowa i Ochotnicza Straż Pożarna cieszą się zaufaniem na poziomie niemal 97% społeczeństwa, a Wojsko Polskie ok. 94%. Są to najwyższe wskaźniki w kraju, znacznie przewyższające poziom zaufania np. do rządu (~37%) czy wymiaru sprawiedliwości (~36%). Oznacza to, że strażacy i żołnierze stanowią w oczach społeczeństwa stabilny filar bezpieczeństwa, postrzegany jako bezstronny i skuteczny (raport IBRiS określa te służby jako „niosące realną pomoc i budujące poczucie wspólnoty”, które łączą Polaków ponad podziałami). Tak wysoki kredyt zaufania przekłada się na gotowość ludzi do słuchania komunikatów tych służb w czasie zagrożeń – np. poleceń ewakuacji wydawanych przez straż pożarną czy zaleceń obrony cywilnej ogłaszanych przez wojsko. Słabsze zaufanie do władz cywilnych czy mediów (poniżej 40%) stanowi wyzwanie – może powodować sceptycyzm wobec komunikatów kryzysowych nadawanych przez organy administracji. Dlatego tak ważne jest budowanie wiarygodności instytucji odpowiedzialnych za bezpieczeństwo poprzez transparentność działań, rzetelną informację i włączanie obywateli w procesy decyzyjne. W tym kontekście kultura bezpieczeństwa pełni rolę „miękkiego spoiwa” systemu – jeśli obywatele ufają, że instytucje działają w ich interesie, a instytucje ufają obywatelom (np. że zastosują się do poleceń i nie wywołają paniki), wówczas wszyscy grają do jednej bramki w obliczu kryzysu. Zaufanie społeczne i zaufanie do instytucji publicznych w Polsce – stan na luty 2024 r. przedstawione zostało na rysunku 17.

⁴⁹² Centrum Badania Opinii Społecznej (CBOS), Zaufanie społeczne, Komunikat z badań nr 40/2024, Warszawa, 2024.



Rysunek 17. Zaufanie społeczne i zaufanie do instytucji publicznych w Polsce (luty 2024 r.)

Źródło: opracowanie własne na podstawie: Centrum Badania Opinii Społecznej (CBOS), Zaufanie społeczne, Komunikat z badań nr 40/2024, Warszawa, 2024.

Kultura bezpieczeństwa kształtuje się nie tylko poprzez formalne instrukcje i regulaminy służb, lecz przede wszystkim w życiu codziennym – poprzez przekazy medialne oraz oddolne wzorce zachowań. Media odgrywają tu ambiwalentną rolę: mogą zarówno budować zaufanie i świadomość, jak i szerzyć dezinformację czy panikę. W Polsce – jak wspomniano – zaufanie do mediów publicznych jest niskie (ok. 35%), nieco wyższe jest do mediów prywatnych (~51%), a jednocześnie społeczeństwo jest spolaryzowane pod względem wiarygodności informacji w mediach społecznościowych. Dlatego niezwykle ważna jest odpowiedzialna komunikacja kryzysowa. Rząd i służby powinny jasno i regularnie informować o zagrożeniach, korzystając z różnych kanałów (TV, radio, Internet, SMS-y Alert RCB). Dobrą praktyką są regularne briefingi prasowe w sytuacjach nadzwyczajnych oraz współpraca z dziennikarzami w celu prostowania nieprawdziwych pogłosek. Media z kolei powinny unikać nadmiernej sensacyjności w relacjonowaniu kryzysów, kładąc nacisk na funkcję poradniczą (np. w czasie pandemii COVID-19 część stacji

emitowała cykle edukacyjne o zdrowiu publicznym). Edukacja nieformalna odbywa się także w ramach społeczności lokalnych – np. przekazywanie sobie w rodzinie czy wśród sąsiadów dobrych nawyków (rodzice uczą dzieci, jak reagować na pożar; rolnicy w danej wsi co roku przypominają o czyszczeniu kominów przed zimą). Państwo może wspierać tę oddolną kulturę bezpieczeństwa inicjując lokalne programy (jak np. „Sąsiedzi Plus” – angażujący mieszkańców osiedli do wspólnego opracowania planów bezpieczeństwa na wypadek awarii). Ważnym ogniwem są także organizacje harcerskie i inne grupy wolontariatu – to one często „humanizują” przekaz i docierają tam, gdzie oficjalne struktury nie sięgają. Przykładowo harcerze od lat krzewią wśród młodzieży zaradność poprzez gry terenowe uczące orientacji w terenie i pierwszej pomocy (Harcerska Szkoła Ratownictwa itp.). Tego typu działania kształtują proaktywne postawy już u młodych ludzi.

Można powiedzieć, że kultura bezpieczeństwa jest miękkim spoiwem całego systemu zarządzania kryzysowego – spaja ona element ludzki, relacje i wartości, których nie da się zadekretować ustawą. Nawet najlepiej wyposażone służby na nic się zdadzą, jeśli ludzie nie będą im wierzyć lub nie będą wiedzieli, jak się zachować. Przykładowo, podczas ewakuacji wielkiego miasta kluczowe jest uniknięcie paniki – to wymaga zarówno zaufania do komunikatów władzy, jak i dyscypliny społecznej. Tam, gdzie kultura bezpieczeństwa jest silna (np. w Japonii), mieszkańcy potrafią sprawnie opuścić zagrożony teren, bo od dziecka ćwiczyli ten scenariusz i ufają organizatorom ewakuacji. W Polsce wyzwaniem pozostaje wzmacnianie kultury bezpieczeństwa na co dzień. Eksperci wskazują na potrzebę rozpoczynania edukacji dla bezpieczeństwa już w przedszkolu i kontynuowania jej przez całe życie. Wiśniewska-Paź zauważa deficyt takiej ciągłości kształcenia – obecnie edukacja formalna w tym zakresie zaczyna się dopiero w VIII klasie podstawówki, co jej zdaniem jest zbyt późno⁴⁹³. Postuluje ona wprowadzenie elementów edukacji na rzecz bezpieczeństwa już na etapie przedszkola i młodszych klas szkoły podstawowej, a także uwzględnienie tej tematyki w programach kształcenia przyszłych nauczycieli (by pedagodzy różnych przedmiotów również

⁴⁹³ B. Wiśniewska-Paź, *Kultura bezpieczeństwa a edukacja – wzajemne konteksty, relacje i wyzwania*, *Pedagogika Społeczna*, 3(77), 2020. <https://doi.org/10.35464/1642-672X.PS.2020.3.07>

kształtowali bezpieczne postawy)⁴⁹⁴. Równie istotne jest kształcenie kadr bezpieczeństwa – czyli osób pełniących funkcje związane z bezpieczeństwem na wszystkich szczeblach, od sołtysa w małej gminie po ministrów w rządzie. Inicjatywy podjęte w ramach ustawy o ochronie ludności i obronie cywilnej zmierzają w tym kierunku, zapewniając m.in. systematyczne szkolenia i ćwiczenia dla administracji. Jednak równie ważne są poczucie misji i etos służby – kultura bezpieczeństwa to także wartości, takie jak odpowiedzialność za innych, odwaga cywilna czy gotowość do poświęceń. Takie cechy kształtuje się latami, m.in. poprzez przykład idący z góry (gdy władze same przestrzegają zasad bezpieczeństwa, społeczeństwo chętniej je naśladuje) oraz poprzez docenianie bohaterstwa i postaw prospołecznych.

Edukacja, szkolenia i kultura bezpieczeństwa to trzy filary, które wzajemnie się uzupełniają w budowaniu odporności państwa na zagrożenia. Edukacja formalna i pozaformalna dostarcza wiedzy oraz umiejętności, szkolenia i ćwiczenia przekuwają tę wiedzę w praktykę i utrwalają kompetencje, zaś kultura bezpieczeństwa tworzy kontekst społeczny, w którym wiedza i kompetencje zostają wykorzystane we właściwy sposób. Polska, podobnie jak wiele innych krajów, stoi przed wyzwaniem wzmacniania wszystkich tych obszarów. Nowe regulacje prawne (ustawa o ochronie ludności) dają solidne ramy instytucjonalne – wyznaczają zadania, obowiązki i standardy. Jednak równie istotne jest zaangażowanie społeczeństwa: aby obywatele czuli współodpowiedzialność za wspólne bezpieczeństwo, a nie postrzegali go wyłącznie jako domenę służb. Takie podejście określa się mianem paradygmatu kooperacyjnego bezpieczeństwa⁴⁹⁵, gdzie każdy – od urzędnika, poprzez ratownika, po zwykłego obywatela – odgrywa ważną rolę w łańcuchu bezpieczeństwa. Budowanie tej wspólnej kultury bezpieczeństwa to proces długofalowy, wymagający cierpliwości i systematycznych działań edukacyjnych. Jak pokazują doświadczenia innych państw, efekty są tego warte: społeczeństwo świadome zagrożeń i wyszkolone w radzeniu sobie z nimi potrafi znacznie lepiej przetrwać kryzysy i szybciej powrócić do normalności po ich ustąpieniu.

⁴⁹⁴ M. Chodyka, Z. Ciekanowski, Ochrona młodych użytkowników Internetu przed cyberzagrożeniami we współczesnym cyfrowym świecie, *Przegląd Naukowo-Metodyczny. Edukacja dla bezpieczeństwa*, 2025, XVIII, 2(67), s. 159-168.

⁴⁹⁵ A. Ciupiński, *Paradygmat kooperacyjnego bezpieczeństwa*, A. Ciupiński (red.), *Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, 2010.

6.5. Kierunki doskonalenia systemu zarządzania kryzysowego w Polsce

System zarządzania kryzysowego w Polsce stanowi element kierowania bezpieczeństwem narodowym i obejmuje logiczny cykl działań organów administracji publicznej: zapobieganie sytuacjom kryzysowym, przygotowanie do przejmowania nad nimi kontroli (planowanie), reagowanie oraz odtwarzanie zasobów i infrastruktury krytycznej (odbudowę/rekonstrukcję)⁴⁹⁶. Takie rozumienie jest utrwalone w definicji ustawowej zarządzania kryzysowego⁴⁹⁷. Na poziomie organizacyjnym polski model jest wieloszczeblowy i powiązany z podziałem terytorialnym państwa: działania są inicjowane możliwie najniżej, a w razie potrzeby eskalowane i wspierane przez szczeble wyższe. Rdzeniem komponentu planistyczno-koordynacyjnego na poziomie krajowym pozostaje Rządowe Centrum Bezpieczeństwa, które odpowiada m.in. za Krajowy Plan Zarządzania Kryzysowego (KPZK) i prowadzi całodobowe monitorowanie zagrożeń w ramach funkcji krajowego centrum zarządzania kryzysowego⁴⁹⁸. Jednocześnie od 1 stycznia 2025 r. obowiązuje kompleksowa ustawa o ochronie ludności i obronie cywilnej⁴⁹⁹, która nadaje ochronie ludności rangę spójnego systemu zdefiniowanego ustawowo, obejmującego organy administracji publicznej, podmioty wykonawcze oraz zasoby ochrony ludności. Ustawa ta wprowadza również definicję obrony cywilnej w powiązaniu z prawem międzynarodowym humanitarnym. Z perspektywy doskonalenia kluczowe jest więc traktowanie zarządzania kryzysowego i ochrony ludności jako dwóch powiązanych porządków: pierwszy porządkuje cykl „zapobieganie-przygotowanie-reagowanie-odbudowa” i narzędzia koordynacyjne, a drugi – po reformie w latach 2024-2025 – ma integrować ochronę życia i zdrowia ludności (w czasie pokoju i wojny) z budową

⁴⁹⁶ M. Chodyka, S. Żurawski, S. Wojciechowska-Filipek, Z. Ciekankowski, S. Mazur, *Critical Infrastructure Security Management in the Era of Cyber Threats*, *European Research Studies Journal*, 2025, 28(2), s. 610-621. <https://doi.org/10.35808/ersj/4000>

⁴⁹⁷ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r., poz. 1907).

