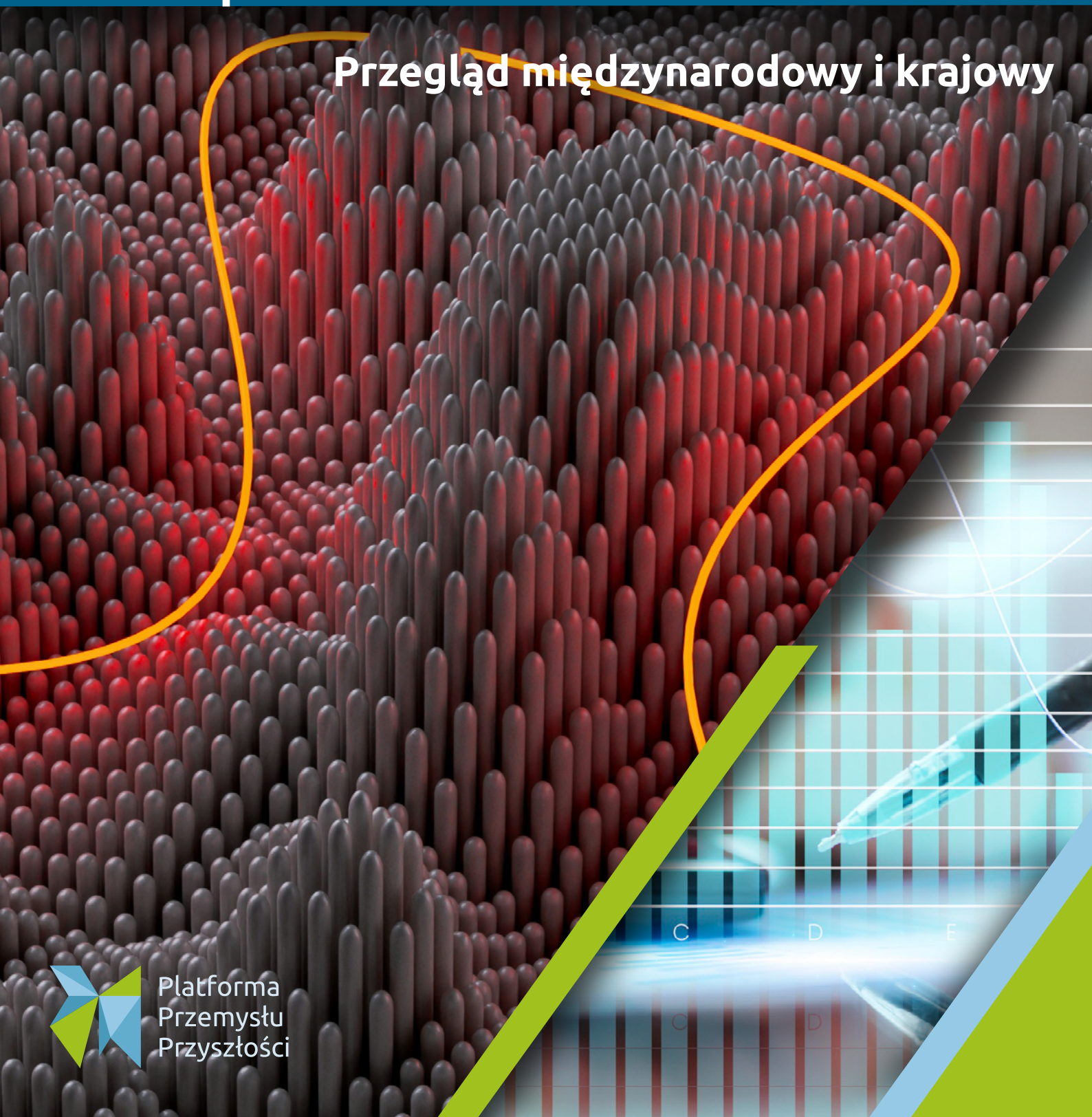
2024

Mechanizmy wzmocnienia odporności gospodarki

w sytuacji zagrożenia

Przegląd międzynarodowy i krajowy



Platforma Przemysłu Przyszłości

2024

Mechanizmy wzmocnienia odporności gospodarki w sytuacji zagrożenia

Przegląd międzynarodowy i krajowy

materiał przygotowany w ramach prac
grupy ds. wykorzystania technologii cyfrowych
w sytuacji zagrożeń
Fundacji Platforma Przemysłu Przyszłości

Opracowali:
dr hab. Joanna Kuczewska
Marek Ostafil
Piotr Wojciechowski

Warszawa, 6 grudnia 2024 roku

Platforma
Przemysłu
Przyszłości

Spis Treści

Streszczenie

Celem niniejszego raportu jest dostarczenie przedsiębiorstwom kompleksowego przeglądu istniejących mechanizmów, które mogą zostać wykorzystane w celu zwiększenia ich odporności na zagrożenia, oraz wskazanie roli współpracy głównych aktorów życia gospodarczego (przedsiębiorstw, nauki i władzy) ze szczególnym uwzględnieniem roli klastrów w przezwyciężaniu sytuacji kryzysowych.

W raporcie zaprezentowano różnorodne modele współpracy między przedsiębiorstwami a instytucjami publicznymi w sytuacji zagrożenia. Modele te oparte są m.in. na koncepcji Potrójnej Helisy, gdzie interakcja między sektorem prywatnym, publicznym i naukowym odgrywa kluczową rolę w tworzeniu innowacyjnych rozwiązań. Treść raportu skupia się na trzech kategoriach zagrożeń: fizycznych (m.in. katastrofy naturalne i czynniki geopolityczne – wojny, ataki terrorystyczne), cybernetycznych oraz zdrowotnych.

Przedstawiono także mechanizmy wzmacniania odporności w ujęciu procesowym, koncentrując się na analizie ryzyka opartej na następujących etapach: identyfikacja ryzyka, zarządzanie ryzykiem, wdrożenie mechanizmów adaptacyjnych i ocena skuteczności działań. W szczególności podkreślono znaczenie klastrów przemysłowych w zapobieganiu zagrożeniom oraz wskazano ich potencjalną rolę w zwiększaniu odporności gospodarki na poziomie regionalnym i krajowym.

Od strony metodycznej opracowanie bazuje głównie na danych wtórnych zebranych na podstawie literatury przedmiotu, a także nawiązuje do doświadczenia eksperckiego autorów zbudowanego w ramach realizacji konkretnych projektów analityczno-doradczych.

Executive Summary

The purpose of this report is to provide businesses with a comprehensive overview of existing mechanisms that can be employed to enhance their resilience to hazards, while highlighting the role of cooperation among key economic actors (businesses, academia, and government) with particular emphasis on the role of clusters in overcoming crisis situations.
The report presents various models of cooperation between enterprises and public institutions in times of crisis. These models are based, inter alia, on the Triple Helix concept, where interaction between the private, public, and academic sectors plays a critical role in creating innovative solutions. The focus is placed on three main categories of threats: physical threats (natural disasters, wars, geopolitical factors, and terrorist attacks), cyber threats, and health threats.

Additionally, the report outlines the mechanisms for strengthening resilience from a process-oriented perspective, emphasizing risk analysis through the following stages: risk identification, risk management, implementation of adaptive mechanisms, and assessment of the effectiveness of these actions. Particular emphasis is placed on the importance of industrial clusters in preventing threats and their potential role in increasing economic resilience at the regional and national levels.

As regards the methodological side, the study is mainly based on secondary data collected from the literature on the subject and also refers to the authors' expert experience built up in the implementation of specific analytical and consultancy projects.

Wstęp

W obliczu rosnącej liczby zagrożeń, zarówno na poziomie międzynarodowym, jak i krajowym, kluczowym staje się budowanie odporności przedsiębiorstw i gospodarek narodowych. Globalizacja procesów gospodarczych, rozwój technologii cyfrowych oraz niezwykle dynamiczne zmiany w sytuacji geopolitycznej powodują, że przedsiębiorstwa muszą nie tylko dostosowywać się do zmiennych warunków, ale także aktywnie rozwijać strategie zarządzania ryzykiem w celu budowania długoterminowej i permanentnej odporności na szoki. Różnorodne zagrożenia np.: fizyczne, cybernetyczne czy zdrowotne mogą prowadzić do znaczących strat, zakłóceń w łańcuchach dostaw oraz ograniczeń działalności biznesowej, co w efekcie zagraża stabilności gospodarki narodowej i międzynarodowej.

Celem niniejszego raportu jest dostarczenie przedsiębiorstwom kompleksowego przeglądu istniejących mechanizmów, które mogą zostać wykorzystane w celu zwiększenia ich odporności na zagrożenia, oraz wskazanie roli współpracy głównych aktorów życia gospodarczego (przedsiębiorstw, nauki i władzy) ze szczególnym uwzględnieniem roli klastrów w przezwyciężaniu sytuacji kryzysowych.

Treść niniejszego raportu koncentruje się na trzech kategoriach zagrożeń: fizycznych (katastrofy naturalne oraz czynniki geopolityczne, w tym wojny i ataki terrorystyczne), cybernetycznych oraz zdrowotnych. Wynika to z najważniejszych zdarzeń i wyzwań współczesnej gospodarki, do których zaliczają się: zmiany klimatyczne, pandemia COVID-19, skrajnie niestabilna sytuacja geopolityczna spowodowana konfliktami zbrojnymi oraz pędząca transformacja cyfrowa i związane z nią cyberbezpieczeństwo. Wybór ograniczonego zakresu przedstawianych zagrożeń wynika również z bardzo szerokiej i różnorodnej klasyfikacji zagrożeń i sytuacji kryzysowych.

Wzmocnienie odporności gospodarki to złożony proces, który obejmuje wdrażanie mechanizmów zapobiegających, łagodzących oraz reagujących na zagrożenia. Różne organizacje proponują różne sposoby rozwiązania kwestii odporności gospodarczej. Najczęściej projektowane działania zgodne są z typowymi i często przytaczanymi w literaturze naukowej etapami, do których zaliczane są: przygotowanie i planowanie działań, reagowanie w czasie sytuacji kryzysowych i odbudowa po ustąpieniu zagrożenia. Mogą również zostać wyodrębnione fazy: zapobiegania, przygotowawcze, reagowania i odbudowy. Na tym tle został przyjęty autorski podział mechanizmów wzmocnienia odporności gospodarki w ujęciu procesowym koncentrujący się na analizie ryzyka, która opiera się na następujących etapach: identyfikacja ryzyka, zarządzanie ryzykiem, wdrożenie mechanizmów adaptacyjnych i ocena skuteczności działań.

Raport ukierunkowany jest na udzielenie odpowiedzi na następujące pytania badawcze:

1. Jakie mechanizmy wzmocnienia odporności gospodarki i przedsiębiorstw wykorzystywane są w obliczu obecnych zagrożeń i niestabilności?
2. Jaka jest rola klastrów jako organizacji bezpośredniego wsparcia w zapobieganiu zagrożeniom?

Przegląd międzynarodowy i krajowy w zakresie identyfikacji mechanizmów wzmocnienia odporności gospodarki w sytuacji zagrożenia został opracowany w oparciu o następujące źródła:

1. przegląd literatury międzynarodowej i krajowej,
2. analiza dostępnych wyników badań naukowych,
3. analiza doniesień medialnych,
4. zaprezentowanie przykładów efektów współpracy klastrowej,
5. analiza własnych obserwacji i doświadczeń autorów wynikających ze współpracy i bezpośrednich kontaktów z przedsiębiorstwami, w tym z racji pełnionych funkcji koordynatorów klastrów.

1. Rodzaje zagrożeń bezpieczeństwa i ich wpływ na działalność przedsiębiorstw

Obecnemu rozwojowi społeczno-gospodarczemu oraz trwającym przemianom cywilizacyjnym towarzyszą liczne zjawiska i procesy, które generują zagrożenia zarówno dla człowieka, jak i środowiska. Nie ulega wątpliwości, że analiza i prognoza ryzyka staje się jednym z priorytetowych obszarów działania. W ostatnich latach szczególnie dotkliwe stały się zagrożenia związane technikami teleinformatycznymi i komunikacyjnymi. Z jednej strony wspierają one człowieka i rozwój gospodarczy, a z drugiej są źródłem wielu nowych niebezpieczeństw, również dla przedsiębiorstw. Nie ulega wątpliwości, że sytuacje kryzysowe i zagrożenia będą stale towarzyszyć ludzkości. Dlatego niezwykle istotne jest, aby mieć świadomość ciągłych zmian w zakresie występowania zagrożeń nowego typu i starać się być na nie przygotowanym. Dotyczy to zarówno państw, jednostek, jak i przedsiębiorstw.

Zgodnie z definicją K. Ficonia zagrożenie należy rozumieć jako zdarzenie spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), wywierające negatywny wpływ na funkcjonowanie danego systemu. Może ono także spowodować niekorzystne (niebezpieczne) zmiany w otoczeniu systemu (Ficoń 2007). Poniższa tabela przedstawia różnorodne klasyfikacje zagrożeń, z uwzględnieniem różnych kategorii podziału. Należą do nich: źródła powstania, rodzaj, czas eliminacji, dziedzina działania, poziom destrukcji, zakres przestrzenny, determinizm przyczyn oraz możliwości antycypacji.

Tabela 1. Kryteria klasyfikacji zagrożeń kryzysowych

Lp.	KRYTERIA KLASYFIKACJI ZAGROŻEŃ	
	KATEGORIE	PODKATEGORIE
1.	źródła powstania	naturalne, techniczne, społeczne, cywilizacyjne, ekologiczne
2.	podział rodzajowy	zdarzenia, katastrofy, klęski, kataklizmy
3.	czas eliminacji	krótkoterminowe, średnioterminowe, długoterminowe, bezterminowe
4.	dziedzina działania	sektorowe, religijne, polityczne, uniwersalne
5.	poziom destrukcji	minimalny, średni, wysoki, totalny
6.	zasięg przestrzenny	lokalny, regionalny, krajowy, międzynarodowy, ogólnoświatowy

7.	determinizm przyczyn	celowe, losowe, mieszane, przyrodnicze
8.	możliwości antycypacji	kontrolowane, prognozowane, nieprzewidywalne

Źródło: (Żebrowski&Szkurlat 2024, za Ficoń 2007).

Ze względu na źródła powstania można wyróżnić następujące zagrożenia (Żebrowski&Szkurlat 2024, za Ficoń 2007):

- naturalne – klimatyczne, tektoniczne, biologiczne (w tym zdrowotne), kosmiczne;
- techniczne – pożary i klęski krajobrazowe, skażenia chemiczne, katastrofy budowlane, katastrofy komunalne, katastrofy komunikacyjne, cyberbezpieczeństwo;
- społeczne – polityczne, prawne, gospodarcze (ekonomiczne), religijne, kulturowo-obyczajowe, związane ze zjawiskiem globalizacji, terroryzm, zorganizowane grupy przestępcze (w tym korupcja polityczna);
- militarne.

1.1. Zagrożenia fizyczne

Zagrożenia fizyczne, takie jak katastrofy naturalne, wojny, ataki terrorystyczne oraz inne czynniki geopolityczne, mają poważny wpływ na działalność przedsiębiorstw. Ze względu na wysokie ryzyko i dynamikę procesów są to najczęściej zagrożenia o obniżonej możliwości predykcji. Ich charakter (tj. zasięg globalny lub oddziaływanie na kluczowe regiony i sektory) wywiera skutki o dużym zasięgu i intensywności zakłócając łańcuchy dostaw, zmniejszając zaufanie inwestorów, ograniczając dostęp do rynków, a w skrajnych przypadkach prowadząc do całkowitego zatrzymania działalności.