⁴⁹⁸ Rządowe Centrum Bezpieczeństwa, *Krajowy Plan Zarządzania Kryzysowego*, 2025.

⁴⁹⁹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r., poz. 1907).

zasobów, szkoleniami, alarmowaniem, obiektami zbiorowej ochrony oraz mechanizmami finansowania sterowanymi programowo.

Do trwałych atutów polskiego modelu należy istnienie wyspecjalizowanej struktury operacyjno-analitycznej na szczeblu centralnym. RCB zapewnia nie tylko planowanie cywilne (KPZK), ale i codzienną świadomość sytuacyjną (monitoring zagrożeń, współpraca informacyjna z resortami i instytucjami, przygotowanie ostrzeżeń). RCB wskazuje wprost, że KPZK obejmuje wszystkie fazy zarządzania kryzysowego i stanowi dokument wyjściowy dla planowania cywilnego na szczeblach centralnym i wojewódzkim. W obszarze reagowania bezpośredniego znaczącą zdolność państwa tworzy komponent ratowniczy – Krajowy System Ratowniczo-Gaśniczy – integrujący działania ratownicze przede wszystkim Państwowej Straży Pożarnej oraz Ochotniczych Straży Pożarnych. W ujęciu oficjalnym system służy likwidacji lub ograniczeniu zagrożeń wynikających m.in. z pożarów, klęsk żywiołowych i innych miejscowych zagrożeń⁵⁰⁰. W ostatniej dekadzie wyraźnym wzmocnieniem odporności informacyjnej stało się upowszechnienie szybkiego alarmowania ludności przez sieci komórkowe, czyli Alert RCB. Zgodnie z informacją RCB, obywatele znajdujący się na obszarze zagrożenia otrzymują SMS bez konieczności wcześniejszej rejestracji; operatorzy mają obowiązek niezwłocznej dystrybucji komunikatu na wskazanym obszarze, a minimalną jednostką obszaru dla wysyłki jest powiat. Wymiar wykonawczy współpracy z operatorami został umocowany w rozporządzeniu Rady Ministrów z 7 grudnia 2018 r. dotyczącym współpracy dyrektora RCB z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu⁵⁰¹. Warto podkreślić, że doskonalenie ostrzegania było reakcją na doświadczenia kryzysowe i wnioski pokontrolne. W odniesieniu do nawałnic z sierpnia 2017 r. RCB opisywało m.in. bilans tragicznych zdarzeń (łącznie 5 ofiar śmiertelnych, w tym dwie harcerki w okolicach Suszka) oraz znaczną skalę interwencji

⁵⁰⁰ KG PSP, Krajowy system ratowniczo-gaśniczy (KSRG), <https://www.gov.pl/web/kgpsp/ksg>, [dostęp: 10.10.2025].

⁵⁰¹ Rozporządzenie Rady Ministrów z dnia 7 grudnia 2018 r. w sprawie współpracy dyrektora Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu (Dz.U. z 2018 r. poz. 2309).

i zakłóceń funkcjonowania infrastruktury⁵⁰². Istotnym elementem „uczenia się systemu” była też instytucjonalizacja wnioskowania po kryzysach. Po nawałnicach 2017 r. powołano międzyresortowy zespół oceniający funkcjonowanie systemu ratownictwa i zarządzania kryzysowego⁵⁰³, a RCB informowało o przyjęciu przez rząd sprawozdania z prac tego zespołu oraz o tym, że nawałnice dotknęły ponad 170 gmin⁵⁰⁴.

Pomimo wskazanych osiągnięć, audyty oraz wystąpienia pokontrolne wskazywały na utrzymujące się, strukturalne słabości – szczególnie na styku poziomu lokalnego, planowania i realnej gotowości organizacyjnej. Charakter tych luk można uporządkować w trzech wiązkach:

- deficyty planistyczne i cyklu aktualizacji,
- niedostatki organizacji całodobowych zdolności koordynacyjnych
- niewystarczająca integracja obszarów zarządzania kryzysowego i obrony cywilnej w dawnym modelu.

Po pierwsze, w dokumentacji kontrolnej NIK widoczne są problemy z utrzymaniem wymaganego cyklu aktualizacji planów oraz z „przełożeniem papieru na działanie”. Przykładowo, w wystąpieniu pokontrolnym dotyczącym Urzędu Gminy Stare Miasto wskazano, że w latach 2015-2017 gmina nie była dostatecznie przygotowana pod względem prawno-organizacyjnym do właściwego wykonywania działań w ramach zarządzania kryzysowego, a kluczową przyczyną był nieaktualny plan reagowania kryzysowego sporządzony w 2008 r. dokument spełniający wymogi wprowadzono dopiero we wrześniu 2017 r., w toku kontroli⁵⁰⁵. Takie ustalenia są o tyle krytyczne, że plan ma być narzędziem operacyjnym, a nie jedynie wypełnieniem formalnego obowiązku. Po drugie, utrzymują się wyzwania związane z funkcjonowaniem powiatowych i wojewódzkich centrów zarządzania kry-

⁵⁰² Rządowe Centrum Bezpieczeństwa (RCB), Skutki frontu burzowego, komunikat z 12.08.2017, <https://archiwum.rcb.gov.pl/skutki-frontu-burzowego/> [dostęp: 16.02.2025].

⁵⁰³ Prezes Rady Ministrów, Zarządzenie nr 101 z dnia 4 września 2017 r. w sprawie Międzyresortowego Zespołu do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego (M.P. 2017 poz. 837).

⁵⁰⁴ P. Domański, Gwałtowne zjawiska pogodowe w sierpniu 2017 – działania ratownicze i zarządzanie kryzysowe, Biuletyn Kwartalny Biura Analiz i Reagowania RCB, 20, s. 16-18. <https://archiwum.rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-20-kopia.pdf>, [dostęp: 10.10.2025].

⁵⁰⁵ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Urząd Gminy Stare Miasto, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.03.2017; P.17.039, Poznań, 22.12.2017.

zysowego jako całodobowych węzłów obiegu informacji. W odniesieniu do powiatu konińskiego w dokumentacji pokontrolnej opisano organizacyjne uruchomienie Powiatowego Centrum Zarządzania Kryzysowego (PCZK) i jego rolę w zapewnianiu całodobowego obiegu informacji⁵⁰⁶. Z kolei w wystąpieniu dotyczącym administracji wojewódzkiej w Małopolsce wskazano m.in., że wojewódzki plan zarządzania kryzysowego nie był aktualizowany przez cztery lata, mimo ustawowego założenia dwuletniego cyklu planowania; równocześnie zauważono, że nawet przy funkcjonowaniu centrów operacyjnych mogą wystąpić deficyty w standardach dyżurowych (np. obsada dyżurów) oraz w regularności ćwiczeń.

Po trzecie, wnioski kontrolne i eksperckie wskazywały na długotrwały problem „dualizmu systemowego”: współistnienie zarządzania kryzysowego oraz obrony cywilnej, regulowanych i wykonywanych w praktyce niespójnie, co sprzyjało rozproszeniu odpowiedzialności oraz dublowaniu planowania. W cytowanym wystąpieniu pokontrolnym wprost wskazano potrzebę integracji przepisów w zakresie zarządzania kryzysowego i obrony cywilnej oraz krytycznie odniesiono się do uzasadnienia utrzymywania odrębnych planów i odrębnego przypisywania zadań dla dwóch systemów⁵⁰⁷. Dodatkowym elementem problemu była historyczna degradacja infrastruktury ochronnej oraz niewystarczające finansowanie obszaru obrony cywilnej, na co zwracano uwagę również w analizach instytucjonalnych⁵⁰⁸. Ostatecznie, diagnozę luk dopełnia perspektywa ekonomiczno-inwestycyjna. Zbyt słaba prewencja bywa kompensowana wysokimi kosztami usuwania skutków. W raporcie NIK dotyczącym infrastruktury przeciwpowodziowej wskazywano m.in. skalę strat powodzi z 2010 r. (ok. 12,5 mld zł) oraz wielkość wydatków publicznych na usuwanie skutków, a także przedstawiano rażące dysproporcje między nakładami na usuwanie skutków a nakładami na

⁵⁰⁶ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Starostwo Powiatowe w Koninie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.02.2017, Poznań, 18.01.2018

⁵⁰⁷ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Małopolski Urząd Wojewódzki w Krakowie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LKR.410.016.01.2017, Kraków, 17.01.2018.

⁵⁰⁸ Rzecznik Praw Obywatelskich (Marcin Wiącek), Wystąpienie do Ministra Spraw Wewnętrznych i Administracji w sprawie organizacji i funkcjonowania obrony cywilnej (m.in. uwagi dot. kosztów budowy i utrzymania schronów), Warszawa, 6.12.2022, sygn. VII.7215.1.2022.MP.

inwestycje i utrzymanie urządzeń chroniących przed powodzią w badanym województwie⁵⁰⁹. W ujęciu systemowym jest to argument za przejściem od logiki „reaktywnej” (płacimy po katastrofie) do logiki „odpornościowej” (inwestujemy w redukcję ryzyka).

Uzasadnienie kierunków doskonalenia wymaga osadzenia w trendach, które zwiększają częstość, niepewność i złożoność sytuacji kryzysowych: zmianach klimatu, transformacji technologicznej oraz zmienionym środowisku bezpieczeństwa. W wymiarze klimatycznym kluczowe znaczenie ma wzrost częstości i intensywności zjawisk ekstremalnych: fal upałów, susz, nawalnych opadów i powodzi błyskawicznych. IMGW-PIB w raporcie „Klimat Polski 2024” syntetyzuje obserwowane trendy wzrostu temperatury i opisuje współczesne spektrum ekstremów pogodowych, które zwiększa presję na służby oraz administrację⁵¹⁰. W ujęciu europejskim IPCC wskazuje na już obserwowane i dalej nasilające się w Europie zmiany w klimatycznych „driverach” ryzyka, w tym rosnące natężenie ekstremalnego upału oraz zmiany w reżimach opadowych⁵¹¹. Skala problemu powoduje, że adaptacja do zmian klimatu staje się elementem polityki bezpieczeństwa, a nie wyłącznie polityki środowiskowej, co koresponduje z celami krajowej polityki adaptacyjnej⁵¹².

W wymiarze technologicznym cyfryzacja zwiększa możliwości monitorowania i analityki, ale równocześnie poszerza powierzchnię ataku cybernetycznego. W praktyce oznacza to, że zdarzenie cybernetyczne (np. zakłócenie telekomunikacji lub sieci energetycznej) może mieć konsekwencje analogiczne do klasycznych katastrof, a zarządzanie kryzysowe musi być powiązane z ochroną infrastruktury i ciągłością usług. Ten kierunek myślenia jest spójny z podejściem odpornościowym promowanym w NATO, gdzie cywilna gotowość i ciągłość podstawowych usług stanowią element

⁵⁰⁹ Najwyższa Izba Kontroli (NIK), Informacja o wynikach kontroli: Realizacja przez administrację publiczną województwa podkarpackiego zadań z zakresu infrastruktury przeciwpowodziowej (kontrola P/15/097; Nr ewid. 185/2015/P/15/097/LRZ; LRZ-410.004.2015), Delegatura NIK w Rzeszowie, marzec 2016, s. 5, 16.

⁵¹⁰ Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy (IMGW-PIB), *Klimat Polski 2024* (raport), 2025.

⁵¹¹ IPCC, *Climate Change 2022: Impacts, Adaptation and Vulnerability. Working Group II Contribution to the Sixth Assessment Report – Chapter 13: Europe*, 2022.

⁵¹² Ministerstwo Środowiska, *Strategiczny plan adaptacji dla sektorów i obszarów wrażliwych na zmiany klimatu do roku 2020 z perspektywą do roku 2030* (SPA 2020), 2013 (przyjęty przez RM 29.10.2013).

odporności państw⁵¹³. W wymiarze bezpieczeństwa międzynarodowego szczególną presję na system ochrony ludności wywarły zagrożenia hybrydowe i wojenne. NIK w raporcie dotyczącym przygotowania państwa na zagrożenia hybrydowe stwierdzała, że organy państwa nie są przygotowane do sprawnej realizacji zadań w ramach systemu zarządzania kryzysowego i obrony cywilnej wobec zagrożeń hybrydowych oraz wskazywała na potrzebę budowania odporności państwa na skutki takich działań⁵¹⁴. To tłumaczyła, dlaczego reforma ochrony ludności i obrony cywilnej została zaprojektowana jako rozwiązanie funkcjonujące zarówno w czasie pokoju, jak i wojny. Wreszcie, istotne są uwarunkowania integracyjne. W ramach Unii Europejskiej rozwijany jest Unijny Mechanizm Ochrony Ludności oraz rezerwa rescEU jako strategiczne, finansowane na poziomie UE zasoby reagowania i zapasy⁵¹⁵. Na poziomie globalnym rośnie znaczenie ram redukcji ryzyka katastrof (Sendai Framework), które akcentują prewencję, zarządzanie ryzykiem i „Build Back Better” w odbudowie⁵¹⁶.

W świetle diagnozy i trendów, doskonalenie polskiego systemu powinno być prowadzone w dwóch komplementarnych strumieniach: podnoszenie dojrzałości zarządzania kryzysowego (procedury, plany, interoperacyjność, gotowość 24/7) oraz (II) konsekwentna implementacja nowego systemu ochrony ludności i obrony cywilnej po reformie z lat 2024-2026 (zasoby, ewidencje, szkolenia, finansowanie programowe, obiekty ochronne, alarmowanie).

W pierwszym strumieniu priorytetem pozostaje profesjonalizacja planowania i egzekwowanie cyklu aktualizacji. RCB przypomina, że KPZK jest dokumentem obejmującym wszystkie fazy zarządzania kryzysowego i służy planowaniu cywilnemu także na szczeblu wojewódzkim, a archiwalne wyjaśnienia RCB akcentują, że aktualizacja KPZK następuje nie rzadziej

⁵¹³ NATO, Resilience, civil preparedness and Article 3 (Baseline Requirements: continuity of government, essential services, civil support to the military), 2024.

⁵¹⁴ Najwyższa Izba Kontroli, Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi (Informacja o wynikach kontroli; nr ewid. 16/2023/P/22/029/KPB; KPB.430.002.2023), 2023.

⁵¹⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36-214).

⁵¹⁶ United Nations (UN), Sendai Framework for Disaster Risk Reduction 2015-2030 (A/RES/69/283), 2015.

niż raz na dwa lata oraz w razie potrzeby po uruchomieniu procedur. Spójność cyklu planowania na wszystkich szczeblach jest warunkiem tworzenia „żywych” procedur, a nie dokumentów martwych – czego brak wprost ilustrują ustalenia NIK w odniesieniu do planów gminnych i wojewódzkich w badanych jednostkach^{517,518}. W drugim strumieniu kluczowe znaczenie ma reforma ochrony ludności i obrony cywilnej oparta na ustawie z 5 grudnia 2024 r. Ustawa wchodzi w życie zasadniczo 1 stycznia 2025 r., przy czym część przepisów wdrożeniowych zacznie obowiązywać 1 stycznia 2026 r., a kolejne mają harmonogram odroczonego⁵¹⁹.

Modernizacja systemu jest już nie tyle postulatem, ile procesem implementacji wymagającym zarządzania zmianą. Najbardziej „nośne” mechanizmy reformy – z punktu widzenia ulepszania realnej zdolności państwa – obejmują:

- Programowe sterowanie finansowaniem i priorytetami. Program Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 został zatwierdzony uchwałą Rady Ministrów i stanowi podstawę planowania działań oraz środków w pierwszej fazie funkcjonowania systemu⁵²⁰. W przepisach przejściowych ustawy wskazano, że pierwszy program jest podstawą finansowania realizacji zadań w latach 2025-2026⁵²¹. W ujęciu zarządczym przesuwamy to system z finansowania reaktywnego w stronę finansowania celowego, mierzalnego i priorytetyzowanego.
- Standaryzację i instytucjonalizację szkoleń. Ustawa zawiera przepisy dotyczące cyklu i adresatów szkoleń, a także wskazuje instytucję odpowiedzialną za szkolenia dla wybranych kategorii organów (w tym ministrów i wojewodów), którą jest Akademia Pożarnicza. Dla diagnostycznych problemów kompetencyjnych na poziomie lokalnym

⁵¹⁷ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Urząd Gminy Stare Miasto, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.03.2017; P.17.039, Poznań, 22.12.2017.

⁵¹⁸ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Małopolski Urząd Wojewódzki w Krakowie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LKR.410.016.01.2017, Kraków, 17.01.2018.

⁵¹⁹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

⁵²⁰ Uchwała nr 72 Rady Ministrów z dnia 27 maja 2025 r. w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 (M.P. 2025 poz. 541).

⁵²¹ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

jest to szczególnie istotne: reforma tworzy ramy do profesjonalizacji, która wcześniej była trudna do wymuszenia samym mechanizmem „obowiązku planu”.

- Budowę ewidencji i zasobów ochrony ludności. Ustawa przewiduje utworzenie centralnych ewidencji zasobów ochrony ludności i obrony cywilnej (oraz innych ewidencji systemowych) i nakłada harmonogram ich uruchomienia. Z perspektywy zarządzania kryzysowego ma to fundamentalne znaczenie dla świadomości sytuacyjnej i logistycznej: zasoby – aby były użyteczne – muszą być zinwentaryzowane, dostępne i możliwe do zadysponowania w czasie rzeczywistym.
- Zintegrowanie alarmowania i ostrzegania. Program OLiOC wskazuje, że ustawa reguluje zasady funkcjonowania systemów wykrywania zagrożeń oraz powiadamiania, ostrzegania i alarmowania⁵²².

W praktyce należy to łączyć z rozwijaniem już istniejących narzędzi, takich jak Alert RCB, który według RCB działa bez rejestracji, na obszarze określonym przez dyrektora RCB, a wiadomości są wysyłane tylko w sytuacjach realnego zagrożenia życia i zdrowia. Niezależnie od reformy ustawowej, polski system powinien równolegle domykać wymagania europejskie dotyczące public warning. Europejski Kodeks Łączności Elektronicznej przewiduje obowiązek zapewnienia systemu publicznego ostrzegania⁵²³, co w praktyce sprzyja wdrażaniu rozwiązań geotargetowanych oraz odpornych na przeciążenia sieci (np. broadcast). W logice doskonalenia oznacza to dążenie do architektury wielokanałowej: SMS (Alert RCB), media, syreny, systemy ostrzegania i komunikaty – spójne proceduralnie i testowane, a nie zestaw niepołączonych narzędzi.

W perspektywie wdrożeniowej (krótko- i średniookresowej) najbardziej krytyczne są trzy zadania zarządcze:

- Zamknięcie luki „centrum-teren” poprzez ujednolicenie standardów pracy centrów zarządzania kryzysowego (dyżury, obsada, łączność zapasowa, procedury eskalacji) i formalne egzekwowanie cyklu

⁵²² Uchwała nr 72 Rady Ministrów z dnia 27 maja 2025 r. w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 (M.P. 2025 poz. 541).

⁵²³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.U. L 321 z 17.12.2018, s. 36-214).

aktualizacji planów, aby uniknąć sytuacji opisanych w dokumentach pokontrolnych^{524,525}.

- Integracja danych i interoperacyjność instytucjonalna, w szczególności rozwój ewidencji i reguł współdzielenia informacji o zasobach, obiektach ochronnych i potrzebach wrażliwych grup, co jest obecnie wspierane przez instrumenty przewidziane w ustawie⁵²⁶.
- Przesunięcie ciężaru z reakcji na prewencję i odporność, zwłaszcza w obszarach klimatycznych (adaptacja, planowanie przestrzenne, infrastruktura deszczowa i przeciwpowodziowa) oraz w obszarach ciągłości usług krytycznych, zgodnie z logiką Sendai⁵²⁷ i ujęciem odpornościowym NATO⁵²⁸.

⁵²⁴ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Urząd Gminy Stare Miasto, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.03.2017; P.17.039, Poznań, 22.12.2017.

⁵²⁵ Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Małopolski Urząd Wojewódzki w Krakowie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LKR.410.016.01.2017, Kraków, 17.01.2018.

⁵²⁶ Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).

⁵²⁷ United Nations (UN), Sendai Framework for Disaster Risk Reduction 2015-2030 (A/RES/69/283), 2015.

⁵²⁸ NATO, Resilience, civil preparedness and Article 3 (Baseline Requirements: continuity of government, essential services, civil support to the military), 2024.

Podsumowanie

Monografia, oparta na analizie literatury przedmiotu, dokumentów normatywnych i strategicznych, a także na wnioskach wynikających z doświadczeń funkcjonowania instytucji publicznych, ukazuje zarządzanie kryzysowe nie jako zbiór doraźnych reakcji, lecz jako spójny cykl działań obejmujący prewencję, przygotowanie, reagowanie, odbudowę oraz uczenie się systemu po zdarzeniu. W pierwszej perspektywie – systemowej – monografia wykazuje, że bezpieczeństwo narodowe należy rozumieć jako proces wielowymiarowy, obejmujący nie tylko wymiar militarny, lecz także polityczny, społeczny, ekonomiczny, informacyjny i środowiskowy. Zastosowanie podejścia systemowego pozwala uchwycić współzależności między podsystemem kierowania, podsystemami wykonawczymi (operacyjnymi) oraz podsystemami wsparcia, a także znaczenie relacji między instytucjami państwa i podmiotami pozapaństwowymi (operatorami usług kluczowych, sektorem prywatnym, organizacjami pozarządowymi). Szczególnie istotne jest wskazanie, że współczesne zagrożenia – zwłaszcza hybrydowe, cybernetyczne i informacyjne – w praktyce zacierają tradycyjny podział na bezpieczeństwo wewnętrzne i zewnętrzne, co wymusza koordynację działań i interoperacyjność kompetencji w skali całego państwa.

W perspektywie pojęciowo-instytucjonalnej monografia porządkuje aparat terminologiczny i wskazuje zarządzanie kryzysowe jako kategorię łączącą dorobek nauk o bezpieczeństwie, zarządzania, prawa i polityk publicznych. Zaprezentowana geneza i ewolucja zarządzania kryzysowego (w Polsce i ujęciu międzynarodowym) prowadzi do wniosku, że dominującym kierunkiem rozwoju jest przejście od logiki reaktywnej ku logice zarządzania ryzykiem oraz budowania odporności (resilience). Jednocześnie wykazano, że skuteczność systemu zależy od klarowności ram prawnych i kompetencyjnych, w tym od relacji pomiędzy reżimem „zwykłego” zarządzania

kryzysowego a instrumentami właściwymi stanom nadzwyczajnym. W tym kontekście szczególne znaczenie mają: wieloszczeblowość systemu, rola administracji publicznej jako organizatora i koordynatora, a także zasady organizacyjne (m.in. subsydiarność, jednoosobowe kierownictwo, odpowiedzialność organów, zespolenie, powszechność/partycypacja oraz jawność i komunikacja), które determinują sprawność działania w warunkach presji czasu i niepewności informacyjnej.