Niejednokrotnie nieprzewidywalne katastrofy naturalne, takie jak trzęsienia ziemi, huragany, powodzie czy pożary, mogą prowadzić do bezpośrednich zniszczeń infrastruktury, majątku trwałego (nieruchomości) i łańcuchów dostaw. Oprócz strat fizycznych, przedsiębiorstwa stają przed wyzwaniem odbudowy i przywrócenia działalności, co może być kosztowne i czasochłonne. Zjawiska te i skalę ich oddziaływania w różnorakich wymiarach (społecznych, przedsiębiorstwa, sektorów gospodarki, kraju czy regionu) prezentuje bardzo bogaty dorobek naukowy. Najczęściej poruszanymi problemami badawczymi w tym zakresie są:

1. Czy jakiś specyficzny atrybut danej populacji (np. społeczny lub ekonomiczny – wyższy dochód lub silniejszy system instytucjonalny) powoduje, że odczuwają one większe lub mniejsze reakcje na ekspozycję klimatyczną?
2. Czy populacje regularnie narażone na określony rodzaj zmian klimatycznych lub zjawisk pogodowych są lepiej wyposażone do radzenia sobie z danym typem zdarzeń charakterystycznych dla tego klimatu?

Przykładami wpływu katastrof naturalnych na funkcjonowanie przedsiębiorstw mogą być:

- Huragan Katrina, 2005 rok, Stany Zjednoczone – nie tylko sparaliżował sektor energetyczny, ale również wpłynął na logistykę i handel międzynarodowy (Hsiang i in. 2014).
- Trzęsienie ziemi, 2011 rok, Tohoku, Japonia – wstrząsy o sile 9.1 w skali Richtera wywołały potężne tsunami, które zniszczyło nie tylko infrastrukturę, ale także za-

kłóciło globalne łańcuchy dostaw. Japoński przemysł motoryzacyjny, w tym firmy takie jak Toyota i Nissan, poniosły znaczne straty. Problemy pojawiły się również w branży produkcji elektroniki, gdzie braki w dostawach kluczowych komponentów spowodowały globalne zakłócenia (Yamamoto 2015).

- Powodzie, 2011 rok, Tajlandia – dotknęły główne centra przemysłowe w rejonie Bangkoku. Zniszczenia fabryk produkujących komponenty elektroniczne i samochodowe, w tym twarde dyski, spowodowały globalne zakłócenia w łańcuchach dostaw. Firmy takie jak Western Digital i Honda zostały poważnie dotknięte, a skutki odczuwano na całym świecie, szczególnie w przemyśle technologicznym (Haraguchi&Lall 2015).

Innym źródłem fizycznych zagrożeń dla bezpieczeństwa są wojny i konflikty zbrojne. Generują one ekstremalne zagrożenia dla działalności firm, szczególnie w obszarze biznesu międzynarodowego. Organizacje działające w strefach konfliktów mogą napotkać takie zagrożenia jak: zniszczenia infrastruktury, przerwanie dostaw, a także ryzyko utraty pracowników. Czynniki geopolityczne, takie jak: napięcia międzynarodowe, sankcje ekonomiczne czy zmiany polityczne, mogą mieć dalekosiężne konsekwencje dla firm. Jednym z ich skutków może być całkowite zablokowanie dostępu do kluczowych rynków i surowców. Korporacje muszą mierzyć się z niestabilnością polityczną, która często prowadzi do zmian w regulacjach handlowych i trudności w przewidywaniu przyszłych działań rządów. Długotrwałe konflikty mogą również wpływać na kursy walutowe, co dodatkowo komplikuje funkcjonowanie firm w globalnym środowisku. Wydarzenia geopolityczne wymagają także zmiany strategii zarządzania ryzykiem, a przedsiębiorstwa muszą dostosowywać swoje modele operacyjne do dynamicznego otoczenia politycznego (Cossin&Lu 2021).

Najbardziej aktualnym i bliskim przykładem zagrożenia tego typu jest wojna w Ukrainie. Liczne badania potwierdzają pogarszające się perspektywy dla światowej gospodarki, u podstaw których leżą: rosnące ceny żywności, paliw i nawozów, zwiększona niestabilność finansowa, dezinwestycje na rzecz zrównoważonego rozwoju, złożone fragmentaryzacje i transformacje globalnych łańcuchów dostaw czy rosnące koszty handlu (UNCTAD 2022; UNDP 2024). W badaniu prezentowanym przez Polski Instytut Ekonomiczny również polskie przedsiębiorstwa wskazują, iż wojna w Ukrainie silnie wpłynęła na: wzrost cen dóbr zaopatrzeniowo-inwestycyjnych, podniesienie cen produktów lub usług oferowanych przez przedsiębiorstwa, wyższe koszty działalności, wzrost ryzyka działalności biznesowej oraz zakłócenia w łańcuchach dostaw (Dębkowska i in. 2023).

Innym rodzajem zagrożenia kreowanego przez niestabilność polityczną, konflikty zbrojne czy wojny są ataki terrorystyczne, które dopełniają katastrofalne skutki tego typu zagrożeń dla gospodarki i przedsiębiorstw. Oprócz bezpośrednich strat materialnych, wpływają one na psychologię inwestorów, zmniejszając zaufanie do stabilności regionu i zmuszając firmy do ponoszenia dodatkowych kosztów na poprawę bezpieczeństwa. W długotrwałej perspektywie zagrożenie terroryzmem powoduje ponadto ograniczenie turystyki, spadek zagranicznych inwestycji bezpośrednich oraz wzrost kosztów ubezpieczeń.

Do największych ataków terrorystycznych, które doprowadziły do zniszczeń infrastruktury, majątku trwałego i łańcuchów dostaw przedsiębiorstw można zaliczyć:

- Ataki z 11 września 2001 roku na World Trade Center w Nowym Jorku miały ogromny wpływ na gospodarkę globalną, szczególnie na sektor finansowy, lotniczy oraz transportowy. Spowodowały straty w nieruchomościach oraz przerwy w działalności (finansowej i logistycznej). Negatywne skutki odczuwalne były także na rynku pracy. Atak doprowadził również do wprowadzenia globalnych restrykcji w transporcie lotniczym (Bram i in. 2002; Rose i in. 2009; New York City Partnership and Chamber of Commerce 2001).
- Zamachy bombowe na londyńskie metro w lipcu 2005 roku zniszczyły część infrastruktury transportowej miasta, co miało znaczący wpływ na funkcjonowanie brytyjskiej gospodarki. Zniszczenia wpłynęły na nieruchomości publiczne, a także na codzienne funkcjonowanie transportu miejskiego, który był kluczowy dla działalności przedsiębiorstw w centrum Londynu (Manelici 2017).
- Atak terrorystyczny na rafinerię Abqaiq w Arabii Saudyjskiej w 2006 roku, która była jednym z kluczowych punktów w globalnym łańcuchu dostaw ropy, spowodował chwilowe zakłócenia w produkcji i przesyłach ropy naftowej. Zakłócenia te wpłynęły na ceny surowców energetycznych oraz funkcjonowanie przedsiębiorstw na całym świecie (Henderson 2006).

1.2. Zagrożenia cybernetyczne

Zagrożenia cybernetyczne stanowią poważne wyzwanie dla współczesnych przedsiębiorstw. Obejmują szerokie spektrum działań związanych z przeciwdziałaniem wykorzystaniu wrogiego oprogramowania i wyciekom danych (szczególnie danych wrażliwych klientów) oraz obroną przed atakami hackerskimi i phishingiem. Wraz z rosnącym poziomem cyfryzacji i coraz większą zależnością od technologii informatycznych, cyberzagrożenia mogą powodować poważne straty finansowe, operacyjne, a także wpływać na reputację firm. Ponadto, w przypadku niektórych sektorów, takich jak infrastruktura krytyczna (np. energetyka, finanse), cyberataki mogą mieć poważne konsekwencje dla stabilności gospodarki i bezpieczeństwa państwa.

We współczesnej, globalnej gospodarce najczęstsze zagrożenia cybernetyczne to:

- Ataki DDoS (Distributed Denial of Service) – wielostronne, jednoczesne ataki DDoS mają na celu przeciążenie infrastruktury IT firmy, co prowadzi do zatrzymania lub spowolnienia działania systemów informatycznych, np. zatrzymania witryny internetowej.
- Oprogramowanie ransomware – jest to oprogramowanie szyfrujące pliki na komputerach i wymagające zapłacenia okupu w zamian za ich odblokowanie.
- Kradzież danych (data breach) – kradzież danych osobowych i handlowych, szczególnie informacji o klientach, co może prowadzić do znacznych strat finansowych oraz problemów prawnych.
- Phishing – wyłudzanie poufnych informacji poprzez podszywanie się pod zaufane instytucje. W ten sposób cyberprzestępcy narażają przedsiębiorstwa na utratę kluczowych danych, co z kolei prowadzi do strat finansowych i naruszenia tajemnic handlowych.
- Złośliwe lub zaszyfrowane oprogramowanie, tzw. malware – w tym np.: wirusy, trojany, robaki, backdoor.

- Cryptojacking – wykorzystanie urządzeń działających w firmie np.: laptopów, smartfonów, tabletów, a nawet serwerów, by bez zgody właściciela "wydobywać" kryptowaluty (ENISA 2023; Parlament Europejski 2022; Kędzior&Pieczarka 2018).

Najczęstsze problemy związane z zapewnieniem cyberbezpieczeństwa w przedsiębiorstwie są następujące (Fałkowski i in. 2024):

- Zastosowanie nieodpowiednich systemów i narzędzi ochrony danych tworzących nieskuteczną zaporę przed atakami hackerskimi.
- Wysokie koszty wdrożenia kompleksowych rozwiązań cyberbezpieczeństwa (np.: oprogramowania antywirusowego, systemów wykrywania ataków hackerskich, zabezpieczenia sieciowe).
- Ograniczenie dostępności do danych i zmniejszenie wydajności spowodowane potencjalnym generowaniem opóźnień w przesyłaniu danych.

Zgodnie z prognozami i statystykami dotyczącymi cyberbezpieczeństwa, przewidywane się następujące trendy. Do 2025 roku globalne szkody spowodowane cyberprzestępczością osiągną 10,5 biliona dolarów rocznie, a globalne wydatki na cyberbezpieczeństwo przekroczą 1,75 biliona dolarów. Natomiast globalne koszty szkód spowodowanych przez ransomware do 2031 roku przekroczą 265 miliardów dolarów. Poznanie tych trendów pomaga spojrzeć na wzrost cyberprzestępczości z perspektywy konieczności budowania odporności cybernetycznej (Cybersecurity Ventures 2023; Cremer i in. 2022).

Prognozy tak wysokich strat wywołanych przez cyberataki wskazują na ich wielokierunkowy wpływ na działalność biznesową. Po pierwsze, są one przyczyną dużych strat finansowych, zarówno bezpośrednich związanych z naprawą szkód, odszkodowaniami czy potencjalnym wypłacaniem okupu w przypadku ataku ransomware, jak i pośrednich związanych z utratą przychodów z powodu przestoju operacyjnego i utratę klientów w wyniku spadku zaufania. Po drugie, cyberataki powodują zakłócenia operacyjne ograniczając lub zatrzymując działalność biznesową na długi czas (np. zatrzymanie produkcji). Po trzecie, utrata bezpieczeństwa i wycieki danych wrażliwych mogą prowadzić do utraty zaufania klientów i prowadzić do poważnego uszczerbku na reputacji firmy. Przedsiębiorstwa, które nie potrafią odpowiednio chronić danych swoich klientów, mogą być pociągnięte do odpowiedzialności zgodnie z przepisami dotyczącymi ochrony danych (Biznes.gov.pl 2023; Kędzior&Pieczarka 2018).

Według badania „Global Cybersecurity Outlook 2023" przeprowadzonego wśród liderów biznesu do wiodących problemów i trendów związanych z cyberbezpieczeństwem należą (World Economic Forum 2023):

- Cyberataki bardziej koncentrują się na zakłóceniach działalności biznesowej i wyrządzeniu szkód w reputacji przedsiębiorstw.
- Przedsiębiorstwa przeznaczają więcej zasobów na codzienne zabezpieczenia niż na inwestycje strategiczne zakładając, że w ciągu najbliższych dwóch lat wystąpienie katastrofalnego zdarzenia cybernetycznego jest przynajmniej w pewnym stopniu prawdopodobne.
- Kadra kierownicza firm przyznaje, że jakość zabezpieczeń w całym łańcuchu dostaw partnerów handlowych i klientów wpływa na poziom ryzyka z zakresu cyberbezpieczeństwa ich organizacji.
- Liderzy mają trudności ze znalezieniem równowagi między wartością nowej technologii a potencjalnym wzrostem ryzyka cybernetycznego w swoich organizacjach.

- Dyrektorzy ds. cyberbezpieczeństwa teraz częściej postrzegają przepisy dotyczące prywatności danych i regulacje dotyczące cyberbezpieczeństwa jako skuteczne narzędzie do ograniczania ryzyka w branży.
- Rekrutacja i utrzymanie talentów stanowią kluczowe wyzwanie w zarządzaniu odpornością cybernetyczną.

1.3. Zagrożenia zdrowotne

Konsekwencje zagrożeń zdrowotnych, których doskonałym przykładem była i jest pandemia COVID-19, są zauważalne w całej gospodarce światowej. Dotykają wielu procesów gospodarczych, powodując zmiany w utrwalonych przez latach relacjach i zachowaniach głównych aktorów życia gospodarczego. Obserwowany jest postępujący proces spowolnienia gospodarki (slowbalisation) (Bakas 2016), gdzie ogniwa łańcuchów dostaw lokalizują się bliżej rynku macierzystego albo głównych rynków sprzedaży. Ponadto następuje znacząca reorganizacja globalnych łańcuchów wartości (GVC – Global Value Chain) i łańcuchów dostaw oraz zmiana relacji i współpracy przedsiębiorstw (Legrian 2020). Zauważalne są również zmiany przepływów zagranicznych inwestycji bezpośrednich (ZIB), a procesy transformacji cyfrowej przedsiębiorstw oraz robotyzacji i automatyzacji produkcji wykazują niesłychaną dynamikę wzrostu.

Zagrożenia wynikające z konieczności zaprzestania lub ograniczenia działalności biznesowej w czasie pandemii COVID-19 istotnie wpłynęły na zmianę modeli biznesowych. Zmusiły one przedsiębiorców do powszechnego wprowadzenia pracy zdalnej, istotnie zmieniły zachowania konsumentów zwiększając drastycznie udział sprzedaży internetowej, a także w istotny sposób wpłynęły na poszczególne elementy łańcuchów wartości. W procesach produkcji oraz projektowania i świadczenia usług drastycznie przyspieszyła transformacja cyfrowa, w tym automatyzacja i robotyzacja. Zmieniła się również organizacja i zakres outsourcingu. W procesie sprzedaży i marketingu ukształtowały się nowe relacje z klientem, zdecydowanie wzrosła rola: wykorzystania analiz dużych zbiorów danych (Big Data), e-handlu, marketingu socjalnego oraz aplikacji mobilnych. W procesie dystrybucji konieczne stały się zmiany modeli biznesowych, rozwój sprzedaży B2B oraz zawieranie nowych partnerstw. W obszarze zarządzania zasobami ludzkimi praca zdalna stała się oficjalną formą świadczenia pracy, co wiąże się z kwestami oceny wydajności i skuteczności pracy. Wyzwaniami stały się kwestia absencji pracowników (opieka nad dziećmi i zwolnienia lekarskie) oraz zwiększenie kompetencji cyfrowych pracowników. Przedsiębiorstwa skoncentrowały się na: konieczności przewartościowania celów i strategii działania (odejście od zysku i efektywności na rzecz bezpieczeństwa i rezyliencji), zawieraniu nowych partnerstw (w tym współpracy w ramach klastrów), utrzymaniu płynności finansowej i zarządzaniu ryzykiem oraz skierowały wysiłki na rzecz wdrożenia zarządzania zwinnego (agile management) (Gorynia, Kuczewska 2023).