Trzon analityczny monografii stanowi omówienie faz i procesów zarządzania kryzysowego. Wskazano, że fundamentem całego cyklu jest identyfikacja zagrożeń i ocena ryzyka, rozumiana jako wieloźródłowe rozpoznanie potencjalnych zdarzeń oraz ich hierarchizacja na podstawie prawdopodobieństwa i skutków. Podkreślono znaczenie metod analitycznych (analizy danych historycznych i trendów, scenariuszy, map ryzyka, baz danych, systemów monitorowania), a także roli narzędzi typu macierz ryzyka w porządkowaniu priorytetów planistycznych. W fazie planowania i przygotowania zaakcentowano wagę dokumentów planistycznych wszystkich szczebli (krajowego, wojewódzkiego, powiatowego i gminnego) oraz konieczność ich realnej użyteczności operacyjnej: plany mają pełnić funkcję narzędzia działania (scenariusze, matryce odpowiedzialności, zasoby, procedury), a nie wyłącznie formalnego wymogu. W fazie reagowania szczegółowo omówiono mechanizmy kierowania działaniami, koordynacji służb, ewakuacji, ochrony infrastruktury krytycznej i porządku publicznego, ze wskazaniem na specyfikę decyzji podejmowanych pod presją czasu i w warunkach niepełnej informacji. Wreszcie, w obszarze odbudowy i odtwarzania uwypuklono wielowymiarowość recovery (infrastrukturalną, gospodarczą i psychospołeczną) oraz rosnące znaczenie podejścia „build back better”, łączącego rekonstrukcję z redukcją przyszłego ryzyka. Cykl domyka faza doskonalenia systemu: mechanizmy analizy po zdarzeniu (AAR), zarządzania wiedzą, wdrażania wniosków do planów, szkoleń i – w razie potrzeby – zmian organizacyjnych oraz legislacyjnych.

W obszarze instrumentów i narzędzi monografia wskazuje, że współczesne zarządzanie kryzysowe coraz silniej opiera się na infrastrukturze informacyjnej: systemach teleinformatycznych, bazach danych, narzędziach analitycznych, a także na zdolnościach centrów zarządzania kryzysowego do pracy w trybie całodobowym. Szczególną rolę przypisano systemom

ostrzegania i alarmowania ludności (syreny, kanały medialne, narzędzia mobilne), podkreślając, że skuteczność ostrzegania zależy nie tylko od technologii, lecz także od procedur, jakości komunikatów i edukacji społecznej. Równocześnie zaakcentowano znaczenie nowych technologii – m.in. GIS, dronów oraz analityki danych – w budowaniu świadomości sytuacyjnej, wsparciu decyzyjnym i koordynacji działań, przy jednoczesnym wskazaniu na ryzyka wynikające z cyfryzacji (zależność od sieci, podatność na incydenty cybernetyczne). Uzupełnieniem obrazu narzędziowego jest logistyka kryzysowa i planowanie zasobów, obejmujące inwentaryzację sił i środków, procedury dysponowania oraz współpracę z sektorem prywatnym w warunkach zakłóconych łańcuchów dostaw. W tym wymiarze monografia pokazuje również komplementarność zarządzania kryzysowego i podejścia ciągłościowego (BCP/BCMS), wskazując na znaczenie standardów i testowania planów ciągłości działania dla utrzymania usług krytycznych.

W wymiarze wieloszczeblowym i międzynarodowym monografia dowodzi, że skuteczność polskiego systemu jest warunkowana nie tylko rozwiązaniami krajowymi, lecz także zdolnością do współdziałania z mechanizmami ponadpaństwowymi oraz do uczenia się z doświadczeń innych państw. Analiza roli samorządu terytorialnego oraz szczebla wojewódzkiego i centralnego prowadzi do wniosku, że kluczowym problemem praktycznym bywa „spięcie” poziomów systemu: zapewnienie spójności planowania, standardów dyżurowych, procedur eskalacji i przepływu informacji w relacji centrum-teren. Z kolei omówienie instrumentów Unii Europejskiej i NATO wskazuje na rosnące znaczenie odporności i cywilnej gotowości (continuity of essential services), a także na potrzebę integrowania krajowych rozwiązań ostrzegania, reagowania i odbudowy z ramami współpracy międzynarodowej, w tym w obszarze wsparcia transgranicznego i koordynacji operacyjnej.

Wnioski prospektywne monografii akcentują, że środowisko bezpieczeństwa wchodzi w fazę trwałej wielozagrożeńowości, w której najsilniejsze presje na system zarządzania kryzysowego wynikają z trzech nakładających się megatrendów: zmian klimatu, zwiększających częstość i intensywność ekstremów pogodowych; transformacji technologicznej, która jednocześnie poszerza możliwości monitoringu i analityki, lecz zwiększa podatność na zdarzenia cybernetyczne; oraz pogorszenia środowiska bezpieczeństwa międzynarodowego, w tym wzrostu znaczenia zagrożeń

hybrydowych. W tej perspektywie zarządzanie kryzysowe powinno być rozwijane jako system oparty na zarządzaniu ryzykiem, planowaniu zdolności, interoperacyjności instytucjonalnej i budowaniu odporności społecznej.

W części syntetyzującej kierunki doskonalenia polskiego systemu podkreślono dwa komplementarne strumienie zmian: z jednej strony podnoszenie dojrzałości klasycznego zarządzania kryzysowego (procedury, egzekwowanie cyklu aktualizacji, gotowość 24/7, interoperacyjność), z drugiej – konsekwentną implementację rozwiązań ochrony ludności i obrony cywilnej w nowym modelu normatywnym, w tym porządkowanie finansowania programowego, standaryzację szkoleń, budowę ewidencji zasobów i integrację systemów ostrzegania. W wymiarze wdrożeniowym jako szczególnie krytyczne wskazano: zamknięcie luki „centrum-teren” poprzez ujednolicanie standardów pracy centrów zarządzania kryzysowego oraz formalne wzmacnianie dyscypliny planistycznej; integrację danych i reguł współdzielenia informacji o zasobach i potrzebach (w tym grup wrażliwych); przesunięcie ciężaru działań z reakcji na prewencję i odporność, zwłaszcza w obszarze adaptacji klimatycznej, planowania przestrzennego, infrastruktury przeciwpowodziowej i zapewnienia ciągłości usług krytycznych.

Całościowo monografia potwierdza, że skuteczny system zarządzania kryzysowego jest w istocie systemem dynamicznym: wymaga równoczesnego rozwijania zdolności analitycznych (rozpoznanie i ocena ryzyka), planistycznych (procedury i zasoby), operacyjnych (reagowanie i koordynacja), odtworzeniowych (odbudowa) oraz poznawczo-uczących (lessons learned). W warunkach rosnącej złożoności zagrożeń kluczowa staje się zdolność do integracji: integracji instytucji, danych, narzędzi, standardów działania i komunikacji z obywatelami. Z tego powodu zarządzanie kryzysowe należy traktować nie jako domenę wąsko rozumianego reagowania, lecz jako element polityki bezpieczeństwa i odporności państwa – rozwijany systemowo, testowany w ćwiczeniach, aktualizowany na podstawie doświadczeń oraz osadzony w współpracy krajowej i międzynarodowej.

Literatura

1. Abgarowicz, I., Plasota, T., Napiórkowski, M., Nowoczesne technologie wspierające raportowanie o zagrożeniach na potrzeby systemu zarządzania kryzysowego RP, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Administracyjne, 882, 7, 2015, s. 104-118. <https://doi.org/10.18276/sa.2015.7-06>
2. Aldrich, D. P., Building Resilience: Social Capital in Post-Disaster Recovery, Chicago, University of Chicago Press, 2012. <https://doi.org/10.7208/chicago/9780226012896.001.0001>
3. Alexander, D., Principles of Emergency Planning and Management, New York, Oxford University Press, 2002.
4. Akter, S., Wamba, S. F., Big data and disaster management: a systematic review and agenda for future research, Annals of Operations Research, 283(1), 2019, s. 939-959. <https://doi.org/10.1007/s10479-017-2584-2>
5. AnonMoos, Poland borders, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Poland_borders.svg, [dostęp: 10.10.2025].
6. Armstrong, M., Jak być lepszym menedżerem, Warszawa, Dom Wydawniczy ABC, 1997.
7. Bednarski, A., Rola Policji w zabezpieczeniu mienia w sytuacjach kryzysowych, w: Wyzwania bezpieczeństwa wewnętrznego, Dobek, K. (red.), Warszawa, Wyższa Szkoła Policji w Szczytnie, 2018.
8. Beiser, V., Organizing Armageddon: What We Learned From the Haiti Earthquake, Wired, <https://www.wired.com/2010/04/ff-haiti/>, [dostęp: 30.09.2025].
9. Bieńkowska, A., Kral, Z., Zabłocka-Kluczka, A., Istota i ewolucja zarządzania kryzysowego, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, 1092, 2005, s. 25-32.
10. Biuro Bezpieczeństwa Narodowego, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2013.
11. Biuro Bezpieczeństwa Narodowego, Biuro Bezpieczeństwa Narodowego 2015-2025, Warszawa, BBN, 2025.

12. Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa, BBN, 2020.
13. Boin, A., 't Hart, P., Stern, E., Sundelius, B., *The Politics of Crisis Management: Public Leadership under Pressure*, Cambridge, Cambridge University Press, 2005. <https://doi.org/10.1017/CBO9780511490880>
14. Borodzicz, E., *Risk, Crisis and Security Management*, Chichester, John Wiley & Sons, 2005.
15. Bourbeau, P., Resiliencism and security studies: initiating a dialogue, w: *Contesting Security: Strategies and Logics*, Balzacq, T. (red.), London-New York, Routledge, 2014, s. 1-15.
16. Brązkiewicz, D., Chodyka, M., Grudniewski, T., Nowicka, J. (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część pierwsza, Biała Podlaska*, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103199>
17. Brązkiewicz, D., Chodyka, M., Grudniewski, T., Żurawski, S., *Wielowymiarowość środowiska bezpieczeństwa. Część druga, Biała Podlaska*, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103205>
18. Broughton, E., The Bhopal disaster and its aftermath: a review, *Environmental Health*, 4(1), 6, 2005. <https://doi.org/10.1186/1476-069X-4-6>
19. Budzisz, R., *Centra zarządzania kryzysowego w systemie bezpieczeństwa wewnętrznego państwa*, Warszawa, Wydawnictwo Szkoły Głównej Służby Pożarniczej, 2020.
20. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Warn-App NINA, https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html, [dostęp: 22.09.2025].
21. Buzan, B., Wæver, O., de Wilde, J., *Security: A New Framework for Analysis*, Boulder (CO), Lynne Rienner Publishers, 1998. <https://doi.org/10.1515/9781685853808>
22. Cabaj, M., Zarządzanie kryzysowe – integralna część bezpieczeństwa narodowego, *Studia z zakresu prawa, administracji i zarządzania UKW*, 6, 2014, s. 101-113.
23. Case, J. H., *From Satellites to Survivors: How GIS Powers Disaster Response*, Team Rubicon, <https://teamrubiconusa.org/news-and-stories/gis-disaster-response>, [dostęp: 22.09.2025].
24. Centre for Research on the Epidemiology of Disasters (CRED), *Cred Crunch*, Issue no. 62: Disaster Year in Review 2020, EM-DAT/CRED – UCLouvain, Brussels, 2021.