W poniższej tabeli zaprezentowano przykłady reakcji konkretnych przedsiębiorstw na wyżej opisane zagrożenia, a także wskazano oceny reakcji tychże podmiotów na dane zagrożenie.

Tabela 2. Przykłady reakcji przedsiębiorstw na zagrożenia

Zagrożenia	Przykłady reakcji przedsiębiorstw	Ocena reakcji na zagrożenia
Zagrożenia fizyczne		
Huragan Katrina (2005 rok, USA)	**Walmart:** 1. Uruchomienie łańcuchów dostaw w trybie awaryjnym m.in. dostarczenie wody i żywności na dotknięte obszary szybciej niż wiele agencji rządowych było w stanie zareagować. 2. Przekazanie ok. 20 mln dolarów na pomoc ofiarom huraganu. 3. Otwarcie sklepów jako tymczasowych punktów dystrybucji dla potrzebujących (Diermeier i in. 2017, Walmart 2024). **FedEx:** 1. Przekierowanie dostaw z rejonu dotkniętego huraganem i zapewnienie ciągłości łańcuchów logistycznych. 2. Pomoc humanitarna – dostarczanie zasobów medycznych i środków pierwszej potrzeby do najbardziej poszkodowanych obszarów (Kratz 2005). **Citibank:** 1. Uruchomienie programów wsparcia dla klientów, w tym zamrożenie płatności kredytów hipotecznych dla osób poszkodowanych (Diermeier i in. 2017). **Entergy:** 1. Odbudowa infrastruktury energetycznej -mobilizacja tysięcy pracowników do przywracania zasilania w regionach dotkniętych przez huragan. 2. Zmiana podejścia do zarządzania ryzykiem. 3. Zwiększenie inwestycji w bardziej odporną infrastrukturę (Entergy 2023).	1. Szybka reakcja. 2. Wykorzystanie przewag logistycznych i lokalizacyjnych. 3. Pomoc charytatywna. 4. Budowa długoterminowych przewag i odporności.
Trzęsienie ziemi (2011 rok, Tohoku, Japonia)	**Toyota:** 1. Wprowadzenie dywersyfikacji łańcucha dostaw i wielozródłowe dostawy kluczowych komponentów. 2. Ograniczenie systemu Just-In-Time (JIT) podczas katastrof w celu utrzymania wyższego poziomu zapasów. 3. Inwestycje w technologie tj. cyfrowe bliźniaki i analizy danych napędzane przez sztuczną inteligencję pozwalające symulować potencjalne zakłócenia łańcucha dostaw i planować je z wyprzedzeniem. 4. Wspieranie dostawców w działaniach naprawczych i pomoc mniejszym podmiotom w powrocie do działania. (Toyota 2023; Congressional Research Service 2011).	1. Zmniejszenie ryzyka związanego z przerwaniem łańcucha dostaw i płynności sprzedaży. 2. Wprowadzenie systemów predykcji przyszłych zagrożeń.

Powodzie (2011 rok, Tajlandia)	**Honda, Toyota:** 1. Zamknięcie czasowe fabryk w Tajlandii. **Western Digital:** 1. Poszukiwanie alternatywnych lokalizacji produkcyjnych, co skutkowało zachwianiem globalnych łańcuchów dostaw. **Nikon, Sony:** 1. Budowa infrastruktury ochronnej tj. wały i bariery przeciwpowodziowe. Dodatkowo niektóre firmy zdecydowały się na dywersyfikację dostawców i lokalizacji produkcji, aby zminimalizować ryzyko zależności od jednego regionu (World Bank 2012; Marks i in. 2017).	1. Ograniczenie lub zawieszenie produkcji. 2. Budowa odporności (również w postaci infrastruktury ochronnej).
Ataki na World Trade Center (11 września 2001 roku, Nowy Jork)	**Morgan Stanley:** 1. Natychmiastowa ewakuacja 3,700 pracowników z biur w South Tower zorganizowana przez szefa bezpieczeństwa Ricka Rescorla. Kluczową rolę w szybkim i skutecznym reagowaniu na ataki odegrały regularne szkolenia ewakuacyjne, wprowadzone przez Rescorlę po wcześniejszym zamachu bombowym z 1993 roku (Knowledge at Warton 2011). **Przedsiębiorstwa z WTC i inne z sektora finansowego:** 1. Zmiana polityki zarządzania ryzykiem. 2. Przeprowadzanie kompleksowych symulacji katastrof związanych nie tylko z zagrożeniami fizycznymi, ale również gospodarczymi (kryzysy finansowe). 3. Inwestycje w zabezpieczenia fizyczne oraz cyberbezpieczeństwo. 4. Wdrożenie nowych standardów w zakresie zabezpieczania infrastruktury oraz systemów IT (Knowledge at Wharton 2011; Dixon&Stern 2014).	1. Szybka reakcja – skuteczne procedury ewakuacyjne. 2. Zmiana polityki zarządzania ryzykiem.
Zamachy bombowe na londyńskie metro (lipiec 2005 roku, Londyn)	**Firmy z londyńskiego City:** 1. Natychmiastowa ewakuacja i wsparcie dla pracowników. 2. Zwiększenie bezpieczeństwa fizycznego i wdrożenie procedur zarządzania kryzysowego. 3. Wykorzystanie pracy zdalnej. 4. Inwestycje w infrastrukturę IT i plany awaryjne (np.: wprowadzono alternatywny system komunikacji pagerowej, który jest nadal w użyciu, rozszerzono zasięg monitoringu CCTV, a liczba kamer podwoiła się (Rusi 2007).	1. Szybka reakcja – skuteczne procedury ewakuacyjne. 2. Zmiana polityki zarządzania ryzykiem.

Wojna w Ukrainie	**Wiele korporacji globalnych m.in.: McDonald's, Coca-Cola, Starbucks, Shell:** 1. Wycofanie działalności lub zawieszenie operacji w Rosji. 2. Pomoc finansowa oraz logistyczna dla uchodźców i osób poszkodowanych w Ukrainie (lista przykładów Smith 2022; U.S.-Ukraine Business Council 2022). 3. Zwiększenie wysiłków w zakresie ochrony przed cyberzagrożeniami, oraz nasilającymi się atakami cybernetycznymi. **Małe i średnie przedsiębiorstwa w Ukrainie:** 1. Od początku wojny 64% MŚP tymczasowo zawiesiło lub zamknęło działalność. Jednak zdecydowana większość wznowiła operację, (w październiku 2023 r. tylko 9,6% firm zagrożonych zamknięciem) (UNDP 2024).	1. Natychmiastowa reakcja. 2. Wprowadzenie sankcji i uruchomienie wsparcia finansowego i logistycznego. 3. Duża odporność MŚP w Ukrainie.
Zagrożenia cybernetyczne	**Sony – atak hakerski w 2014 roku:** 1. Wprowadzenie znacznych usprawnień w systemach zabezpieczeń. 2. Wdrożenie zaawansowanych mechanizmów ochrony danych tj. szyfrowanie danych, firewalle, systemy wykrywania zagrożeń czy technologie monitorowania sieci (Gapiński 2015; Steinberg 2014). **IBM i Microsoft:** 1. Zwiększenie inwestycji w technologie AI – rozwój sztucznej inteligencji w kontekście cyberbezpieczeństwa, wykorzystanie narzędzi do wykrywania i reagowania na zagrożenia w czasie rzeczywistym (IBM 2024, Microsoft 2024). **Colonial Pipeline – masowe ataki ransomware w 2021 roku:** 1. Wprowadzenie bardziej rygorystycznych procedur bezpieczeństwa. 2. Wzmocnienie zespołów ds. zarządzania ryzykiem cybernetycznym (Kerner 2021). **Mastercard:** 1. Współpraca międzynarodowa z organami ścigania, w tym umowa z Interpolem odnośnie współpracy w zakresie zwalczania cyberprzestępczości (Marciniak 2021).	1. Natychmiastowa reakcja. 2. Inwestycje w nowe technologie cyfrowe. 3. Permanentne zmiany w zarządzaniu ryzykiem.

Zagrożenia zdrowotne (pandemia COVID-19)	**Google, Microsoft, Twitter (oraz wiele innych korporacji):** 1. Przejście na pracę zdalną. 2. Rozwój i wdrożenie zaawansowanych platform do pracy zdalnej, takiej jak: Zoom, Microsoft Teams czy Slack. **McDonalds, Walmart, Amazon:** 1. zmiana modeli biznesowych – szybka adaptacja do e-commerce. **Toyota, Apple:** 1. Zabezpieczenie, dostosowanie i zdywersyfikowanie źródeł dostaw. 2. Przeniesienie produkcji bliżej lokalnych rynków. 3. Zwiększenie zapasów krytycznych komponentów (Tang i in. 2022; Haiyan 2023). **Różne organizacje, w tym korporacje i mniejsze przedsiębiorstwa:** Uruchomienie pomocy humanitarnej i logistycznej w celu łagodzenia skutków pandemii, np. Unilever przeznaczył 100 milionów euro na działania skierowane do ogółu społeczeństwa – klientów, dostawców, pracowników Unilever, a także pracowników ochrony zdrowia oraz organizacji pozarządowych (Unilever 2020). **Różne organizacje, w tym korporacje i mniejsze przedsiębiorstwa:** 1. Rozwój działań na rzecz wsparcia zdrowia psychicznego i well-being jako odpowiedź na stres i izolację wywołaną pandemią COVID-19. 2. Unilever – wprowadzenie programu wsparcia psychologicznego dla pracowników, m.in.: zaoferowanie bezpłatnych sesji terapeutycznych, elastycznych godzin pracy i urlopów zdrowotnych (Unilever 2024). 3. Starbucks – wprowadzenie inicjatywy na rzecz zdrowia psychicznego, zapewnienie wszystkim pracownikom w USA i uprawnionym członkom rodziny bezpłatnego dostępu do 20 sesji rocznie z terapeutą lub trenerem zdrowia psychicznego (Starbucks 2020).	

Źródło: opracowanie własne.

Na podstawie analizowanych zagrożeń i przykładów reakcji na nie, można wskazać kilka kluczowych elementów, które mogłyby zostać wdrożone i wykorzystane przez polskie przedsiębiorstwa w zakresie budowania odporności, reagowania i radzenia sobie w stanie zagrożenia, tj.:

1. Zarządzanie kryzysowe i planowanie awaryjne – wzmocnienie roli, powołanie jednostki lub opracowanie planu zarządzania kryzysowego, implementacja systemów monitorujących i wczesnego ostrzegania połączona z inwestycjami w technologie cyfrowe wykorzystywane przy monitorowaniu zagrożeń.
2. Inwestycje w technologie, szczególnie technologie cyfrowe oraz wdrażanie innowacji – przyspieszenie procesu transformacji cyfrowej, szczególnie poprzez wykorzystanie AI, automatyzację procesów oraz rozwój platform cyfrowych.
3. Zwiększenie bezpieczeństwa cybernetycznego – wdrożenie działań edukacyjnych i szkoleniowych dla pracowników z zakresu cyberbezpieczeństwa oraz wykonywanie regularnych aktualizacji systemów zabezpieczeń.
4. Dywersyfikacja łańcuchów dostaw – różnicowanie dostawców, zmiana pozycji w łańcuchach dostaw, korzystanie ze źródeł lokalnych (tu ważna jest rola klastrów).
5. Współpraca wewnątrz i międzysektorowa – budowanie sieci współpracy pomiędzy przedsiębiorstwami, rządem a organizacjami pozarządowymi; rozwój partnerstwa publiczno-prywatnego i wypracowanie procedur reagowania w sytuacjach zagrożenia.
6. Wsparcie infrastruktury zdrowotnej – rozwój projektów partnerstw publiczno-prywatnych (PPP) w celu zwiększenia dostępności usług zdrowotnych np.: rozwój telemedycyny, platform e-zdrowia, wdrażanie aplikacji do monitorowania zdrowia oraz systemów zdalnej obsługi pacjentów. Ponadto włączenie w projekty budowania procedur organizowania pomocy humanitarnej w sytuacji zagrożenia.

2. Modele współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia

2.1 Koncepcja współpracy przedsiębiorstw, instytucji publicznych i naukowych w modelu Potrójnej Helisy i rola Regionalnych Systemów Innowacji

Współczesna systemowa i strukturalna idea gospodarki opartej na wiedzy łączy subsystemy generacji wiedzy (ośrodki badawcze) z subsystemami wykorzystania wiedzy (przedsiębiorstwa) przy wsparciu organizacji transferu technologii. Systemy te współdziałają w ramach Regionalnych Systemów Innowacji (RIS)[1], które gwarantują przenikanie wiedzy analitycznej, syntetycznej i symbolicznej[2] do gospodarek poszczególnych regionów i krajów (Cooke&Leydesdorff 2006). Zarządzanie RIS odbywa się przy udziale najważniejszych aktorów gospodarki: przedsiębiorstw, nauki oraz władzy (rządu).

Relacje pomiędzy nimi determinują kierunek i kształt zarządzania przewagami regionu/kraju (Etzkowitz&Leydesdorff 1995; Leydesdorf 2000). Taki model współdziałania został zaprezentowany w pracy Leydesdorffa i Etzkowitza z 1995 roku i nazwany „Modelem Potrójnej Helisy". Głównym założeniem koncepcji było zwiększenie roli, jaką odgrywają uczelnie wyższe we wdrażaniu innowacji. Zgodnie z modelem zachodzi w nim kompromis pomiędzy integracją a zróżnicowaniem. Każdy z partnerów helisy bowiem ma swoją misję i interesy a jednocześnie nadaje kształt możliwej synergii i interakcjom (Lawton&Leydesdorff 2014). Zdaniem autorów koncepcji uczelnie wyższe przeszły podwójną transformację. Włączyły do swojej misji rozwój gospodarczy, szkolenia i badania oraz przeszły z orientacji indywidualnej do organizacyjnej w podejściu do każdego zadania i misji. Ponadto ośrodki naukowe i władza przejęły rolę przedsiębiorstw (uczelnie poprzez tworzenie inkubatorów przedsiębiorczości, władze poprzez promowanie venture capital). Natomiast przedsiębiorstwa przejęły rolę uczelni w rozwoju szkoleń i badań (Etzkowitz 2002; Etzkowitz&Klofsten 2005).

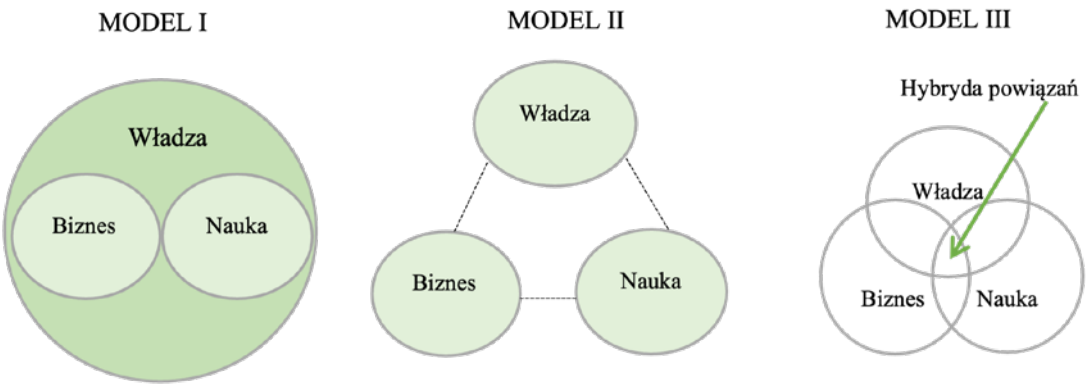
W literaturze odnajdujemy trzy modele Potrójnej Helisy, które różnią się rodzajem powiązań pomiędzy przedsiębiorstwami, nauką i władzą (rządem) (Rys. 1). W modelu I to państwo decyduje i kształtuje relacje pomiędzy nauką i przedsiębiorstwami. Jest to ujęcie historyczne, reprezentowane przez byłe kraje ZSRR i Europy Środkowo-Wschodniej w okresie przed rozpadem ZSRR. Model II wyróżnia trzy oddzielne sfery instytucjonalne: nauki, przedsiębiorstw i władzy, jednak wciąż z silnie zaznaczonymi granicami pomię-

1 Do najważniejszych funkcji Regionalnych Systemów Innowacji (RIS) zalicza się poszukiwanie i wykorzystywanie wiedzy oraz kontrolę organizacyjną poprzez system powiązanych i oddziałujących wzajemnie przedsiębiorstw – odpowiedzialnych za tworzenie i rozprzestrzenianie się wiedzy i innowacji oraz instytucji które tworzą środowisko do rozwoju nauki, technologii i przedsiębiorczości (Weresa 2012, 2014).

2 Wiedza analityczna (kodowana) – know-why przeważa w branżach, dla których bardzo ważna jest wiedza naukowa np. biotechnologia czy nanotechnologia. Właściwymi działaniami są zatem badania podstawowe i stosowane oraz systematyczny rozwój produktu lub procesów.
Wiedza syntetyczna (milcząca) – know-how polega na wprowadzaniu innowacji w oparciu o doświadczenie i umiejętności znane przedsiębiorstwu. Jest odpowiedzią na potrzeby klienta i dostawców. Badania i rozwój są mniej istotne, wykorzystuje się bowiem technologie znane, a nacisk kładzie się na rozwój produktu lub procesu.
Wiedza symboliczna know-who, związana jest z estetycznymi atrybutami produktów, kreacją wzorów i wizerunków oraz ekonomicznym wykorzystaniem różnego rodzaju kulturalnych artefaktów. Determinowana jest przez rozwój przemysłów związanych z kulturą (Asheim&Hansen 2009; Kuczewska 2012).

dzy nimi. Przykładem takich relacji była Szwecja. Natomiast w modelu III generowanie infrastruktury wiedzy odbywa się poprzez pokonywanie granic miedzy trzema ogniwami helisy i tworzenie wspólnego pola działania. Powstaje zatem swoista hybryda współpracy i powiązań biznesu, nauki oraz władzy (Etzkowitz&Leydesdorff 2000).

Rysunek 1. Modele koncepcji Potrójnej Helisy



Źródło: (Etzkowitz&Leydesdorff 2000, s. 111).

Współczesne regiony i państwa najczęściej tworzą relacje w ramach powiązań helisy bazującej na modelu trzecim. Wspólnym celem jest tworzenie otoczenia innowacyjnego składającego się z: naukowych firm typu spin-off, inicjatyw dla rozwoju gospodarczego opartego na wiedzy, aliansów strategicznych pomiędzy firmami, publicznych laboratoriów badawczych oraz badawczych grup akademickich. Powiązania te kształtowane są samoistnie (Leydesdorff 2005), a nie poprzez kontrolę rządu. Rząd zapewnia tylko wsparcie finansowe i niefinansowe oraz gwarantuje wyrównywanie pola gry poprzez respektowanie zasad uczciwej konkurencji (Etzkowitz&Leydesdorff 2000).

Rozwój badań w zakresie zarządzania RIS w warunkach gospodarki opartej na wiedzy przy udziale głównych aktorów potrójnej helisy zaowocował propozycją ewolucji modelu 3H do modelu poczwórnej helisy (Quadruple Helix) oraz kolejnej pięcioelementowej helisy (Quintuple Helix). W 2009 roku Carayannis i Campbell dodali do modelu 3H czwartą helisę, którą określili jako „sfera publiczna oparta na mediach i kulturze.” (Carayannis&-Campbell 2009). Rok później ponownie Carayannis i Campbell rozwinęli koncepcję modelu 5H (Quintuple Helix), gdzie w ramach piątej helisy dodano analizę nauk przyrodniczych oraz nauk społecznych i humanistycznych. W kolejnych pracach Leydesdorff również podkreśla możliwość dodawania kolejnych helis do modelu 3H. Uważa, że nie tylko modele 4H i 5H, ale również n-H są przewidywane w najbliższej przyszłości, zważając na niezwykłą dynamikę zmian w gospodarce globalnej i znaczenie innowacji w gospodarce opartej na wiedzy (Leydesdorff 2012).

Taka perspektywa badawcza pozwoliła na wykorzystanie koncepcji 3H dla sformułowania strategii rozwoju regionów np.: w Szwecji (Jacob 2006) i Polsce (Kuczewska 2012, 2013a, 2014a).

2.2 Modele współpracy międzynarodowej i krajowej

Model europejski (UE)

Jednym z modeli współpracy przedsiębiorstw i instytucji publicznych w stanie zagrożenia kryzysowego jest model wypracowany przez instytucje Unii Europejskiej i krajów członkowskich (Rys. 2). Ze względu na stopień integracji gospodarczej i walutowej możliwa jest ponadnarodowa koordynacja działań oraz wdrażanie mechanizmów budowania odporności gospodarek i przedsiębiorstw na kryzysy i zagrożenia. Strategia UE zakłada współpracę instytucji europejskich oraz państw członkowskich i obejmuje przede wszystkim wymianę informacji i danych w zakresie zapobiegania, przygotowania, reagowania, rozwoju i odbudowy po sytuacjach kryzysowych. Współpraca ta polega na zaangażowaniu poszczególnych krajów Wspólnoty i udziale ich instytucji publicznych w wymienionych działaniach. Sama UE nie posiada instytucji właściwych dedykowanych zarządzaniu całą wspólnotą w stanie kryzysu lub zagrożenia. Wspólne działania są uzgadniane i zatwierdzane na forum Rady Europejskiej i Rady UE. Polegają one na organizowaniu wspólnych programów, tworzeniu systemu wsparcia finansowego, rozwiązań legislacyjnych oraz wspólnej koordynacji działań w sytuacji zagrożenia (np. decyzje dotyczące ruchu lotniczego po wybuch wulkanu na Islandii w 2010 r.).

W 2013 r. ustanowiony został mechanizm wzmacniania zdolności UE do podejmowania szybkich decyzji politycznych w związku z koniecznością reakcji w obliczu sytuacji kryzysowej, tj. Zintegrowany System Reagowania Kryzysowego Unii Europejskiej (The EU Integrated Political Crisis Response Arrangements - IPCR). W ramach ICPR działania podejmowane są na trzech poziomach: monitorowania (nie stanowi aktywacji IPCR), oraz dwóch poziomów aktywacji, dla których dostępne są narzędzia pomocnicze: tryb udostępniania informacji i pełna aktywacja IPCR. Monitorowanie umożliwia dobrowolne udostępnianie informacji o kryzysie. Udostępnianie informacji wiąże się z obowiązkiem instytucji unijnych do sporządzania raportów, natomiast pełna aktywacja IPCR zwiększa widoczność reakcji UE i ułatwia radzenie sobie z kryzysem na szczeblu unijnym poprzez organizację posiedzeń Rady UE lub Rady Europejskiej. Ponadto, pełna aktywacja obejmuje przygotowanie propozycji działań w odniesieniu do reakcji UE na zagrożenie (Council of the EU 2016).

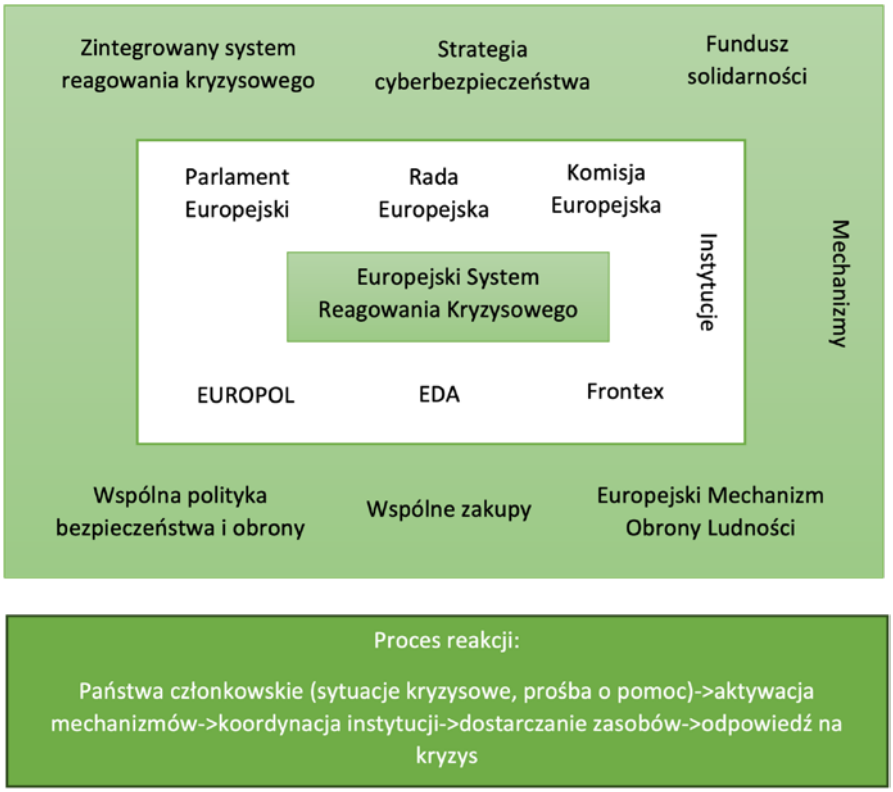
Kluczowy element współpracy międzynarodowej w zakresie zarządzania kryzysowego w Europie, angażujący nie tyko instytucje UE i krajów członkowskich, ale również pośrednio przedsiębiorstwa i organizacje pozarządowe to Mechanizm Ochrony Ludności Unii Europejskiej. Jego najważniejszym elementem jest Centrum Koordynacji Reagowania Kryzysowego (Emergency Response Coordination Centre - ERCC), którego zadaniem jest koordynacja i udzielanie pomocy krajom dotkniętym klęskami, w tym dostarczanie artykułów pierwszej potrzeby, wiedzy, zespołów ds. ochrony ludności i specjalistycznego sprzętu. ERCC działa przez 24 godziny na dobę, 7 dni w tygodniu. Na przykład w 2022 roku mechanizm został uruchomiony 106 razy w odpowiedzi na m.in.: wojnę w Ukrainie, pożary lasów w Europie, pandemię COVID-19 oraz powodzie w Pakistanie (Komisja Europejska 2024).
Mechanizm Ochrony Ludności w UE dysponuje zasobami pomocowymi dobrowolnie deklarowanymi przez państwa członkowskie. W 2019 r. uruchomiono rezerwę rescEU, która obejmuje dodatkowo: flotę samolotów i śmigłowców strażackich oraz do ewakuacji medycznej, zespoły ratownictwa medycznego i szpitale polowe, zapas środków medycz-

nych i mobilne laboratoria, środki tymczasowego zakwaterowania, transport i logistykę oraz zdolności reagowania na incydenty chemiczne, biologiczne, radiologiczne i jądrowe. Ostatnie interwencje w ramach Mechanizmu Ochrony Ludności UE uruchamiano z następujących powodów: trzęsienie ziemi w Turcji i Syrii (2023 rok), wojna Rosja – Ukraina (lata 2022-2024), kryzys zdrowotny związany z pandemią COVID-19 (lata 2020-2022), pożary lasów w Europie (lata 2021-2022) czy repatriacje z Afganistanu (2021 rok) (Rada UE 2024).

Ponadto do wspólnotowych działań w zakresie budowania odporności krajów członkowskich w obliczu zagrożeń należą:

- Europejska Agencja Obrony (European Defence Agency - EDA) – koordynuje współpracę między państwami członkowskimi w dziedzinie obrony. W sytuacjach kryzysowych związanych z zagrożeniami geopolitycznymi, jak np. wojna w Ukrainie, EDA wspiera wspólne programy zbrojeniowe oraz udziela pomocy w zakresie cyberbezpieczeństwa (EDA 2024).
- Europol i współpraca w zakresie walki z terroryzmem – wspólne działania zwalczania terroryzmu i cyberprzestępczości. Aktualnym przykładem wspólnych działań jest odpowiedź na zamachy w Paryżu i Brukseli, która obejmowała wymianę informacji oraz koordynację działań policyjnych w ramach całej Europy (Europol 2024).
- Frontex (Europejska Agencja Straży Granicznej i Przybrzeżnej) – wspiera państwa członkowskie UE i państwa stowarzyszone w ramach strefy Schengen w zarządzaniu granicami zewnętrznymi UE i walce z przestępczością transgraniczną. Oprócz działań związanych ze zwalczaniem przestępczości funkcjonariusze Frontexu mogą reagować w przypadku innych zagrożeń, np. w Finlandii zostali poinformowani o pożarze w lesie położonym na trudno dostępnym terenie w gminie Ilomantsi. Wyruszyli, aby zlokalizować miejsce i pracowali wraz z fińskimi władzami, aby opanować pożar (Frontex 2024).
- Wspólny zakup szczepionek podczas pandemii COVID-19 – koordynacja zakupu szczepionek dla całej UE, co zwiększyło szanse na dostępność i szybsze dostawy.
- Europejski Zielony Ład (European Green Deal - GD) – budowanie odporności na kryzysy klimatyczne, wspólne inwestycje w odnawialne źródła energii i technologie odporne na zmiany klimatu (Green Deal 2024).
- Europejska Solidarność Energetyczna (ESE) – wspólne budowanie bezpieczeństwa energetycznego. Aktualnie najważniejszym działaniem w ramach ESE było uruchomienie mechanizmów solidarnościowych, np. wspólnych zakupów gazu, w odpowiedzi na kryzys wywołany wojną w Ukrainie.

Rysunek 2. Europejski model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne.

Model amerykański

Kluczową rolę identyfikacji odpowiedzialności w procesie budowania odporności gospodarki USA wobec różnorakich zagrożeń odgrywa Administracja ds. Rozwoju Gospodarczego (US Economic Development Administration – EDA), która przeprowadza analizę sytuacji przed oraz po wystąpieniu zagrożenia. (Rys. 3).

Przykłady inicjatyw na rzecz budowania odporności gospodarczej w stanie ustalonym (przed wystąpieniem zagrożenia) obejmują m.in. (EDA 2024):

- Podejmowanie kompleksowych działań planistycznych, które obejmują szerokie zaangażowanie społeczności w celu zdefiniowania i wdrożenia wspólnej wizji odporności wraz ze wskazaniem źródeł finansowania.
- Podejmowanie działań w celu powiększenia bazy przemysłowej i ukierunkowanie rozwoju powstających klastrów lub branż, tak aby opierały się na unikalnych zasobach i mocnych stronach regionu i zapewniały stabilność w okresach recesji.
- Dostosowywanie programów retencji i ekspansji przedsiębiorstw (np. ogrodnictwa ekologicznego lub innych form wsparcia przedsiębiorstw) w celu pomocy firmom w ożywieniu gospodarczym po wystąpieniu zakłóceń.
- Budowanie odpornej i elastycznej grupy pracowników, która może elastycznie zmieniać miejsca pracy lub branże, gdy ich podstawowe zatrudnienie jest zagrożone.