25. Centre for Research on the Epidemiology of Disasters (CRED), EM-DAT: międzynarodowa baza danych o katastrofach (opis w portalu Climate-ADAPT), European Environment Agency, 2022.
26. Centrum Badania Opinii Społecznej (CBOS), Zaufanie społeczne, Komunikat z badań nr 40/2024, Warszawa, 2024.
27. Chapman, A., Leveraging Big Data and AI for Disaster Resilience and Recovery, Texas A&M University College of Engineering News, <https://engineering.tamu.edu/news/2023/06/leveraging-big-data-and-ai-for-disaster-resilience-and-recovery.html>, [dostęp: 22.09.2025].
28. Chodyka, M., Ciekanowski, Z., Ochrona młodych użytkowników Internetu przed cyberzagrożeniami we współczesnym cyfrowym świecie, Przegląd Naukowo-Metodyczny. Edukacja dla bezpieczeństwa, 2025, XVIII, 2(67), s. 159-168.
29. Chodyka, M., Ciekanowski, Z., Analiza treści audiowizualnych jako element systemów bezpieczeństwa państwa, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2024.
30. Chodyka, M., Żurawski, S., Wojciechowska-Filipek, S., Ciekanowski, Z., Mazur, S., Critical Infrastructure Security Management in the Era of Cyber Threats, European Research Studies Journal, 2025, 28(2), s. 610-621. <https://doi.org/10.35808/ersj/4000>
31. Chruzik, K., Zarządzanie ryzykiem w sytuacjach kryzysowych, Journal of KON-BiN, 49(4), 2019, s. 261-273. <https://doi.org/10.2478/jok-2019-0085>
32. Ciupiński, A., Paradygmat kooperacyjnego bezpieczeństwa, w: Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej, Ciupiński, A. (red.), Akademia Obrony Narodowej, 2010.
33. Ciekanowski, Z. (red.), Infrastruktura bezpieczeństwa publicznego: ogólnokrajowe i lokalne wyzwania cywilizacyjne, Warszawa, Wyższa Szkoła Zarządzania i Prawa, 2010.
34. Ciekanowski, Z., Błaszczak, B., Malinowska, I., System zarządzania kryzysowego NATO a zagrożenia hybrydowe, Prawo i Bezpieczeństwo – Law & Security, 1(2), 2024, s. 7-19. <https://doi.org/10.4467/29567610PIB.24.001.19837>
35. Ciekanowski, Z., Człowiek wobec współczesnych zagrożeń bezpieczeństwa państwa, Studia Bezpieczeństwa Narodowego, 11(1), 2017, s. 31-52. <https://doi.org/10.37055/sbn/129880>
36. Ciekanowski, Z., Nowicka, J., Wyrębek, H., Bezpieczeństwo państwa w obliczu współczesnych zagrożeń, Siedlce, Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, 2016.

37. Ciekanowski, Z., Nowicka, J., Wyrębek, H., Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych, Warszawa, CeDeWu, 2017.
38. Ciekanowski, Z., Krysiński, S., Zarządzanie kryzysowe w Polsce w sytuacjach zagrożeń niemilitarnych jako sposób umacniania państwa, Wydawnictwo Państwowej Wyższej Szkoły Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza, 2014.
39. Ciekanowski, Z., Żurawski, S., Zarządzanie kryzysowe na szczeblu samorządowym na przykładzie gmin powiatu przemyskiego, Warszawa, Wydawnictwo im. Profesora Leszka J. Krzyżanowskiego Menadżerskiej Akademii Nauk Stosowanych w Warszawie, 2022, s. 14.
40. Cieślarczyk, M., Kultura bezpieczeństwa i obronności, Siedlce, Wydawnictwo Akademii Podlaskiej, 2007.
41. Clarke, M., Charakterystyka zachowania się w kryzysie (maszynopis wykładu wygłoszonego w Brukseli), 1995.
42. Comfort, L. K., Birkland, T. A., Cigler, B. A., Nance, E., Retrospectives and Prospectives on Hurricane Katrina: Five Years and Counting, *Public Administration Review*, 70(5), 2010, s. 669-678.
43. Coombs, W. T., *Ongoing crisis communication: planning, managing, and responding*, 4th ed., Thousand Oaks (CA), Sage, 2015.
44. Crandall, W., Menefee, M. L., Crisis Management in the Midst of Labor Strife: Preparing for the Worst, *S.A.M. Advanced Management Journal*, 61(1), 1996.
45. Dalton, D., Three Mile Island Led To "Sweeping And Permanent" Changes, *NucNet Bulletin*, 23.03.2009.
46. Domański, P., Gwałtowne zjawiska pogodowe w sierpniu 2017 – działania ratownicze i zarządzanie kryzysowe, *Biuletyn Kwartalny Biura Analiz i Regagowania RCB*, 20, s. 16-18. <https://archiwum.rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-20-kopia.pdf>, [dostęp: 10.10.2025].
47. DRIVER+, Common Information Space (CIS) – narzędzie wymiany danych w zarządzaniu kryzysowym, 2025, <https://tgm.ercis.org/pl/metody-i-narzedzia/common-information-space>, [dostęp: 22.09.2025].
48. Dyner, A. M., The Border Crisis as an Example of Hybrid Warfare, *Polski Instytut Spraw Międzynarodowych (PISM)*, 02.02.2022, 2022.
49. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.U. UE L 321 z 17.12.2018, s. 36-214).
50. Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS2) (Dz. Urz. UE L 333 z 27.12.2022).

51. Dyrektywa (UE) 2022/2557 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych oraz uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022).
52. ECMWF Newsletter, The European Flood Awareness System (EFAS) at ECMWF: towards operational implementation, ECMWF Newsletter, No. 131, Spring 2012.
53. Edwards, C., Hurricane Katrina: Remembering the Federal Failures, Cato Institute, Cato at Liberty, 2015.
54. Esri, ArcGIS Solutions: Introduction to Know Your Zone, <https://doc.arcgis.com/en/arcgis-solutions/latest/reference/introduction-to-know-your-zone.htm>, [dostęp: 22.09.2025].
55. ETSI, ETSI TS 102 900: European Public Warning Service (EU-Alert) using Cell Broadcast, ETSI, 2023.
56. European External Action Service, Countering Hybrid Threats, 2022.
57. European Parliamentary Research Service (EPRS), Japan's disaster risk reduction and preparedness – selected solutions, European Parliament, 2025, [dostęp: 10.10.2025].
58. Europejski Trybunał Obrachunkowy, Instytucje UE a pandemia COVID19. Reakcja była szybka, ale wciąż istnieją wyzwania, jak w optymalny sposób wykorzystać innowacje i elastyczność będące wynikiem kryzysu, Sprawozdanie specjalne nr 18/2022, Luksemburg, 2022. <https://doi.org/10.2865/116653>
59. Fagel, M. J., Crisis management and emergency planning: preparing for today's challenges, Boca Raton, CRC Press, 2014. <https://doi.org/10.1201/b16072>
60. Falecki, J., Organizacja gier decyzyjnych w zarządzaniu kryzysowym, Sosnowiec, Oficyna Wydawnicza Humanitas, 2016.
61. Federal Communications Commission, Wireless Emergency Alerts (WEA), <https://www.fcc.gov/consumers/guides/wireless-emergency-alerts>, [dostęp: 22.09.2025].
62. Federal Emergency Management Agency, Community Emergency Response Team (CERT). Basic Training: Participant Manual, National CERT Program, 2011, https://www.fema.gov/sites/default/files/2020-07/fema-cert_basic-training-participant-manual_01-01-2011.pdf#page=1&zoom=auto,-263,798, [dostęp: 10.10.2025].
63. Federal Emergency Management Agency, National Disaster Recovery Framework, 2011, <https://www.fema.gov/pdf/recoveryframework/ndrf.pdf#page=1&zoom=auto,-263,552>, [dostęp: 22.09.2025].
64. Federation of European Risk Management Associations (FERMA), A Risk Management Standard, FERMA/AIRMIC/ALARM, Bruksela, 2002.

65. Fenigstein, M., Doskonalenie procesu decyzyjnego w sytuacjach kryzysowych poprzez gry decyzyjne, *Zeszyty Naukowe Akademii Obrony Narodowej*, 2(119), 2020, s. 45-59.
66. Ferris-Rotman, A., How drones are helping Nepal recover from the earthquake, *Huffington Post*, https://www.huffpost.com/entry/nepal-earthquake-drones_n_7232764, [dostęp: 22.09.2025].
67. Filipek, A., Gałek, C., Istota kultury bezpieczeństwa i jej znaczenie dla człowieka i grup społecznych, *Kultura Bezpieczeństwa*, 2014, s. 17-57.
68. Fink, S., *Crisis Management. Planning for the Inevitable*, An Authors Guild Backinprint.com Edition, Lincoln, iUniverse.com, Inc., 2000.
69. FSD (Fondation Suisse de Déminage), *Drones in Humanitarian Action – A Guide to the Use of Airborne Systems in Humanitarian Crises*, Swiss Foundation for Mine Action, <https://www.updwg.org/wp-content/uploads/2019/04/Drones-in-Humanitarian-Action.pdf#page=3&zoom=auto,-272,559>, [dostęp: 22.09.2025].
70. Fraunhofer FOKUS / KATWARN, KATWARN – warning system (public warnings and behavioural advice), https://www.fokus.fraunhofer.de/en/espri/projects/en_katwarn.html, [dostęp: 22.09.2025].
71. Goraj, J., Społeczna odporność – obywatel jako uczestnik systemu bezpieczeństwa, *Stowarzyszenie Świadoma Obrona Cywilna*, <https://swiadomaoc.org/spoleczna-odpornosc-obywatel-jako-uczestnik-systemu-bezpieczenstwa>, [dostęp: 22.09.2025].
72. Grudniewski, T. M., Czernastek, M., Lasek-Surowiec, I., Franelak, M., Bezpieczeństwo energetyczne w regionach przygranicznych Polski, w: *Ochrona granicy Rzeczypospolitej Polskiej w dobie współczesnych zagrożeń bezpieczeństwa*, red. S. Żurawski, M. Oskierko, T. Grudniewski, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025, s. 283-294. https://doi.org/10.29316/9788368103236_17
73. Gryz, J., Kitler, W. (red.), *System reagowania kryzysowego*, Toruń, Wydawnictwo Adam Marszałek, 2007.
74. Güreşci, H., Arpat, R. S., Usage of Social Network Analysis (SNA) in Crisis Management, *Journal on Baltic Security*, 2016, s. 72-88.
75. Hermann, C., Some Consequences of Crisis Which Limit the Viability of Organizations, *Administrative Science Quarterly*, 8(1), 1963, s. 61-82. <https://doi.org/10.2307/2390887>
76. Holser, M., *The Importance of GIS in Emergency Management*, *Environmental Law Journal* (Environmental Law Review Syndicate – Scholarship), New York University School of Law, 2016.

77. Hsu, E. B., Community Empowerment Strategies for Disaster Resilience, *Journal of Homeland Security and Emergency Management*, 13(3), 2016, s. 347-367.
78. Iannuli, F. EU Civil Protection Mechanism: History and Perspectives, TEMA Project, 11.05.2023, <https://tema-project.eu/articles/eu-civil-protection-mechanism-history-and-perspectives>, [dostęp: 22.09.2025].
79. IBRiS, Kryzys zaufania do instytucji. Kto zyskuje, a kto traci?, <https://ibris.pl/kryzys-zaufania-do-instytucji-kto-zyskuje-a-kto-traci/>, [dostęp: 10.10.2025].
80. Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy (IMGWPIB), *Klimat Polski 2024 (raport)*, 2025.
81. IPCC, *Climate Change 2022: Impacts, Adaptation and Vulnerability. Working Group II Contribution to the Sixth Assessment Report – Chapter 13: Europe*, 2022.
82. IPCC, *Zmiana klimatu 2021: Podstawy fizyczne. Wkład Grupy Roboczej I do Szóstego Raportu Oceniającego Genewa*, IPCC, 2021.
83. Ipsos, *Zaufanie do ludzi w Polsce i na świecie*, Ipsos Global Advisor, 2022, <https://www.ipsos.com/pl-pl/zaufanie-do-ludzi-w-polsce-i-na-swiecie>, [dostęp: 10.10.2025].
84. Jaślan, M., W 2024 r. liczba cyberataków na Polskę może przekroczyć 100 tys. TELKO, 2024, <https://www.telko.in/w-2024-r-liczba-cyberatakow-na-polske-moze-przekroczyc-100-tys-2>, [dostęp: 10.10.2025].
85. Kaczmarczyk, B. (red.), *Zarządzanie kryzysowe w Polsce i w państwach sąsiednich*, Wrocław, Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki, 2017.
86. Kapucu, N., Dougherty, R. B., Hu, Q., Network Governance for Coordinated Disaster Response, *Public Administration Quarterly*, 46(4), 2022, s. 309-333. <https://doi.org/10.37808/paq.46.4.2>
87. Kąkol, U., Marczewski, M., Metody analizy i oceny ryzyka stosowane w zarządzaniu kryzysowym na poziomie gminnym, *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, 11(959), 2016, s. 53-69. <https://doi.org/10.15678/ZNUEK.2016.0959.1104>
88. Keplin, J. Ł., Budowanie odporności państwa na działania hybrydowe, *Przegląd Bezpieczeństwa Wewnętrznego*, 15(29), 2023. <https://doi.org/10.4467/20801335PBW.23.018.18760>
89. Kielczykowska, A., *Badanie: 73 proc. Polaków uważa, że w mediach społecznościowych celowo rozprzestrzeniane są nieprawdziwe lub niedokładne informacje*, Nauka w Polsce – PAP, 2022.