- Utrzymywanie systemów informacji geograficznej (GIS), które łączą się z różnymi bazami danych przedsiębiorstw w celu śledzenia lokalnych i regionalnych „rotacji" (zmiany liczby podmiotów w regionie oraz w zakresie alokacji i koncentracji) oraz dostępnych miejsc rozwoju.
- Zapewnienie redundancji w sieciach telekomunikacyjnych i szerokopasmowych na wypadek klęsk żywiołowych lub katastrof w celu ochrony bezpieczeństwa publicznego i gospodarki.
- Promowanie ciągłości i gotowości biznesowej w obliczu zakłóceń oraz gotowości do podjęcia działań w celu wznowienia działalności po zdarzeniu.
- Stosowanie bezpiecznych praktyk rozwoju w dzielnicach biznesowych i okolicznych społecznościach.

Przykłady inicjatyw na rzecz budowania odporności gospodarczej po wystąpieniu zagrożenia (EDA 2024):

- Planowanie odbudowy po katastrofie – definiowanie kluczowych interesariuszy, ról, obowiązków i kluczowych działań.
- Ustanowienie procesu regularnej komunikacji, monitorowania i aktualizacji potrzeb i problemów społeczności oraz biznesu.
- Szybki kontakt z kluczowymi lokalnymi, regionalnymi, stanowymi i federalnymi urzędnikami w celu komunikowania potrzeb sektora biznesowego i koordynowania działań w zakresie oceny skutków.
- Ustanowienie i wykorzystanie mechanizmów koordynacji i planów sukcesji przywództwa w celu zapewnienia permanentnych działań na rzecz odbudowy.

Ponadto najczęstszą formą współpracy przedsiębiorstw i instytucji publicznych w stanie zagrożenia kryzysowego są tzw. partnerstwa publiczno-prywatne (PPP), które polegają na współpracy między rządem federalnym, stanowym lub lokalnym a sektorem prywatnym w celu efektywnego zarządzania sytuacjami kryzysowymi. Taka współpraca obejmuje planowanie, przygotowanie, reagowanie i odbudowę po katastrofach. Partnerstwa te mają na celu wzmocnienie zdolności reakcji na kryzysy, zwiększenie efektywności działań oraz minimalizację szkód dla społeczności i gospodarki.

Jednym z najlepszych przykładów takiej współpracy jest model agencji FEMA (Federal Emergency Management Agency). W zakresie planowania i przygotowania do katastrofy FEMA współpracuje z firmami w celu opracowania planów zarządzania kryzysowego, które uwzględniają specyfikę poszczególnych branż oraz organizuje wspólne szkolenia i ćwiczenia z udziałem przedstawicieli sektora publicznego i prywatnego. W sytuacji kryzysowej, firmy prywatne mogą udostępniać swoje zasoby (np. ciężki sprzęt, magazyny, transport, personel) na potrzeby działań ratunkowych i logistycznych. Dostarczają niezbędne produkty i usługi, takie jak: żywność, woda, leki, materiały budowlane, a także pomoc techniczna. Partnerstwo z sieciami handlowymi, firmami logistycznymi i dostawcami energii odgrywa kluczową rolę w szybkim przywracaniu normalnego funkcjonowania społeczności. Sektor prywatny uczestniczy również w procesie odbudowy zniszczonej infrastruktury (np. energetycznej, drogowej, budynków). Firmy budowlane, energetyczne i telekomunikacyjne współpracują z rządem, aby jak najszybciej przywrócić normalne warunki życia (FEMA 2024). Partnerstwa publiczno-prywatne promują również rozwój i implementację nowych technologii, które mogą poprawić zarządzanie kryzysowe, np. systemy ostrzegania, drony lub narzędzia analityczne oparte na wykorzystaniu Big Data.

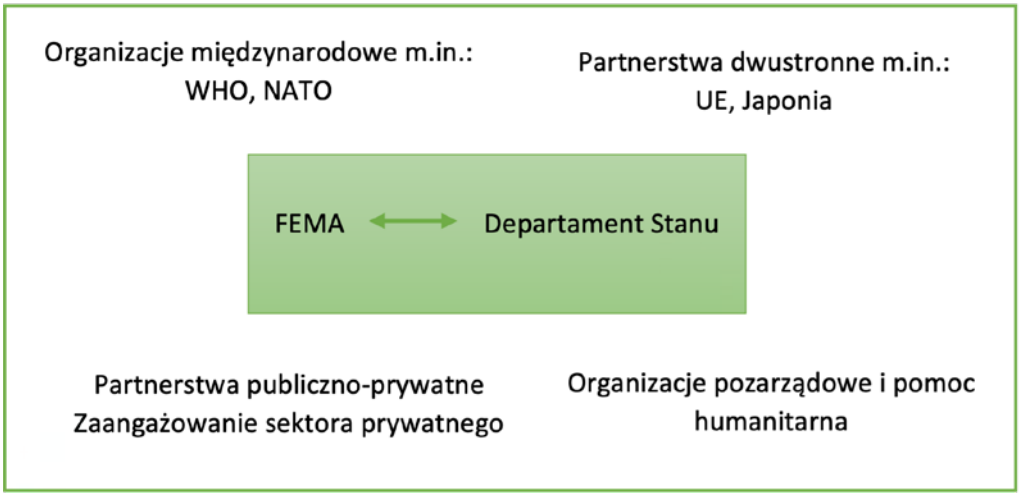
PPP w zarządzaniu kryzysowym w USA są często formalizowane poprzez umowy lub

porozumienia, które określają zakres współpracy, obowiązki stron oraz warunki działania w sytuacjach kryzysowych. Przykładami partnerstw z udziałem FEMA są: FEMA's Small Business Program (SBP), gdzie biuro SBP aktywnie współpracuje z personelem FEMA odpowiedzialnym za zamówienia publiczne, aby zapewnić małym przedsiębiorstwom jak największą możliwość uczestniczenia w kontraktach. Innym przykładem amerykańskiego PPP jest Krajowe Centrum Operacji Kryzysowych Biznesu (National Business Emergency Operations Center – NBEOC), gdzie FEMA koordynuje i usprawnia wymianę informacji pomiędzy partnerami rządowymi a organizacjami biznesowymi, przemysłowymi i infrastrukturalnymi przed, w trakcie i po katastrofach (FEMA 2024a).

Ponadto do wspólnych działań w zakresie budowania odporności w obliczu zagrożeń w modelu amerykańskim należą:

- Inicjowanie i koordynowanie współpracy międzynarodowej za pośrednictwem agencji tj. FEMA i Departament Stanu – na przykład po przejściu huraganu Katrina, agencje wspierały nie tylko lokalne działania, ale również angażowały partnerów międzynarodowych do działań pomocowych.
- Reakcje na kryzysy zdrowotne – podczas pandemii COVID-19, współpraca z WHO oraz międzynarodowymi partnerami, poprzez organizowanie dostaw sprzętu medycznego i szczepionek dla krajów na całym świecie.
- Pomoc humanitarna i wojskowa – po atakach z 11 września, USA znacząco rozszerzyły swoje działania na arenie międzynarodowej, angażując się w globalne operacje antyterrorystyczne oraz wspierając działania stabilizacyjne w regionach dotkniętych konfliktami, tj. Afganistan, Irak, Izrael czy Ukraina.
- Współpraca w zakresie cyberbezpieczeństwa – zwiększenie aktywności USA w zakresie współpracy z NATO, OECD i ONZ, w zakresie opracowywania norm i standardów mające na celu poprawę globalnej odporności na ataki cybernetyczne.

Rysunek 3. Amerykański model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne.

Model azjatycki

Przykładami krajów azjatyckich, które wypracowały zaawansowane modele współpracy publiczno-prywatnej w zarządzaniu kryzysowym, szczególnie w kontekście częstych katastrof naturalnych (np. trzęsienia ziemi, tsunami i tajfuny) są Japonia i Korea Południowa.

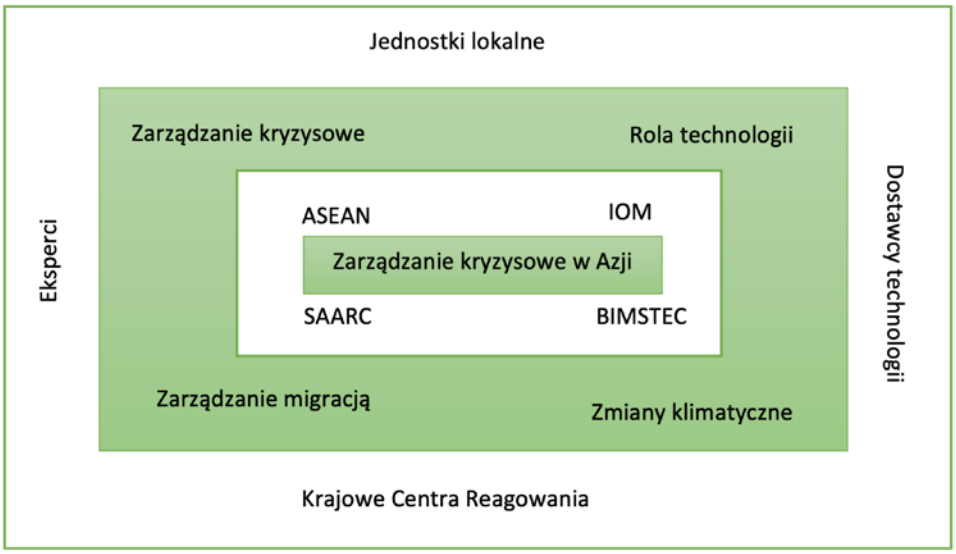
Ze względu na położenie geograficzne Japonia regularnie zmaga się z naturalnymi klęskami żywiołowymi, takimi jak trzęsienia ziemi, powodzie czy wybuchy wulkanów. W odpowiedzi na te zagrożenia kraj ten opracował jeden z najbardziej zaawansowanych systemów zarządzania katastrofami na świecie, bazujący na ścisłej współpracy między sektorem publicznym, prywatnym oraz społecznościami lokalnymi (Rys. 4). Główną rolę w procesie zarządzania kryzysowego pełni Rządowe Biuro Zarządzania Kryzysowego (Cabinet Office's Disaster Management Bureau). W ramach Biura funkcjonuje Krajowa Rada Zarządzania Katastrofami (The National Disaster Management Council), która koordynuje wszystkie działania związane z zapobieganiem, reagowaniem oraz odbudową po katastrofach. W skład Rady wchodzą premier (pełniący funkcję przewodniczącego), inni członkowie Gabinetu, szefowie głównych korporacji publicznych oraz eksperci. Funkcjonuje ona w ścisłej współpracy z przedsiębiorstwami odpowiadającymi za infrastrukturę krytyczną w zakresie m.in. energetyki, transportu i telekomunikacji, które odgrywają kluczową rolę w procesach odbudowy po katastrofach. Przedsiębiorstwa uczestniczą w specjalnych programach szkoleniowych oraz biorą udział w ćwiczeniach organizowanych przez rząd, które mają na celu szybkie przywracanie działalności gospodarczej (Cabinet Office Japan 2021). Japonia inwestuje również znaczne środki w technologie wykrywania zagrożeń. Przykładem jest J-Alert – narodowy system ostrzegania o katastrofach, który informuje obywateli o nadchodzących zagrożeniach, takich jak trzęsienia ziemi, tsunami czy erupcje wulkanów. Sektor prywatny, szczególnie media i telekomunikacja, jest integralną częścią tego systemu, zapewniając szybką dystrybucję informacji (Centre for Public Impact 2024).

Korea Południowa, choć w mniejszym stopniu narażona na klęski żywiołowe niż Japonia, również rozwinęła silny model zarządzania kryzysowego. Obejmuje on szeroką współpracę z sektorem prywatnym. Głównym organem koordynującym działania jest Narodowa Rada ds. Zarządzania Kryzysowego (National Disaster and Safety Control Center – NDSCC), która udostępnia platformę National Disaster and Safety Portal. Pełni ona rolę koordynatora działań rządowych oraz współpracuje z przedsiębiorstwami odpowiedzialnymi za zarządzanie infrastrukturą krytyczną w zakresie jej ochrony przed różnorodnymi zagrożeniami (naturalnymi, cybernetycznymi i in.). Przedsiębiorstwa sektora energetycznego i telekomunikacyjnego uczestniczą w specjalnych ćwiczeniach i programach szkoleniowych organizowanych przez Narodową Radę (NDSCC 2024). Korea Południowa, podobnie jak Japonia, intensywnie inwestuje w rozwój systemów wczesnego ostrzegania i monitorowania zagrożeń. Wykorzystują one innowacyjne technologie cyfrowe, w tym Big Data i analizę predykcyjną, aby przewidywać możliwe zagrożenia i reagować na nie w sposób proaktywny. Skuteczny system wczesnego ostrzegania prognozuje trzęsienia ziemi i tsunami, a także informuje o planach działań awaryjnych, wydaje alarmy ostrzegające o katastrofach. Jego wykorzystanie pomaga również w: zapewnieniu systemu bezpiecznego schronienia, organizowaniu szkoleń dla mieszkańców, a także organizacji awaryjnego odzyskiwania obiektów oraz pomocy doraźnej dla ofiar (Yeong 2024).

Ponadto do wspólnych działań, opierających się na współpracy regionalnej i międzynarodowej w zakresie budowania odporności w obliczu zagrożeń w modelu azjatyckim należą:

- Współpraca w zakresie zarządzania katastrofami naturalnymi – współpraca międzynarodowa w tym zakresie gwarantuje szybką reakcję w celu udzielenia pomocy humanitarnej. Inicjatywy takie jak Stowarzyszenie na rzecz Współpracy Regionalnej Azji Południowej (the South Asia Association for Regional Cooperation – SAARC) oraz Inicjatywa Zatoki Bengalskiej na rzecz wielosektorowej współpracy technicznej i gospodarczej (the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation – BIMSTEC), podejmują wysiłki na rzecz poprawy współpracy regionalnej w zakresie zarządzania katastrofami (NBR 2022).
- Międzynarodowa Organizacja ds. Migracji (The International Organization for Migration – IOM) – działania w obszarze zarządzania kryzysowego, m.in.: śledzenie migracji, reagowanie na kryzysy humanitarne oraz wspieranie długoterminowej odbudowy. Organizacja ta prowadzi też programy zwiększające odporność społeczności na przyszłe kryzysy, a także monitoruje przemieszczenia ludzi w wyniku konfliktów i katastrof (IOM 2014).
- Stowarzyszenie Narodów Azji Południowo-Wschodniej (The Association of Southeast Asian Nations – ASEAN) – podejmuje szerokie działania w sytuacjach kryzysowych, szczególnie w zakresie reagowania na klęski żywiołowe, np.:
  - Centrum Koordynacyjne ASEAN ds. Pomocy Humanitarnej (ASEAN Coordinating Centre for Humanitarian Assistance – AHA Centre), koordynuje działania humanitarne i reagowanie na katastrofy w regionie ASEAN. Działa jako hub informacji i zarządzania zasobami. Przykładem działania centrum jest szybka reakcja na trzęsienie ziemi i tsunami w Indonezji w 2018 roku, gdzie AHA Centre dostarczyło wsparcie logistyczne oraz zarządzało pomocą międzynarodową (https://ahacentre.org/).
  - Porozumienie ASEAN w sprawie zarządzania katastrofami i reagowania kryzysowego (ASEAN Agreement on Disaster Management and Emergency Response – AADMER) – rama prawna dla współpracy regionalnej w zakresie zarządzania katastrofami.
  - Program „One ASEAN, One Response" – wspólna reakcja państw ASEAN na katastrofy w regionie i poza nim.
  - System logistyki kryzysowej ASEAN (ASEAN Disaster Emergency Logistics System for ASEAN – DELSA) - umożliwia szybkie dostarczanie niezbędnych materiałów pomocowych w regionie.
- Kluczowa rola technologii cyfrowych i analizy danych – wzrost znaczenia technologii w zarządzaniu kryzysami, na przykład poprzez zbieranie i analizowanie danych dotyczących przemieszczania się ludzi w sytuacjach kryzysowych (NBR 2022).