90. Kitler, W., Bezpieczeństwo wewnętrzne w świetle współczesnych wyzwań teorii i praktyki problemu, *Wiedza Obronna*, 282(1), 2023, s. 117-148. <https://doi.org/10.34752/2023-f282>
91. Kitler, W., System bezpieczeństwa narodowego RP – aspekty prawnoorganizacyjne, *Wiedza Obronna*, 268(3), 2019, s. 5-33.
92. KG PSP, Krajowy system ratowniczo-gaśniczy (KSRG), <https://www.gov.pl/web/kgpsp/ksrg>, [dostęp: 10.10.2025].
93. KG PSP, Wyższy Kursu Ochrony Ludności dla osób pełniących funkcje ministrów, sekretarzy stanu, podsekretarzy stanu i kierowników urzędów centralnych (WKOL-C), <https://www.gov.pl/web/kgpsp/wyzszy-kursu-ochrony-ludnosci-dla-osob-pelniacych-funkcje-ministrow-sekretarzy-stanu-podsekretarzy-stanu-i-kierownikow-urzedow-centralnych-wkol-c>, [dostęp: 10.10.2025].
94. Klein, G., *Sources of Power: How People Make Decisions*, Cambridge (MA), MIT Press, 1998.
95. Komisja Europejska, EU Security Union Strategy (COM/2020/605 final), 2020.
96. Komisja Europejska, EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises – Blueprint (EU Cybersecurity Blueprint), Bruksela, 2017.
97. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).
98. Kopaliński, W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa, 1968, s. 417.
99. Kożuch, B., Sienkiewicz-Małyjurek, K., Kożuch, A. J., Communication in local emergency management networks (Part 2), *International Journal of Contemporary Management*, 14(1), 2015, s. 91-104.
100. Krystek, U., *Unternehmungskrisen. Beschreibung, Vermeidung und Bewältigung überlebenskritischer Prozesse in Unternehmungen*, Wiesbaden, Gabler GmbH, 1987.
101. Kuziemski, M., Misuraca, G., AI governance in the public sector: Three tales from the frontiers of automated decisionmaking in democratic settings, *Telecommunications Policy*, 44(6), 101976, 2020. <https://doi.org/10.1016/j.telpol.2020.101976>
102. Leszczyńska, A., Wybrane uwarunkowania odbudowy organizacji po wystąpieniu klęsk, *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, 2018, s. 273-285.
103. Leśniakiewicz, W., Strażacy o powodzi: 19 ofiar, 30 tys. ewakuowanych (wypowiedź Komendanta Głównego PSP; dane o zaangażowaniu: 17 tys. strażaków, 13 tys. policjantów, 8 tys. żołnierzy), depesza PAP, 17.06.2010, 2010.

104. Lidwa, W., Krzeszowski, W., Więcek, W., Zarządzanie w sytuacjach zagrożeń niemilitarnych, Warszawa, Akademia Obrony Narodowej, 2010.
105. Majcher, P., Alert RCB – dotychczasowe doświadczenia, Biuletyn kwartalny Rządowego Centrum Bezpieczeństwa (Biuro Analiz i Reagowania), nr 29 (październik-grudzień 2019), 2020.
106. Majchrzak, D., Michalski, K., Reginia-Zacharski, J., Readiness of the Polish Crisis Management System to Respond to Long-Term, Large-Scale Power Shortages and Failures (Blackouts), *Energies*, 14(24), 8286, 2021, s. 1-33. <https://doi.org/10.3390/en14248286>
107. Makinoshima, F., Yotsui, S., Sato, S., Imamura, F., Large-scale geolocation data reveal evacuation behaviour during the 2024 Noto Peninsula earthquake and tsunami, *Communications Earth & Environment*, 6, 891, 2025. <https://doi.org/10.1038/s43247-025-02819-8>
108. Marjak, H., Potencjał i rola mediów społecznościowych w zarządzaniu kryzysowym, *Zeszyty Naukowe Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej*, 2, 2019.
109. Maślanka, Ł., Szymański, P., Odporność Unii Europejskiej i NATO w dobie multikryzysu, *Komentarze OSW*, nr 646, Warszawa, Ośrodek Studiów Wschodnich im. Marka Karpia, 2025.
110. Ministerstwo Spraw Wewnętrznych i Administracji, Modernizujemy system alarmowy – ponad 4 tys. lokalizacji z nowoczesnymi syrenami, gov.pl, <https://www.gov.pl/web/obrona-cywilna/modernizujemy-system-alarmowy--ponad-4-tys-lokalizacji-z-nowoczesnymi-syrenami>, [dostęp: 31.10.2025].
111. Ministerstwo Spraw Wewnętrznych i Administracji, Regionalny System Ostrzegania, <https://www.gov.pl/web/mswia/regionalny-system-ostrzegania>, [dostęp: 22.09.2025].
112. Ministerstwo Środowiska, Strategiczny plan adaptacji dla sektorów i obszarów wrażliwych na zmiany klimatu do roku 2020 z perspektywą do roku 2030 (SPA 2020), 2013 (przyjęty przez RM 29.10.2013).
113. Mitchell, A., Risk and Resilience: From Good Idea to Good Practice, OECD Development Cooperation Working Papers, nr 13, Paris, OECD Publishing, 2013. <https://doi.org/10.1787/5k3ttg4cxcbp-en>
114. Molek, W., Stec, K., Marciniak, R., Zarządzanie kryzysowe w systemie kierowania bezpieczeństwem narodowym, *Bezpieczeństwo Narodowe*, 17, 2011, s. 45-60.
115. Mooney, M. F., Paton, D., de Terte, I., Johal, S., Karanci, A. N., Psychosocial Recovery from Disasters: A Framework Informed by Evidence, *New Zealand Journal of Psychology*, 40(4), 2011, s. 26-38.

116. Najwyższa Izba Kontroli (NIK), Hybrydowe zagrożenie – przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi (wyniki kontroli), Warszawa, NIK, 2023.
117. Najwyższa Izba Kontroli (NIK), Informacja o wynikach kontroli: Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej (Nr P/17/039; nr ewid.: P/17/039 (KPB.430.009.2017; Nr ewid. 147/2018/P/17/039/KPB)), Warszawa, NIK, 2019.
118. Najwyższa Izba Kontroli (NIK), Informacja o wynikach kontroli: Realizacja przez administrację publiczną województwa podkarpackiego zadań z zakresu infrastruktury przeciwpowodziowej (kontrola P/15/097; Nr ewid. 185/2015/P/15/097/LRZ; LRZ410.004.2015), Delegatura NIK w Rzeszowie, marzec 2016, s. 5, 16.
119. Najwyższa Izba Kontroli (NIK), NIK: gminy i powiaty nieprzygotowane organizacyjnie na sytuacje kryzysowe, Serwis Samorządowy PAP, 2019.
120. Najwyższa Izba Kontroli (NIK), Przygotowanie państwa na zagrożenia hybrydowe (synteza wyników kontroli), Warszawa, NIK, 2023.
121. Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Małopolski Urząd Wojewódzki w Krakowie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LKR.410.016.01.2017, Kraków, 17.01.2018.
122. Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Starostwo Powiatowe w Koninie, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.02.2017, Poznań, 18.01.2018.
123. Najwyższa Izba Kontroli (NIK), Wystąpienie pokontrolne: Urząd Gminy Stare Miasto, kontrola P/17/039, Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej, sygn. LPO.410.017.03.2017; P.17.039, Poznań, 22.12.2017.
124. Nalepa, P., Obrona Cywilna dziś – stan, wyzwania, perspektywy, Warszawa, Bellona, 2019.
125. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), dokument rządowy przyjęty uchwałą Rady Ministrów z dnia 26 marca 2013 r., 2013.
126. Narodowy Program Ochrony Infrastruktury Krytycznej, przyjęty uchwałą Rady Ministrów, Warszawa, Rządowe Centrum Bezpieczeństwa, 2020.
127. NATO, Crisis management, NATO, 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/crisis-management>, [dostęp: 22.09.2025].
128. NATO, Resilience, civil preparedness and Article 3 (Baseline Requirements: continuity of government, essential services, civil support to the military), 2024.
129. NATO, Strategic Concept (Madryt, 29.06.2022), 2022.

130. Negi, S., Humanitarian logistics challenges in disaster relief operations: A humanitarian organisations' perspective, *Journal of Transport and Supply Chain Management*, 16, 2022, e1167. <https://doi.org/10.4102/jtscm.v16i0.691>
131. Nowak, A., Rola i zadania Wojewódzkiego Centrum Zarządzania Kryzysowego, *Zeszyty Naukowe WSOSP*, 4, 2019, s. 67-80.
132. Nowak, E., Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych, Warszawa, Akademia Obrony Narodowej, 2007.
133. Nowicka, J., Chodyka, M., Chodkowski, R. (red.), Wyzwania w obszarze komunikacji i bezpieczeństwa, Biała Podlaska, Wydawnictwo Akademii Białskiej im. Jana Pawła II, 2025. <https://doi.org/10.29316/9788368103243>
134. Ochyra-Żurawska, K., Nowicka, J., Ciekanski, Z., Organizacje pozarządowe w systemie bezpieczeństwa państwa na przykładzie Ochotniczych Straży Pożarnych, w: *Prakseologia w zarządzaniu i dowodzeniu*, t. 8: Etyczność w dowodzeniu, Kieżun, W., Wołeszo, J., Mikurenda, K. (red.), Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2020, s. 23-40.
135. OECD, Wsparcie realizacji audytu planów ciągłości świadczenia usług publicznych w Polsce (wytyczne/metodyka audytu), OECD, 2024.
136. Olech, A., Przygotowani na wojnę, czyli szwedzka obrona powszechna, *InfoSecurity24*, <https://infosecurity24.pl/za-granica/przygotowani-na-wojne-czyli-szwedzka-obrona-powszechna>, 2025, [dostęp: 10.10.2025];
137. Olejnik, T., Zarządzanie kryzysowe a komunikacja, czyli jak i kiedy informować ludzi, *Security, Economy & Law*, 1(14), 2017, s. 37-46.
138. Opolski Urząd Wojewódzki, Rozpoczęły się kolejne szkolenia dla władz samorządowych z Opolszczyzny w zakresie ustawy o ochronie ludności i obronie cywilnej, <https://www.gov.pl/web/uw-opolski/rozpoczely-sie-kolejne-szkolenia-dla-wladz-samorzadowych-z-opolszczyzny-w-zakresie-ustawy-o-ochronie-ludnosci-i-obronie-cywilnej>, [dostęp: 10.10.2025].
139. Ostrowski, J., Krzysztofik, D., Człowiek największym wyzwaniem systemu ochrony ludności, *Wspólnota (Pismo Samorządu Terytorialnego)*, 2024.
140. Otwinowski, W., Kryzys i sytuacja kryzysowa, *Przegląd Naukowo-Metodyczny Edukacja dla Bezpieczeństwa*, 2, 2010, s. 83-89.
141. Otwinowski, W., Podstawy zarządzania kryzysowego i systemu obronnego, *Poznań*, Wydawnictwo Naukowe Wyższej Szkoły Handlu i Usług, 2015.
142. Pac, B., Istota zarządzania zabezpieczeniem logistycznym w sytuacjach kryzysowych i stanach nadzwyczajnych, w: *Ekonomiczne, społeczne i środowiskowe uwarunkowania logistyki*, *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, 383, 2015, s. 132-153.