Rysunek 4. Azjatycki model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne

Model polski

W Polsce współpraca między sektorem publicznym a prywatnym w zakresie bezpieczeństwa narodowego opiera się na wielopoziomowej koordynacji działań oraz na ramowych przepisach prawnych, szczególnie w kontekście zarządzania kryzysowego i ochrony infrastruktury krytycznej (rys. 5.). Kluczową rolę odgrywa ustawa o zarządzaniu kryzysowym, która nakłada na przedsiębiorstwa zarządzające infrastrukturą krytyczną obowiązek wdrażania planów ciągłości działania oraz współpracy z administracją publiczną w sytuacjach zagrożenia. Przedsiębiorstwa energetyczne, telekomunikacyjne, wodociągowe i transportowe muszą regularnie przeprowadzać analizy ryzyka oraz wdrażać procedury reagowania na zagrożenia. Przykładem takiej współpracy są ćwiczenia międzysektorowe prowadzone z udziałem służb ratunkowych, wojska i administracji.

Współpraca opiera się także na partnerstwach publiczno-prywatnych, które umożliwiają efektywne wykorzystanie zasobów prywatnych w zarządzaniu kryzysowym. W szczególności w sektorze IT przedsiębiorstwa prywatne są zaangażowane w tworzenie i utrzymanie systemów wczesnego ostrzegania o zagrożeniach cybernetycznych, które mają na celu ochronę sieci krytycznych oraz zapewnienie bezpieczeństwa informacyjnego. Przykładem ich znaczenia jest znaczna liczna PPP zawartych w czasie pandemii COVID-19 przy wykorzystaniu znacznych nadwyżek kapitałowych prywatnych inwestorów i funduszy (Cenkier&Dec 2021).

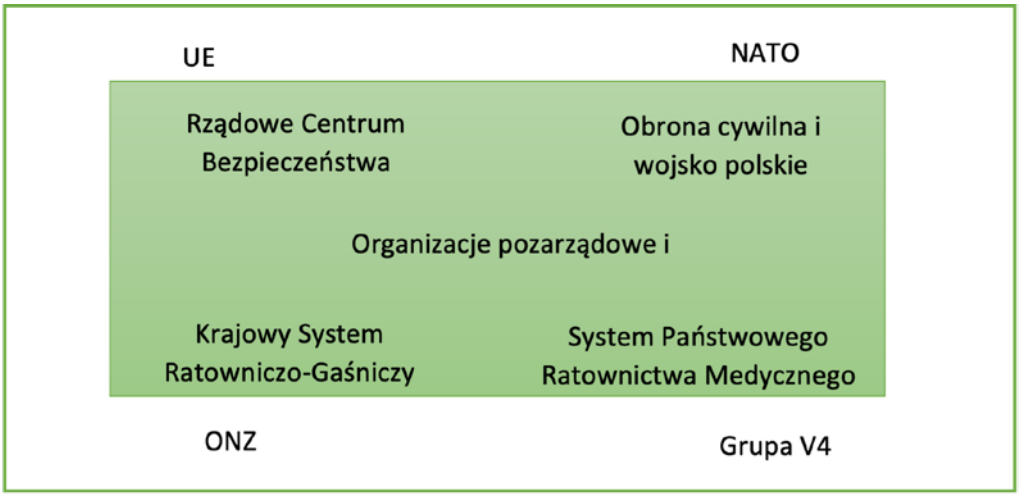
Ponadto ważną rolę w systemie zarządzania kryzysowego i przeciwdziałania zagrożeniom pełnią organizacje pozarządowe, głównie organizacje pożytku publicznego. Współpraca ta została uregulowana w 2003 roku przepisami ustawy o działalności pożytku publicznego i o wolontariacie. Katalog obszarów w sferze działalności publicznej, w których organizacje pożytku publicznego mogą wykonywać swoje zadania obejmuje m.in.: ratownictwo i ochronę ludności, pomoc ofiarom katastrof, klęsk żywiołowych, konfliktów zbrojnych i wojen w kraju i za granicą.

W fazie zapobiegania zagrożeniom podmioty, które mają brać udział w działaniach ratowniczych szkolą się i są wyposażane w sprzęt specjalistyczny. Uzgadniane są również narzędzia i techniki komunikacji oraz przygotowywany jest system dowodzenia. W fazie przygotowawczej opracowywane są plany zarządzania kryzysowego, procedury i scenariusze działań. Organizowane są też systemy alarmowania, ostrzegania, monitorowania, łączności i komunikacji, jak również informowania ludności cywilnej oraz tworzenia i utrzymania zabezpieczenia socjalno-bytowego dla potencjalnych poszkodowanych. W fazie reagowania współpraca organizacji pożytku publicznego z władzami to ich aktywny udział w bezpośrednich działaniach ratunkowych. Wsparcie w tej fazie najbardziej zależy od doświadczenia i potencjału, jakim dysponuje organizacja. Najważniejszą rolę odgrywają w tym etapie ochotnicze straże pożarne oraz społeczne organizacje ratownicze. Zadaniem wszystkich podmiotów w fazie odbudowy jest przede wszystkim odtworzenie obiektów czy infrastruktury oraz udzielanie pomocy poszkodowanym, przede wszystkim w zakresie socjalno-bytowym (Morawski 2014).

Ponadto do wspólnych działań, opierających się na współpracy regionalnej i międzynarodowej w zakresie budowania odporności w obliczu zagrożeń w modelu polskim należą:

- Współpraca z Unią Europejską – udział w mechanizmie ochrony ludności i udzielanie wzajemnej pomocy w przypadku klęsk żywiołowych, katastrof technologicznych oraz kryzysów zdrowotnych. Przykładem wspólnych działań była pomoc humanitarna oraz sprzęt medyczny wysyłany w czasie pandemii COVID-19.
- Współpraca w ramach Sojuszu Północnoatlantyckiego – Polska jako członek NATO bierze udział w operacjach reagowania kryzysowego, np. w ramach Euro-Atlantic Disaster Response Coordination Centre (EADRCC). Centrum to koordynuje wsparcie humanitarne i logistyczne w razie katastrof, jak również odpowiada na zagrożenia militarne. Przykładem aktywności Polski jest udział w ćwiczeniach NATO dotyczących zarządzania kryzysowego i reagowania na katastrofy, np. podczas ćwiczeń Vigorous Warrior.
- Współpraca z ONZ – w ramach organizowania pomocy humanitarnej i zarządzania kryzysowego. Polska deleguje swoje siły i zasoby na misje pokojowe oraz do udzielania pomocy humanitarnej.
- Współpraca w ramach Inicjatywy Środkowoeuropejskiej (CEI) oraz Grupy Wyszehradzkiej (V4) w zakresie zarządzania kryzysowego – przykładem jest współpraca przy wspólnych ćwiczeniach ratunkowych, takich jak Carpathian Eagle, które mają na celu poprawę gotowości do reagowania na klęski żywiołowe.

Rysunek 5. Polski model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne

Model skandynawski

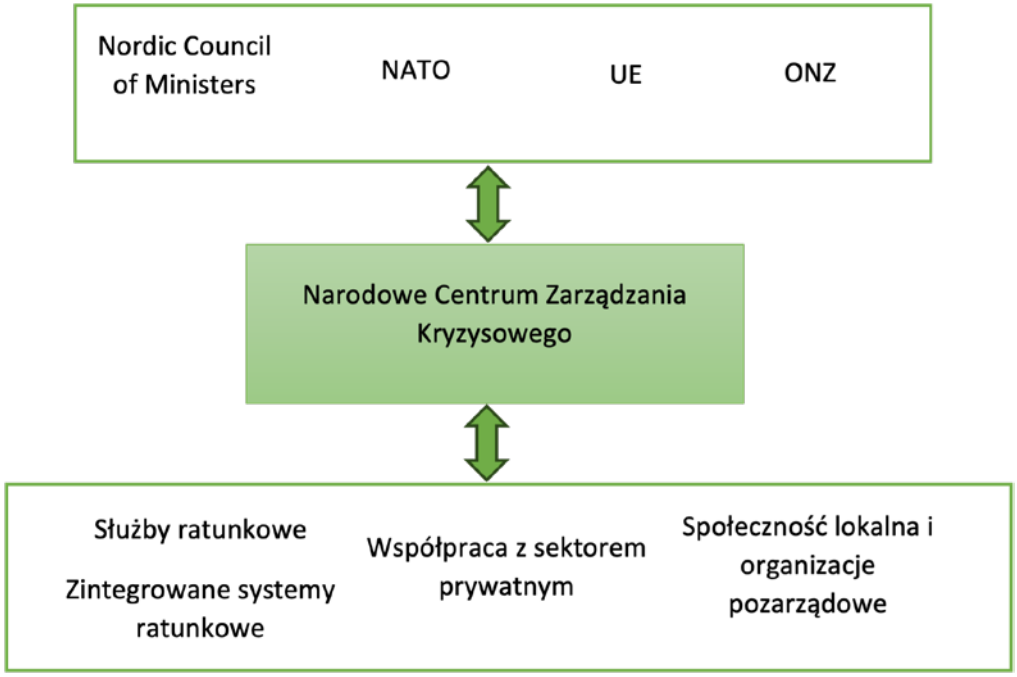
W krajach skandynawskich (Szwecja, Norwegia, Dania) współpracę w zakresie zarządzania kryzysowego charakteryzuje wysoki stopień decentralizacji działań, co oznacza silny nacisk na lokalne i regionalne podejście do zarządzania ryzykiem. Wspólne działania angażują zarówno sektor publiczny, jak i prywatny (Rys. 6.). Samorządy lokalne są odpowiedzialne za przygotowanie planów reagowania na kryzysy, a także za współpracę z lokalnymi przedsiębiorstwami. W Szwecji odpowiedzialność za koordynację zarządzania na wypadek sytuacji nadzwyczajnych podejmuje Ministerstwo Obrony Cywilnej, w Norwegii Ministerstwo Sprawiedliwości i Bezpieczeństwa Publicznego, a w Danii Ministerstwo Obrony.

W Skandynawii zarządzanie kryzysowe opiera się na zasadzie odpowiedzialności sektorowej. Oznacza to, że odpowiedzialność za bezpieczeństwo społeczne jest podzielona między sektory takie jak: policja, służba zdrowia, energetyka, transport i obrona. W ostatnich latach sektor energetyczny odgrywał coraz większą rolę w ogólnej sytuacji zagrożenia, podobnie jak sektor transportu, co wskazuje na kluczowe znaczenie utrzymania łańcuchów dostaw.
W wymienionych krajach duże znaczenie w sytuacji zagrożenia mają również partnerstwa publiczno-prywatne. Podobnie jak w wielu innych krajach, przedsiębiorstwa działające w sektorach, takich jak energetyka, telekomunikacja i transport, współpracują z lokalnymi władzami w zakresie zapewnienia ciągłości dostaw w sytuacjach zagrożenia. Modele te są oparte na współdzieleniu zasobów, wiedzy oraz infrastruktury.

W krajach skandynawskich, wydawałoby się bardzo zbliżonych w działaniu na rzecz zarządzania kryzysowego i przeciwdziałaniu zagrożeniom, podobieństwa te coraz szybciej znikają. Wyraźne różnice były widoczne w czasie pandemii COVID-19. Wówczas Szwecja była krajem, który zaszedł najdalej w zdecentralizowanym zarządzaniu – władza decyzyjna pozostała w rękach władz, ale rząd nie zajmował się faktycznym zarządzaniem kryzysowym. Na drugim końcu skali znalazła się Dania, z wysoce scentralizowanym zarządzaniem, podczas gdy Norwegia znajdowała się w połowie drogi pomiędzy Danią a Szwecją (NordForsk 2024).

Na uwagę w modelu skandynawskim zasługuje również współpraca w ramach Nordic Council of Ministers polegająca na regionalnej współpracy pomiędzy krajami skandynawskimi w zakresie bezpieczeństwa, zarządzania kryzysowego i wymiany informacji oraz realizacji wspólnych ćwiczeń ratunkowych (https://www.norden.org/). Ponadto kraje skandynawskie wykazują dużą aktywność w ramach współpracy z organizacjami międzynarodowymi tj. NATO, UE i ONZ.

Rysunek 6. Skandynawski model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne

Model brytyjski

W Wielkiej Brytanii współpraca między rządem a sektorem prywatnym w sytuacjach kryzysowych ma długą tradycję, a kluczową rolę odgrywają w niej instytucje takie jak: Cabinet Office oraz Civil Contingencies Secretariat, które nadzorują zarządzanie kryzysowe na poziomie krajowym oraz Local Resilience Forums (LRF) – regionalne jednostki reagowania, współpracujące z lokalnymi władzami, służbami ratunkowymi i organizacjami non-profit, nadzorujące zarządzanie kryzysowe na poziomie regionalnym (rys. 7.).

Wielka Brytania posiada kompleksowy system identyfikacji i oceny ryzyka na poziomie krajowym (National Risk Register – NRR). Zawiera on informacje o 89 zagrożeniach, w ramach 9 tematów ryzyka:

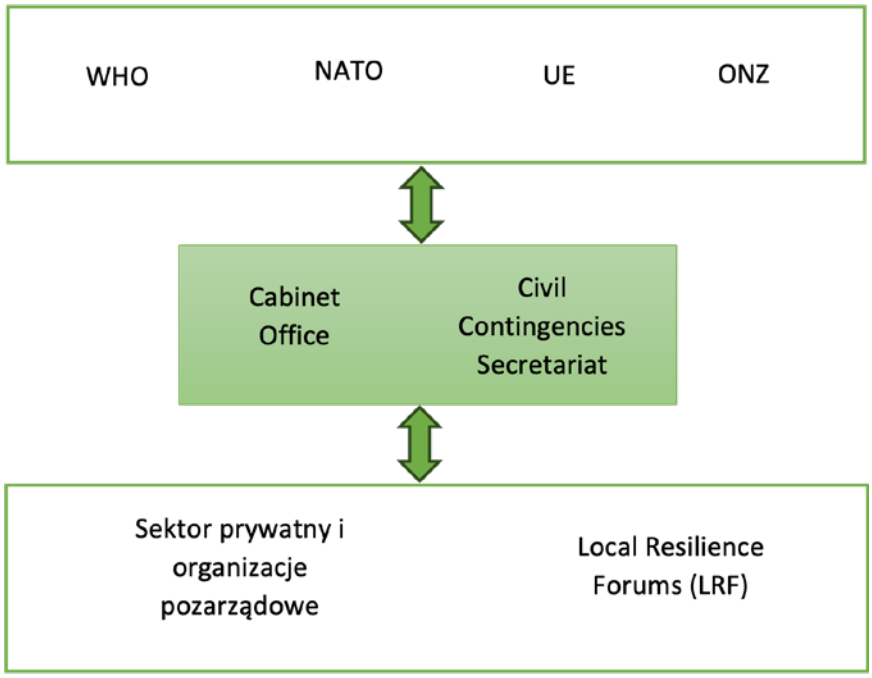
- wypadki i awarie systemów,
- konflikty i niestabilność,
- zagrożenia cybernetyczne, geograficzne i dyplomatyczne,
- zdrowie ludzi, zwierząt i roślin,
- zagrożenia naturalne i środowiskowe,
- zagrożenia społeczne i państwowe,
- terroryzm.