143. Parapura, H., Kowalewski, M., Kowalczyk, B., Ostrzeżanie i alarmowanie ludności w niebezpieczeństwie – rozwiązania w Polsce i na świecie, *Telekomunikacja i Techniki Informacyjne*, 1-2/2013, 2013, s. 74-83.
144. PCPM, Odporni na kryzys – rekomendacje dla włączenia społeczności lokalnej w system zarządzania kryzysowego, Warszawa, Fundacja PCPM, 2025.
145. Perry, N., Examining the Use of Unmanned Aerial Devices to Conduct Damage Assessment in the City of Norfolk, Executive Fire Officer Program, U.S. Fire Administration, FEMA, Emmitsburg (MD), 2017.
146. Pietrek, G., Poziomy, struktura i zadania systemu zarządzania kryzysowego administracji rządowej, *Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Łądowych im. gen. Tadeusza Kościuszki we Wrocławiu*, 3(161), 2011, s. 376-388.
147. Pilarz, K., Specyfika relacji organów administracji publicznej z otoczeniem w sytuacjach kryzysowych, *Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji*, CXI, nr 3802, Wrocław, 2017, s. 123-138. <https://doi.org/10.19195/0137-1134.111.9>
148. Polska Agencja Prasowa, Budżet 2025. Jest decyzja rządu, <https://www.money.pl/gospodarka/budzet-2025-jest-decyzja-rzadu-7075937101695840a.html>, [dostęp: 30.09.2025].
149. Prezes Rady Ministrów, Zarządzenie nr 101 z dnia 4 września 2017 r. w sprawie Międzyresortowego Zespołu do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego (M.P. 2017 poz. 837).
150. Protokół Dodatkowy (I) do Konwencji Genewskich z 1949 r., art. 61.
151. Public Safety Canada, National Public Alerting System (Alert Ready), <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sst-m-en.aspx>, [dostęp: 22.09.2025].
152. Rachwalska, M., MSWiA przejmuje dyżur. Służba Dyżurna Państwa zastąpi RCB, *InfoSecurity24.pl*, 2022, <https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/mswia-przejmuje-dyzur-sluzba-dyzurna-panstwa-zastapi-rcb>, [dostęp: 22.09.2025].
153. Rada Unii Europejskiej, Unijna ochrona ludności, <https://www.consilium.europa.eu/pl/policies/civil-protection/>, [dostęp: 10.10.2025].
154. Rada Unii Europejskiej, Zagrożenia hybrydowe, Bruksela, 2024, <https://www.consilium.europa.eu/pl/policies/hybrid-threats/>, [dostęp: 10.10.2025].
155. Reconstruction Agency, After the Great East Japan Earthquake (informacja o 10-letnim horyzoncie odbudowy i alokacji 25 bln JPY na okres intensywnej odbudowy), Reconstruction Agency, 2021.

156. Reynolds, B., Seeger, M., Crisis and Emergency Risk Communication as an Integrative Model, *Journal of Health Communication*, 10(1), 2005, s. 43-55. <https://doi.org/10.1080/10810730590904571>
157. Reznikova, O., *National Resilience in a Changing Security Environment*, Kyiv, National Institute for Strategic Studies, 2022.
158. Ristvej, J., Zagorecki, A., Information Systems for Crisis Management – Current Applications and Future Directions, *Communications – Scientific Letters of the University of Žilina*, 13(2), 2011, s. 59-63. <https://doi.org/10.26552/com.C.2011.2.59-63>
159. Rosicki, R., O pojęciu i istocie bezpieczeństwa, *Przegląd Politologiczny*, (3), 2010, s. 23-32. <https://doi.org/10.14746/pp.2010.15.3.2>
160. Rostis, A., Make no Mistake: The Effectiveness of the Lessons Learned Approach to Emergency Management in Canada, *International Journal of Emergency Management*, 4(2), 2007, s. 250-259. <https://doi.org/10.1504/IJEM.2007.013990>
161. Rubin, C.B., *Emergency Management in the 21st Century: Dealing with Al Qaeda, Tom Ridge, and Julie Gerberding*, Working Paper #108, The Natural Hazards Center, Boulder, University of Colorado, 2004.
162. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2011 r. w sprawie form i zakresu dokumentacji planistycznej, 2011.
163. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 6 lutego 2025 r. w sprawie programów szkoleń z zakresu ochrony ludności i obrony cywilnej oraz wymagań dla podmiotów prowadzących szkolenia (Dz.U. z 2025 r. poz. 162).
164. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2018 r. w sprawie współpracy dyrektora Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu (Dz.U. z 2018 r. poz. 2309).
165. Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (Dz.U. z 2008 r. Nr 128 poz. 821).
166. Rozporządzenie Rady Ministrów z dnia 11 grudnia 2020 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. z 2020 r. poz. 2344).
167. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r. Nr 83, poz. 541).
168. Rozporządzenie Rady Ministrów z dnia 30 maja 2025 r. w sprawie ewakuacji ludności oraz zabezpieczenia mienia (Dz.U. z 2025 r. poz. 765, § 18).

169. Rozporządzenie Rady Ministrów z dnia 31 sierpnia 2020 r. w sprawie współpracy dyrektora Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu (Dz.U. z 2020 r. poz. 1527).
170. Rysz, S. J., Integracja informatyczna w obszarze zarządzania kryzysowego, *Modern Management Review*, 22(2), 2017, s. 117-130. <https://doi.org/10.7862/rz.2017.mmr.20>
171. Rządowa Agencja Rezerw Strategicznych, Historia, (informacja o przekształceniu ARM w RARS na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych, obowiązującej od 23 lutego 2021 r.), <https://www.gov.pl/web/rars/historia2>, [dostęp: 10.07.2025].
172. Rządowa Agencja Rezerw Strategicznych, Projekty EU, <https://www.gov.pl/web/rars/projekty-eu>, [dostęp: 10.10.2025].
173. Rządowe Centrum Bezpieczeństwa, Alert RCB – najważniejsze pytania i odpowiedzi, <https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi>, [dostęp: 10.07.2025].
174. Rządowe Centrum Bezpieczeństwa, Alert RCB – przykładowe wiadomości (SMS), gov.pl, <https://www.gov.pl/web/rcb/alert-rcb---przykladowe-wiadomosci-sms>, [dostęp: 22.09.2025].
175. Rządowe Centrum Bezpieczeństwa, Informacje o systemie ostrzegania ludności (Alert RCB), <https://www.gov.pl/web/rcb>, [dostęp: 10.07.2025].
176. Rządowe Centrum Bezpieczeństwa, Krajowy Plan Zarządzania Kryzysowego 2025 (część A, lipiec 2025; część B, lipiec 2025).
177. Rządowe Centrum Bezpieczeństwa, Księga Komunikacji Kryzysowej, Warszawa, RCB, 2017.
178. Rządowe Centrum Bezpieczeństwa, Księga komunikacji kryzysowej. Podstawy zarządzania informacją w kryzysie, Warszawa, RCB, 2018.
179. Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity, Warszawa, RCB, 2023.
180. Rządowe Centrum Bezpieczeństwa, Obieg informacji i rola RCB w systemie zarządzania kryzysowego, Gov.pl, 2024, <https://www.gov.pl/web/rcb/obieg-informacji-i-rola-rcb-w-systemie-zarzadzania-kryzysowego>, [dostęp: 22.09.2025].
181. Rządowe Centrum Bezpieczeństwa (RCB), Ocena ryzyka na potrzeby zarządzania kryzysowego, Warszawa, RCB, 2013.
182. Rządowe Centrum Bezpieczeństwa (RCB), Skutki frontu burzowego, komunikat z 12.08.2017, <https://archiwum.rcb.gov.pl/skutki-frontu-burzowego/> [dostęp: 16.02.2025].

183. Rządowe Centrum Bezpieczeństwa, Wymiana polskich i niemieckich doświadczeń w zakresie zarządzania kryzysowego, RCB – Archiwum, 2012.
184. Rządowe Centrum Bezpieczeństwa (RCB), Zagrożenia okresowe występujące w Polsce – aktualizacja, Warszawa, RCB, 2013.
185. Rzecznik Praw Obywatelskich (Wiącek, M.), Wystąpienie do Ministra Spraw Wewnętrznych i Administracji w sprawie organizacji i funkcjonowania obrony cywilnej, Warszawa, 06.12.2022, sygn. VII.7215.1.2022.MP.
186. Sabak, J. System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, Serwis Defence24.pl, 2021, <https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych>, [dostęp: 22.09.2025].
187. Sawczuk-Gołaszewska, B., Chodyka, M., Grudniewski, T. M., Ciekankowski, Z., Bezpieczeństwo placówek edukacyjnych szkolnictwa średniego w czasie pandemii COVID-19, Warszawa, Menedżerska Akademia Nauk Stosowanych w Warszawie (Wydawnictwo im. Prof. Leszka J. Krzyżanowskiego), 2024.
188. Sienkiewicz-Małyjurek, K., Krynojewski, F. R., Zarządzanie kryzysowe w administracji publicznej, Warszawa, Difin, 2010.
189. Sienkiewicz-Małyjurek, K., Interorganizational collaboration and public sector innovativeness – the case of Poland, *International Journal of Contemporary Management*, 12(30), 2013, s. 8-25.
190. Sienkiewicz-Małyjurek, K., Skuteczne zarządzanie kryzysowe, Difin, Warszawa, 2015.
191. Skrabacz, A., Pajka, A., Więckowski, B., Crisis Management as a Research Province of Security Science, *Roczniki Nauk Społecznych*, 52(1), 2024, s. 7-25. <https://doi.org/10.18290/rns2024.0010>
192. Skrabacz, A., Kanarski, L., Loranty, K. (red.), Edukacja dla bezpieczeństwa: o kształtowaniu kultury bezpieczeństwa, Warszawa, Wojskowe Centrum Edukacji Obywatelskiej im. płk. dypl. Mariana Porwita, 2015.
193. Skoczylas, L., Aktualna współpraca transgraniczna Polski z wybranymi sąsiadami, *Białostockie Studia Prawnicze*, 12, 2012, s. 123-136. <https://doi.org/10.15290/bsp.2012.12.06>
194. Skomra, W., Edukacja jako element zarządzania kryzysowego, *Wiadomości Ubezpieczeniowe* (wydanie specjalne: Powódź – Infrastruktura – Finansowanie), Polska Izba Ubezpieczeń, 2012, s. 13-18.
195. Skomra, W., Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy, Warszawa, BEL Studio, 2018.