NRR obejmuje również współpracę z przedsiębiorstwami prywatnymi w zakresie analizy ryzyka i planowania działań zaradczych, np. prowadzone są regularne konsultacje z przedsiębiorstwami odpowiedzialnymi za infrastrukturę krytyczną, takimi jak dostawcy energii, wody i transportu.

W sytuacji zagrożenia rząd brytyjski pełni funkcję koordynatora działań. Ma opracowane plany zarządzania ryzykiem oraz kompleksowe plany budowania odporności w różnorodnych zakresach np.: Strategia Net Zero (Net Zero Strategy), Narodowa Strategia Cybernetyczna (The National Cyber Strategy), Strategia Żywnościowa Rządu (Government Food Strategy), Brytyjska Strategia Bezpieczeństwa Energetycznego (The British Energy Security Strategy) i Brytyjska Strategia Bezpieczeństwa Biologicznego (The UK Biological Security Strategy). NBR jest regularnie monitorowany oraz poddawany ewaluacji, w konsekwencji czego formułowane są benchmarki (najlepsze praktyki) (NRR 2023).

Ponadto, w Wielkiej Brytanii przedsiębiorstwa prywatne są zobowiązane do opracowania i wdrażania planów ciągłości działania, które są ściśle koordynowane z rządowymi wytycznymi dotyczącymi zarządzania kryzysowego. Oznacza to, że kluczowe sektory, takie jak bankowość, telekomunikacja i transport, muszą wdrożyć mechanizmy, które zapewnią szybkie przywrócenie działalności po kryzysie.

Rysunek 7. Brytyjski model współpracy sektora przedsiębiorstw z instytucjami publicznymi w stanach zagrożenia



Źródło: opracowanie własne

Podsumowując, amerykański model współpracy publiczno-prywatnej w zarządzaniu kryzysowym opiera się na szeroko zakrojonej koordynacji między sektorem publicznym a prywatnym przy wykorzystaniu technologii cyfrowych. Modele współpracy publiczno-prywatnej w zakresie zarządzania kryzysowego w Europie, Japonii i Korei Południowej opierają się na zintegrowanym podejściu do zarządzania ryzykiem, które obejmu-

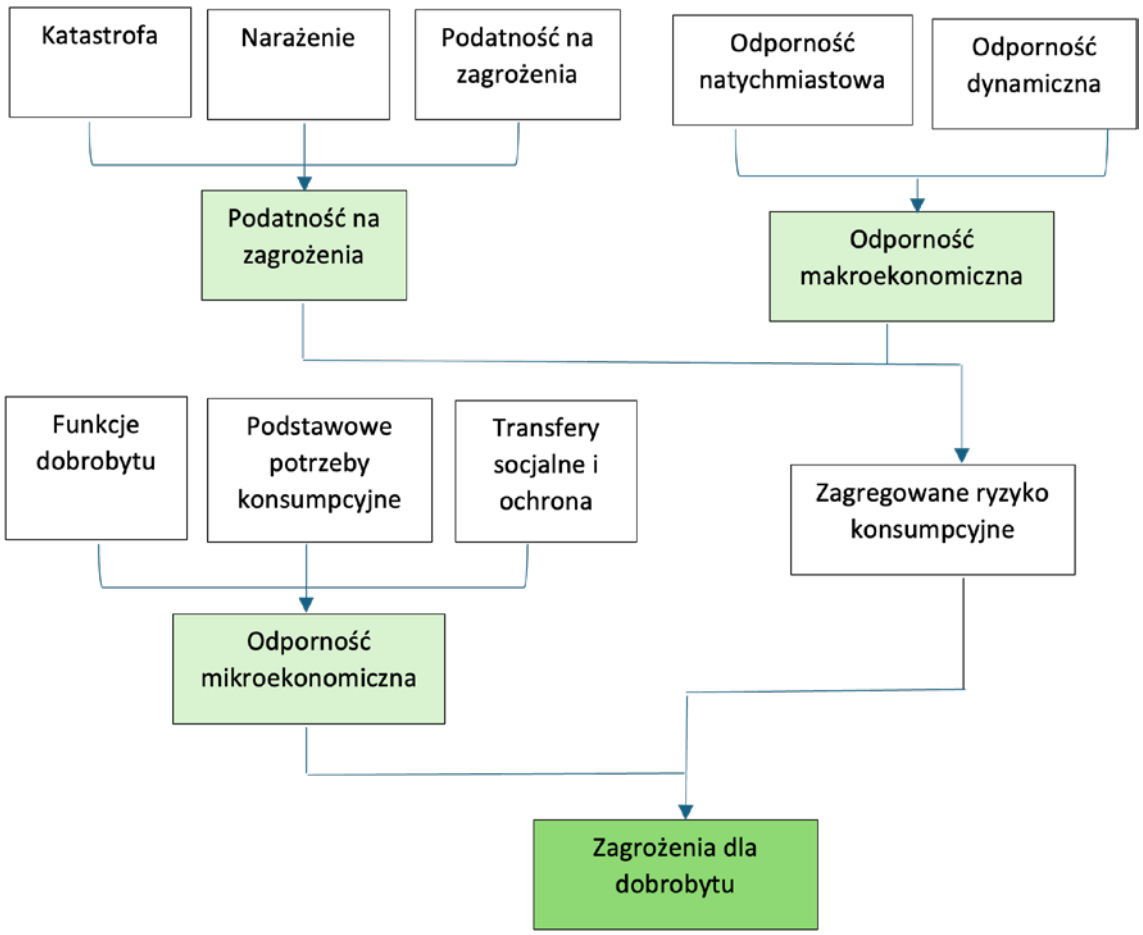
je zaangażowanie sektora prywatnego w przygotowanie, reagowanie i odbudowę po katastrofach. Kluczowym elementem jest integracja sektora prywatnego z rządowymi planami zarządzania kryzysowego. W Polsce model opiera się na ochronie infrastruktury krytycznej i wykorzystaniu partnerstw publiczno-prywatnych, natomiast w Skandynawii nacisk kładziony jest na inicjatywy lokalne i regionalne oraz współpracę z lokalnymi przedsiębiorstwami. Natomiast w Wielkiej Brytanii sektor prywatny jest ściśle związany z narodowymi systemami zarządzania kryzysowego i koordynacją działań w sytuacjach zagrożenia.

3. Mechanizmy wzmocnienia odporności gospodarki

Wzmocnienie odporności gospodarki to złożony proces, który obejmuje wdrażanie mechanizmów zapobiegających, łagodzących oraz reagujących na zagrożenia. W tym kontekście najistotniejszym wyzwaniem jest budowanie odporności gospodarki (resilience) i budowanie systemu gospodarczego zdolnego do radzenia sobie z zakłóceniami, minimalizowania ich negatywnych skutków oraz szybkiego powrotu do normalnej działalności po wystąpieniu kryzysu. Odporność gospodarki wskazuje, jak system gospodarczy reaguje na wstrząsy, zakłócenia i perturbacje (Alessi i in. 2020). Sprawę komplikuje charakter i czas trwania danego zagrożenia. Większość kryzysów obejmuje stosunkowo ograniczoną przestrzeń i czas (np. katastrofy naturalne – powodzie, wybuchy wulkanów itp.). Jednak niektóre zagrożenia mają charakter długoterminowy (np. efekty zmian klimatycznych), inne utrzymują się przez miesiące lub lata (np. pandemie czy konflikty zbrojne) (Trump&Linkov 2020). Stąd koncepcja odporności wciąż obejmuje wiele niezgodności co do sposobu rozumienia jej przyczyn, istoty i wpływu na długoterminowy wzrost (Martin&Sunley 2020).

Zgodnie z koncepcją konkurencyjności systemowej odporność gospodarki zależy od działań podejmowanych na poziomie makroekonomicznym, mezoekonomicznym (sektory i regiony) oraz mikroekonomicznym (przedsiębiorstwa, gospodarstwa domowe). Odporność makroekonomiczna ma dwie składowe: odporność natychmiastową, czyli zdolność do ograniczenia wielkości strat w sytuacji zagrożenia oraz dynamiczną, czyli zdolność do rekonstrukcji i odbudowy. Odporność mikroekonomiczna zależy od rozkładu strat, czyli od wrażliwości gospodarstw domowych i przedsiębiorstw, to jest ich dochodu przed katastrofą i zdolności do łagodzenia wstrząsów w czasie za pomocą oszczędności, pożyczek i ubezpieczeń, a także systemu ochrony socjalnej (Hallegatte 2014) (rys. 8.).

Rysunek 8. Struktura oceny ryzyka zagrożeń dla dobrobytu



Źródło: Hallegatte 2014, s. 3.

Różne organizacje proponują zróżnicowane sposoby rozwiązania kwestii odporności gospodarczej. Na przykład grupa G20 przyjęła listę zasad odporności, podczas gdy Międzynarodowy Fundusz Walutowy przedstawił obszerną listę konkretnych polityk niezbędnych dla solidnej i odpornej gospodarki. Europejski Bank Centralny przeprowadził analizę czynników wpływających na odporność gospodarczą (European Central Bank 2016; Sondermann 2018). Również Komisja Europejska podjęła wspólną debatę na temat odporności w kontekście politycznym, której pierwszym rezultatem było opracowanie ram koncepcyjnych poświęconych ocenie i pomiarowi odporności (Manca i in. 2017) (Gorynia&Kuczewska 2023).

Budowanie strategicznej odporności gospodarczej obejmuje zatem wdrażanie wielu różnych elementów, takich jak polityki i mechanizmy (w tym gospodarcze i polityczne) na szczeblu krajowym, ale też na poziomie organizacji międzynarodowych (takich jak EU), które chronią i wzmacniają gospodarkę kraju przed wstrząsami zewnętrznymi. Na przykład elementy odporności przedsiębiorstwa, takie jak: postawy przyjęte wobec kryzysu, charakterystyka organizacji, relacje z interesariuszami zewnętrznymi, kapitał ludzki i społeczny oraz zarządzanie strategiczne (Castro&Zermeño 2021) stanowią podstawę dyskusji na temat równowagi wyboru pomiędzy korygowaniem skutków a samoregulacją.

Wobec różnorodności podejść w definiowaniu odporności gospodarki i kategoryzacji mechanizmów wzmacniających tą odporność w niniejszym opracowaniu zostanie zaproponowany autorski podział mechanizmów wzmocnienia odporności gospodarki w ujęciu procesowym koncentrując się na analizie ryzyka. Procesowe podejście do wzmacniania odporności gospodarki opiera się na następujących etapach: identyfikacja ryzyka, zarządzanie ryzykiem, wdrożenie mechanizmów adaptacyjnych i ocena skuteczności działań (tab. 3.).

Tabela 3. Mechanizmy wzmacniania odporności gospodarki i przedsiębiorstw w ujęciu procesowym

1. Identyfikacja ryzyka – identyfikacja i predykcja zagrożeń • struktury instytucjonalne, • problemy polityczne, • zagrożenia gospodarcze, • zagrożenia klimatyczne, • pandemie i inne zagrożenia zdrowotne, • predykcja zagrożeń fizycznych (naturalnych).
2. Zarządzanie ryzykiem – redukowanie podatności gospodarki na zakłócenia Przedsiębiorstwa (poziom mikro): • dywersyfikacja źródeł zaopatrzenia. • optymalizacja łańcuchów dostaw, • rozwój infrastruktury informacyjnej. Poziom mezo- i makroekonomiczny (rola instytucji publicznych): • systemy wczesnego ostrzegania, • rozwiązania legislacyjne, • system wsparcia finansowego, • inwestowanie w infrastrukturę krytyczną.
3. Wdrażanie mechanizmów adaptacyjnych Przedsiębiorstwa (poziom mikro): • zmiana modeli biznesowych, • wprowadzenie nowego modelu czasu pracy i zmiany struktury zatrudnienia (np. praca zdalna), • automatyzacja procesów i transformacja cyfrowa. Poziom mezo- i makroekonomiczny (rola instytucji publicznych): • partnerstwa publiczno-prywatne (PPP), • koordynacja zasobów w sytuacji zagrożeń, • zapewnienie bezpieczeństwa energetycznego.
4. Ocena skuteczności • symulacje kryzysowe, • analiza skuteczności działań prewencyjnych i zaradczych.

Źródło: opracowanie własne.

Podejście to odzwierciedla typowe i często przytaczane w literaturze naukowej etapy: przygotowania i planowania działań, reagowania w czasie sytuacji kryzysowych i odbudowy po ustąpieniu zagrożenia (Morawski 2014) lub wyodrębniania faz: zapobiegania, przygotowawczej, reagowania i odbudowy (Sienkiewicz-Małyjurek 2010).

3.1 Identyfikacja ryzyka

Identyfikacja zagrożeń jest kluczowym elementem zarządzania ryzykiem w procesie wzmacniania odporności gospodarki. Etap ten polega na systematycznym rozpoznaniu potencjalnych niebezpieczeństw, które mogą wpłynąć na funkcjonowanie przedsiębiorstw, sektorów gospodarki, czy całych gospodarek. Celem identyfikacji ryzyka jest stworzenie pełnej mapy zagrożeń, aby można było skutecznie reagować, ograniczać ich wpływ, a także wdrażać odpowiednie strategie prewencyjne.

Zgodnie z koncepcją konkurencyjności systemowej, konkretne instytucje odpowiedzialne są za podejmowanie inicjatyw zapewniających właściwą identyfikację ryzyka w procesie budowania odporności gospodarki. Są to: władze krajowe i samorządowe, instytucje naukowe, organizacje non-profit, partnerstwa sektora prywatnego (przedsiębiorstwa) oraz obywatele, rodziny i gospodarstwa domowe. Każda z tych instytucji odgrywa inną rolę zarówno w analizie długotrwałych czynników zagrożeń, jak i analizie przed i po wstąpieniu zagrożenia (szoku) (tab. 4.)

Tabela 4. Rola kluczowych instytucji w budowaniu odporności gospodarki

Instytucja	Długotrwałe czynniki zagrożeń	Przed wystąpieniem zagrożenia (szoku)	Po wstąpieniu zagrożenia (szoku)
władze krajowe i samorządowe	Identyfikacja silnych i słabych stron oraz szans i zagrożeń w systemie gospodarczym. Poszukiwanie zasobów dla przeciwdziałania długotrwałym czynnikom zagrożeń.	Integracja zarządzania kryzysowego i tworzenia planów odporności gospodarki do rozwoju gospodarczego. Włączenie oceny ryzyka do planów rozwoju gospodarczego.	Odbudowa krytycznej infrastruktury i sieci, aby zapewnić stabilny wzrost i uniknąć przyszłych strat. Koordynowanie zasobów w celu wsparcia odpornej gospodarki i zapewnienia ożywienia gospodarczego.
instytucje naukowe	Badanie i analizowanie przyczyn i potencjalnych interwencji. Opracowanie strategii opartych na dowodach w celu budowania odporności.	Dostarczanie kluczowych danych i rekomendacji dotyczących polityki, aby wspierać podejmowanie świadomych decyzji i tworzyć skuteczne strategie ograniczania ryzyka i reagowania na zagrożenie.	Prowadzenie badań, w celu zrozumienia zmian w środowisku naturalnym, na rynku pracy i środowisku gospodarczym.

organizacje non-profit	Dostarczanie specjalistycznej wiedzy, zasobów i ekspertyz, które wzmacniają i rozszerzają wysiłki rządu na rzecz budowania odporności, a także rozwiązują podstawowe przyczyny długotrwałych zagrożeń.	Tworzenie partnerstw, które mają na celu szybką mobilizację w przypadku wystąpienia zagrożenia (szoku).	Wsparcie działań rządu i pomoc w procesie odbudowy. Zapewnienie przepływu zasobów do najbardziej narażonych miejsc.
partnerstwa sektora prywatnego (przedsiębiorstwa)	Wykorzystanie zasobów i zarządzania zwinnego (agile), w celu wsparcia działań na rzecz wzmocnienia innowacyjności i zdolność adaptacji.	Rozwijanie i wzmacnianie łańcuchów dostaw oraz sieci współpracy biznesowej.	Zapewnienie kluczowych zasobów, usług i rozwiązań adaptacyjnych w procesie odbudowy.
obywatele, rodziny i gospodarstwa domowe	Aktywne uczestnictwo w działaniach na rzecz wzmacniania odporności społeczeństwa. Dostarczanie spostrzeżeń dotyczących lokalnych potrzeb.	Wspieranie działań mających na celu zmniejszenie ryzyka i podatności na wstrząsy.	Kontakt i współpraca z sąsiadami. Tworzenie sieci wsparcia na rzecz odbudowy. Wyciągnięcie wniosków na przyszłość.