196. Speranza, L., Six reasons NATO's Euro-Atlantic Disaster Response Coordination Centre is important for our future security, Atlantic Council, New Atlanticist, 2020.
197. Spustek, H., Paluch, A., Struktura systemu bezpieczeństwa narodowego Polski, Zeszyty Naukowe Politechniki Śląskiej. Seria: Organizacja i Zarządzanie, (100), 2017, s. 428-440.
198. Staśkiewicz, J., Budowanie odporności na zagrożenia – rola samorządów w zarządzaniu kryzysowym, OpenSecurity.pl, 2024, <https://opensecurity.pl/budowanie-odpornosci-na-zagrozenia-rola-samorzadow-w-zarzadzaniu-kryzysowym/>, [dostęp: 22.09.2025].
199. Stachoń, M., Raport Grupy Zadaniowej NATO-UE ds. odporności infrastruktury krytycznej, NASK – Cyber Policy, <https://cyberpolicy.nask.pl/raport-grupy-zadaniowej-nato-ue-ds-odpornosci-infrastruktury-krytycznej/>, [dostęp: 10.10.2025].
200. Sterczewska, I., Wybrane elementy zarządzania kryzysowego, Bezpieczeństwo. Teoria i Praktyka, 4, 2016, s. 81-95.
201. Stępka, M., Rezyliencja jako paradygmat bezpieczeństwa w czasach przewlekłych kryzysów, Przegląd Politologiczny, 26(2), 2021, s. 105-117. <https://doi.org/10.14746/pp.2021.26.2.7>
202. Sześciło, D., Ustawa o ochronie ludności i obronie cywilnej – jak zorganizować współpracę samorządu z organizacjami pozarządowymi?, Warszawa, Fundacja im. Stefana Batorego, 2025, s. 1-12.
203. Szymonik, A., Logistyka w bezpieczeństwie, Warszawa, Difin, 2011.
204. Świątek, Z. (red.), Mały słownik języka polskiego: Obrona cywilna i zarządzanie kryzysowe, Warszawa, Wydawnictwo Ministerstwa Obrony Narodowej, 2012.
205. Świdorski, K., Współpraca formacji mundurowych w utrzymaniu bezpieczeństwa transgranicznego Polski, Wschodnioznawstwo, 12, 2018, s. 127-142.
206. The World Bank (Trustee), Haiti Reconstruction Fund Trust Fund Financial Summary as of December 31, 2018, The World Bank Group, 2018.
207. Traktat Północnoatlantycki, sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. z 2000 r. Nr 87, poz. 970).
208. Tworzydło, D., Łaszyn, A., Szuba, P., Zarządzanie kryzysem w polskich przedsiębiorstwach. Podsumowanie 10 lat badań nad kryzysami, Rzeszów, Wydawnictwo Newslime, 2018.
209. Uchwała nr 72 Rady Ministrów z dnia 27 maja 2025 r. w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 (M.P. 2025 poz. 541).
210. UNDP, Human Development Report 1994, 1994.

211. UNDRR, *The Human Cost of Disasters: An overview of the last 20 years (2000-2019)*, Geneva, 2020.
212. United Nations, *Sendai Framework for Disaster Risk Reduction 2015-2030 (A/RES/69/283)*, United Nations, Geneva, 2015.
213. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. z 2024 r. poz. 1907).
214. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. (Dz.U. z 2024 r. poz. 1077 ze zm.).
215. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2024 r. poz. 145 ze zm.).
216. Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2024 r. poz. 652 ze zm.).
217. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2024 r. poz. 1198 ze zm.).
218. Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2024 r. poz. 266 ze zm.).
219. Ustawa z dnia 10 maja 2018 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. z 2018 r. poz. 1118).
220. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2024 r. poz. 248 ze zm.).
221. Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz.U. z 1985 r. Nr 12, poz. 49 z późn. zm.).
222. Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz.U. z 2024 r. poz. 1598 ze zm.).
223. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62, poz. 558 z późn. zm.).
224. Ustawa z dnia 18 lipca 2001 r. – Prawo wodne (Dz.U. z 2001 r. Nr 115, poz. 1229).
225. Ustawa z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz.U. z 1991 r. Nr 77, poz. 335 z późn. zm.).
226. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. Nr 113, poz. 985 z późn. zm.).
227. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2025 r. poz. 902 ze zm.).
228. Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. z 1991 r. Nr 81, poz. 351 z późn. zm.).
229. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz.U. z 1991 r. Nr 88, poz. 400 z późn. zm.).

230. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późn. zm.).
231. Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe (Dz.U. z 2001 r. Nr 3, poz. 18).
232. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. poz. 1301).
233. Van Wassenhove, L. N., Humanitarian aid logistics: supply chain management in high gear, *Journal of the Operational Research Society*, 57(5), 2006, s. 475-489. <https://doi.org/10.1057/palgrave.jors.2602125>
234. Wiktorowski, T., Systemy ostrzegania i informowania ludności jako narzędzie zwiększania odporności społecznej, *Bezpieczeństwo. Teoria i Praktyka*, 2024.
235. Wilkinson, P., *Crisis Management in Business*, London, Kogan Page, 2010.
236. Wiśniewska-Paź, B., Kultura bezpieczeństwa a edukacja – wzajemne konteksty, relacje i wyzwania, *Pedagogika Społeczna*, XIX, 3(77), 2020, s. 101-118. <https://doi.org/10.35464/1642-672X.PS.2020.3.07>
237. Wiśniewska-Paź, B., *Współczesne zagrożenia – bezpieczeństwo – edukacja, czyli jak uczyć społeczeństwo zasad bezpieczeństwa*, Wrocław, Wydawnictwo Uniwersytetu Wrocławskiego, 2018.
238. Wiśniewski, B., Kaczmarczyk, B. (red.), *Zarządzanie kryzysowe. Uwarunkowania teoretyczne, prawne i organizacyjne*, Legnica, Wydawnictwo PWSZ im. Witelona, 2012, s. 86-88.
239. Wiśniewski, M., Analysis of the integrity of district crisis management plans in Poland, *International Journal of Disaster Risk Reduction*, 67, 102650, 2022. <https://doi.org/10.1016/j.ijdr.2021.102650>
240. Wiśniewski, M., Procedury budowy scenariuszy zdarzeń niekorzystnych w strukturze procesu planowania cywilnego, *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, (128), 2018, s. 451-473.
241. Wojciechowska-Filipek, S., Ciekanski, Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, wyd. 2, Wydawnictwo CeDeWu, 2019.
242. Wołęjszo, J. (red.), *Innowacje i nowe technologie w bezpieczeństwie*, Kalisz, Wydawnictwo Naukowe Uniwersytetu Kaliskiego, 2025.
243. Wołęjszo, J., Rejman, K., Wilczyńska, M. (red.), *Bezpieczeństwo informacji w zarządzaniu kryzysowym*, Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2025.
244. Yucesoy, E., Balcik, B., Coban, E., The role of drones in disaster response: A literature review of operations research applications, *International Transactions*

- in *Operational Research*, 32(2), 2024, s. 981-1025. <https://doi.org/10.1111/itor.13484>
245. Zakrzewska, S., Kierunki doskonalenia systemu zarządzania kryzysowego w kontekście ochrony ludności i ratownictwa, *Doctrina. Studia Społeczno-Polityczne*, 18, 2021, s. 225-239. <https://doi.org/10.34739/doc.2021.18.14>
 246. Zarządzenie nr 53 Prezesa Rady Ministrów z dnia 16 maja 2024 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego (M.P. 2024 poz. 372).
 247. Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (M.P. 2014 poz. 926).
 248. Zaskórski, P., Żbik, D., Monitorowanie zagrożeń z wykorzystaniem systemów informacji geograficznej, *Studia Bezpieczeństwa Narodowego*, 9(1), 2016, s. 397-413. <https://doi.org/10.37055/sbn/129836>
 249. Zeng, L., Starbird, K., Spiro, E. S., Rumors at the speed of light? Modeling the rate of rumor transmission during crisis, w: *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, Honolulu, 2016, s. 1969-1978. <https://doi.org/10.1109/HICSS.2016.248>
 250. Ziarko, J., Uwarunkowania zarządczego podejścia do społecznej odporności na zagrożenia kryzysowe, *Bezpieczeństwo. Teoria i Praktyka*, 2024, 4(LVII). <https://doi.org/10.48269/2451-0718-btip-2024-4-009>
 251. Ziobro, J., Ratownictwo transgraniczne jako forma współpracy i integracji międzynarodowej oraz środków w procesie zapewniania bezpieczeństwa powszechnego – wybrane aspekty organizacji transgranicznych działań ratowniczych, *Scientific Reports of Fire University (ZN SGSP)*, 73(1), 2020, s. 165-191, <https://doi.org/10.5604/01.3001.0014.0781>
 252. Związek Banków Polskich (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, rozdz. 9: Współpraca z jednostkami publicznymi, Warszawa, ZBP, 2017, s. 145-160.
 253. Żurawski, S., Chodyka, M., Systemy wczesnego ostrzegania przed cyberzagrożeniami jako narzędzie bezpieczeństwa państwa, *Przegląd Naukowo-Metodyczny. Edukacja dla bezpieczeństwa*, 2025, XVIII, 2(67), s. 81-92.
 254. Żurawski, S., Nowicka, J., Ciekanowski, Z., Systemy zarządzania kryzysowego w wybranych państwach NATO, w: *Prakseologia w zarządzaniu i dowodzeniu*, t. 8: Etyczność w dowodzeniu, Kieżun, W., Wołęjszo, J., Mikurenda, K. (red.), Kalisz, Kaliskie Towarzystwo Przyjaciół Nauk, 2020, s. 41-54.
 255. <https://ochronaludnosci.edu.pl>, [dostęp: 10.10.2025].

Spis rysunków

Rysunek 1. Struktura systemu bezpieczeństwa narodowego RP – podsystem kierowania oraz podsystemy wykonawcze (operacyjne i wsparcia)	18
Rysunek 2. Operacyjne podsystemy wykonawcze systemu bezpieczeństwa narodowego RP – komponent obronny i ochronny . . .	35
Rysunek 3. Miejsce podsystemów wsparcia w strukturze systemu bezpieczeństwa narodowego RP.	46
Rysunek 4. Bezpieczeństwo państwa w ujęciu dualnym	57
Rysunek 5. Cykl zarządzania kryzysowego – cztery podstawowe fazy działań: zapobieganie, przygotowanie, reagowanie, odbudowa.	71
Rysunek 6. Globalne przemiany w podejściu do redukcji ryzyka katastrof (lata 1979-2015)	108
Rysunek 7. Kluczowe etapy rozwoju europejskiego systemu ochrony ludności	112
Rysunek 8. Ewolucja polskiego systemu zarządzania kryzysowego . .	118
Rysunek 9. Struktura systemu zarządzania kryzysowego w Polsce od szczebla centralnego do gminnego (schemat hierarchiczny)	134
Rysunek 10. Macierz ryzyka wykorzystywana do jakościowej oceny ryzyka na podstawie prawdopodobieństwa (oś pionowa) oraz dotkliwości skutków (oś pozioma) zdarzenia	153
Rysunek 11. Udział służb w reagowaniu na powódź 2010 r. w Polsce – liczba funkcjonariuszy zaangażowanych w działania ratunkowe (Straż Pożarna, Policja, Wojsko).	178

Rysunek 12. Schemat ciągłości procesu odbudowy po katastrofie – zakres zadań i nakładanie się faz krótkoterminowej, pośredniej i długoterminowej	186
Rysunek 13. Obieg informacji w systemie ostrzegania i reagowania. .	227
Rysunek 14. Panel sytuacyjny GIS – rozmieszczenie działań organizacji pozarządowych po huraganach Helene i Milton (dashboard „NGO Response to Hurricanes Helene & Milton”)	234
Rysunek 15. Liczba aktywacji Unijnego Mechanizmu Ochrony Ludności (UCPM) w latach 2007-2022	293
Rysunek 16. Długości granic Polski z państwami sąsiednimi oraz granica morska (km).	310
Rysunek 17. Zaufanie społeczne i zaufanie do instytucji publicznych w Polsce (luty 2024 r.)	374

Spis tabel

Tabela 1. Ujęcia definicyjne zarządzania kryzysowego w literaturze i prawie.	69
Tabela 2. Fazy zarządzania kryzysowego i przykładowe typy działań . .	72
Tabela 3. Przykładowe kategorie zagrożeń i ich atrybuty (częstość, skala, zasięg) w Polsce.	148
Tabela 4. Wybrane zagraniczne rozwiązania w ochronie ludności i ich potencjał transferu do Polski.	326
Tabela 5. Klasyfikacja państw według poziomu analizowanego wskaźnika	347



ISBN 978-83-68103-32-8