Źródło: Guibert i in. 2023, s. 7.

W różnych przestudiowanych koncepcjach i podejściach budowania odporności gospodarki, podkreślana jest rola współpracy kluczowych aktorów życia gospodarczego (czyli przedsiębiorstw, instytucji naukowych i rządowych) zgodnie z koncepcją współpracy w modelu Potrójnej Helisy (rozdział 2.).

Proces identyfikacji ryzyka obejmuje kilka kluczowych kroków, które w literaturze naukowej często są dzielone na różne kategorie. Zazwyczaj pierwszym etapem działań jest ustalenie kontekstu wewnętrznego i zewnętrznego organizacji lub systemu, który ma być chroniony przed ryzykiem. Następnie identyfikowane są konkretne zagrożenia i ich potencjalne źródła. W dalszej kolejności oceniane są prawdopodobieństwa ich wystąpienia, a także prowadzona analiza potencjalnych skutków oraz priorytetyzacja ryzyka. W końcowym etapie analizowane są systemowe interakcje pomiędzy różnymi sektorami gospodarki oraz powiązaniami globalnymi, które mogą wpływać na występowanie i rozprzestrzenianie się ryzyka. Powyższe postępowanie powinno obejmować analizę ryzyka wystąpienia szerokiego spektrum niebezpieczeństw mających źródło m.in. w następujących zagrożeniach:

- funkcjonowanie struktur instytucjonalnych,
- problemy polityczne,
- niestabilność i turbulencje gospodarcze,
- zmiany klimatyczne,
- pandemie i inne zagrożenia zdrowotne,
- katastrofy naturalne (powodzie, pożary, wybuchy wulkanów itp.).

3.2 Zarządzanie ryzykiem

W kolejnym etapie wzmacniania odporności gospodarki i przedsiębiorstw kluczowe jest zarządzanie ryzykiem. Obejmuje ono strategie redukowania podatności gospodarki na zakłócenia. Przedsiębiorstwa i rządy opracowują działania prewencyjne i wdrażają narzędzia, które zmniejszają ryzyko przerwania działalności.

Przedsiębiorstwa:
- dywersyfikują źródła pozyskiwania surowców,
- optymalizują łańcuchy dostaw,
- rozwijają infrastrukturę informacyjną z wykorzystaniem nowoczesnych technologii cyfrowych.

Rządy:
- wdrażają systemy wczesnego ostrzegania,
- inwestują w infrastrukturę krytyczną,
- wprowadzają właściwe rozwiązania legislacyjne,
- budują system wsparcia finansowego,
- zapewniają bezpieczeństwo energetyczne.

Jednym z podstawowych działań zarówno w UE, jak i w USA jest dywersyfikacja łańcuchów dostaw, spowodowana zwłaszcza doświadczeniami wynikającymi z pandemii COVID-19 oraz wojny w Ukrainie. Stany Zjednoczone skupiły się na reshoringu[3] kluczowych branż, w szczególności technologii ICT, farmaceutyków i półprzewodników, aby zmniejszyć zależność od zagranicznych dostawców, zwłaszcza z krajów takich jak Chiny. Podobnie UE uruchomiła politykę „otwartej autonomii strategicznej" (Komisja Europejska 2023), której celem jest zmniejszenie zależności od rynków zewnętrznych poprzez inwestowanie w produkcję w krajach członkowskich, w szczególności w zakresie zielonych technologii, energii i infrastruktury cyfrowej. Jednym ze szczególnie istotnych działań UE w tym zakresie jest wsparcie budowy półprzewodników na terenie Unii (Komisja Europejska 2024), także poprzez przyjęcie tzw. Chips Act – europejskiej ustawy o mikroprocesorach (Komisja Europejska 2024a).

W wyniku międzynarodowej specjalizacji łańcuchy dostaw we współczesnej gospodarce są zglobalizowane i rozdrobnione jednocześnie. Przynosi to korzyści ekonomiczne, a jednocześnie może zwiększać ryzyko rozprzestrzeniania się zagrożeń wzdłuż łańcuchów dostaw. Ze względu na nasilenie poważnych sytuacji kryzysowych i katastrof, konieczne jest opracowanie skuteczniejszych strategii mających na celu wzmocnienie ich odporności (supply chain resilience – SCR).

3 Przeniesienie działalności lub części działalności przedsiębiorstwa z kraju trzeciego ponownie bliżej siedziby organizacji.

Podstawowym aspektem zapewniania bezpieczeństwa łańcucha dostaw jest budowanie rozwiązań logistycznych mających na celu płynne dostarczanie produktów. Zwiększenie elastyczności oznacza poprawę zdolności firmy lub samego łańcucha do dostosowywania się do zmieniających się wymagań przy minimalnym czasie i wysiłku. Innym rozwiązaniem pozwalającym na radzenie sobie z zakłóceniami jest tworzenie nadmiarowości poprzez wykorzystanie wolnych mocy produkcyjnych. Takie działanie wiąże się jednak ze zwiększeniem kosztów. Natomiast poprawa zwinności wzmacnia zdolność do szybkiego reagowania na nieprzewidywalne zmiany podaży lub popytu. Tworzenie współpracy w łańcuchu dostaw prowadzi do uzyskania wzajemnych korzyści, np. poprzez dzielenie się informacjami, materiałami i innymi zasobami niezbędnymi do reagowania na zakłócenia (Yang i in. 2023; Dey i in. 2023; Yan i in. 2023).

Kluczowe znaczenie w redukcji ryzyka katastrof naturalnych, takich jak trzęsienia ziemi, tsunami czy huragany mają systemy wczesnego ostrzegania (Early Warning Systems – EWS). W ich skład wchodzą zintegrowane sieci czujników, systemy analizy danych oraz mechanizmy komunikacji, które umożliwiają szybkie ostrzeżenie społeczności o zbliżającym się zagrożeniu. Na przykład, po niszczycielskim tsunami na Oceanie Indyjskim w 2004 roku, rząd Indii utworzył Indyjski System Wczesnego Ostrzegania przed Tsunami (Indian Tsunami Early Warning System – ITEWS) z siedzibą w Hajdarabadzie, które podlega Ministerstwu Nauk o Ziemi (MoES). ITEWS wykorzystuje dane z krajowych i międzynarodowych sieci obserwacyjnych stacji sejsmicznych, stacji pomiaru poziomu morza i boi tsunami rozmieszczonych na Oceanie Indyjskim i Spokojnym. Dane z około 400 sejsmometrów są odbierane w czasie rzeczywistym i przetwarzane automatycznie w celu wykrycia trzęsienia ziemi o magnitudzie 4.0 lub większej w dowolnym miejscu na świecie (Sunanda i in. 2016; Satake 2014).
Równie istotne są inwestycje w infrastrukturę krytyczną, która obejmuje takie sektory jak: energetyka, wodociągi, transport czy telekomunikacja. Nieodzownym elementem wzmacniania odporności gospodarek jest ochrona infrastruktury krytycznej oraz rozwój technologii zabezpieczeń przed zagrożeniami, w tym atakami cybernetycznymi i fizycznymi.

W kontekście budowania infrastruktury zapobiegającej powodziom wyróżniającym się przykładem jest Holandia, będąca pionierem w zakresie zarządzania ryzykiem powodzi. Holenderski system ochrony przeciwpowodziowej obejmuje zarówno tradycyjne struktury, takie jak tamy i groble, jak i nowoczesne systemy zarządzania wodą, takie jak Room for the River[4]. Inicjatywa ta polega na inwestowaniu w infrastrukturę hydrotechniczną oraz tworzenie przestrzeni, gdzie woda może swobodnie rozlewać się w przypadku wzrostu poziomu rzek, co minimalizuje ryzyko powodzi (De Bruijn i in. 2008).

Kolejnym warunkiem koniecznym do budowania odpornej i konkurencyjnej globalnie gospodarki jest elastyczność fiskalna i koordynacja polityki w tym zakresie, umożliwiająca rozwój sektora prywatnego w zakresie prowadzenia prac badawczo-rozwojowych. Zarówno USA, jak i UE stosują narzędzia monetarne i fiskalne, aby reagować na kryzysy na poziomie makroekonomicznym. Polityka pieniężna amerykańskiej Rezerwy Federalnej, w tym tzw. „luzowanie ilościowe[5]" podczas kryzysu finansowego w 2008 r. i pandemii COVID-19, zapewniła wówczas płynność na rynkach i bodźce, które miały wspierać funkcjonowanie gospodarki w czasie kryzysu.

4 https://www.dutchwatersector.com/news/room-for-the-river-programme
5 Definicja pojęcia – patrz: Luzowanie ilościowe (NBP 2024), https://nbp.pl/wp-content/uploads/2022/09/luzowanie-ilosciowe.pdf

Przez dziesięciolecia Stany Zjednoczone stały na czele inicjatyw badawczo-rozwojowych i tworzenia innowacji technologicznych poprzez olbrzymie inwestycje (publiczne i prywatne) w badania i rozwój różnych sektorów gospodarki. Efektem tych działań stał się ekosystem tzw. Doliny Krzemowej, którego podwaliną były ogromne fundusze rządowe przeznaczone na rozwój technologii i obronność. Efektem współpracy sektora publicznego i prywatnego było stworzenie unikalnego ekosystemu podmiotów prywatnych, uczelni i firm pracujących na zlecenie rządu USA, w którym wykształcono nie tylko technologie, ale również kapitał ludzki, konieczny do ich dalszego rozwijania. UE próbuje realizować podobne strategie poprzez inicjatywy takie jak programy grantowe wpierające inicjatywy badawczo-rozwojowe (np. Horyzont Europa, Digital Europe Programme, European Innovation Council – EIC), które promują badania i rozwój w wielu obszarach technologicznych – m.in. zrównoważonej energii, technologii cyfrowych i opieki zdrowotnej.

Unijny fundusz Next Generation EU, czyli pakiet naprawczy i stymulacyjny o wartości 806 mld euro, miał na celu zapewnienie skoordynowanej odbudowy po pandemii. Zapewnione środki były przeznaczone na osiągnięcie planów Unii Europejskiej w konkretnych obszarach, zidentyfikowanych jako strategiczne kierunki jej rozwoju. Jednym z nich są inwestycje w zieloną transformację. UE zdecydowała się na budowanie odporności i niezależności ekonomicznej poprzez transformację w kierunku bardziej ekologicznych gospodarek. Zarówno unijny Zielony Ład, jak i amerykańska ustawa o redukcji inflacji oferują znaczne inwestycje w energię odnawialną, mające na celu zmniejszenie zależności energetycznej i wspieranie zrównoważonego przemysłu. Wobec tego kluczowe są działania na rzecz dywersyfikacji źródeł energii (rozwój odnawialnych źródeł energii, zwiększenie liczby dostawców) oraz modernizacji i zabezpieczenia krytycznych elementów infrastruktury (sieci przesyłowych, elektrowni, magazynów energii), tak aby były odporne na awarie i ataki. Ważne jest również budowanie rezerw strategicznych – gromadzenie zapasów paliw i energii oraz stosowanie inteligentnych sieci energetycznych i systemów zarządzania energią, które optymalizują zużycie energii i zapobiegają przeciążeniom w sieci.

3.3 Wdrażanie mechanizmów adaptacyjnych

Zarządzanie kryzysowe oraz mechanizmy adaptacyjne stanowią trzeci kluczowy komponent wzmacniania odporności gospodarki. Przedsiębiorstwa oraz rządy wprowadzają procedury, które umożliwiają szybkie dostosowanie się do nowych warunków, takich jak np. zmiany struktury i sposobów zatrudnienia (elastyczność pracy – praca zdalna), oraz automatyzacja procesów (rozdział 1.3.).

Budowanie przez przedsiębiorstwa odporności łańcuchów dostaw poprzez m.in.: dywersyfikację dostaw, fragmentaryzację łańcuchów czy nawiązywanie partnerstw strategicznych, umożliwia podtrzymanie działalności biznesowej w sytuacji zagrożenia. Możliwość dostarczania oferty klientom, nawet w obliczu drastycznie rosnących kosztów, pozwala na przetrwanie kryzysu i adaptację do nowych warunków. Zmiana modeli biznesowych oraz niezwykle dynamiczna transformacja cyfrowa jest doskonałym przykładem wdrażania mechanizmów adaptacyjnych w przedsiębiorstwach w obliczu ostatnich zagrożeń jakimi są pandemia COVID-19 czy wojna w Ukrainie.

Główne kierunki zmian modeli biznesowych to:

- wykorzystanie pracy zdalnej i zmiana struktury zatrudnienia,
- rozwój sprzedaży internetowej,
- wykorzystanie technologii cyfrowych w celu usprawnienia procesów zarządzania (np. Internet Rzeczy czy blockchain) oraz przetwarzania danych strategicznych (Big Data czy rozwiązania chmurowe),
- pozyskiwanie komponentów na aukcjach internetowych.

Ważnym aspektem jest też tworzenie partnerstw publiczno-prywatnych (PPP) (przykłady – rozdział 2.3.), które zwiększają efektywność reagowania na kryzysy poprzez lepszą koordynację zasobów w oparciu o współpracę głównych aktorów życia gospodarczego (model Potrójnej Helisy).

W warunkach kryzysu kluczowym elementem jest właściwa alokacja zasobów tam, gdzie są one najbardziej potrzebne, z naciskiem na sektor infrastruktury krytycznej (np. służba zdrowia, energetyka, komunikacja). Możliwe jest wówczas zapewnienie bezpieczeństwa i ograniczanie skutków kryzysu. Alokacja zasobów powinna być elastyczna, aby umożliwić szybkie dostosowanie się do zmieniających się warunków w sytuacji zagrożenia. Zarządzanie priorytetami może być wspierane przez narzędzia analityczne i modele decyzyjne. Przykładem potrzeby takiej koordynacji zasobów jest wsparcie w przypadku zagrożenia powodzią, co pokazała powódź z września 2024 roku, która dotknęła południowe i zachodnie województwa Polski. Ponadto bardzo ważnym elementem skutecznej koordynacji zasobów jest zarządzanie przepływem informacji między różnymi podmiotami zaangażowanymi w działania kryzysowe. Odpowiednie i sprawne systemy informatyczne, platformy komunikacyjne oraz integracja danych pozwalają na bieżące dostosowywanie działań. Komunikacja między organizacjami publicznymi, prywatnymi i międzynarodowymi ma kluczowe znaczenie dla szybkiego reagowania na zagrożenie. Współpraca międzysektorowa (sieci współpracy), współpraca w klastrach i współpraca w regionach umożliwia lepsze wykorzystanie dostępnych zasobów. Ważnym elementem jest także integracja różnych poziomów władzy (lokalnych, regionalnych, centralnych) oraz współpraca z organizacjami międzynarodowymi.

Szczególnie istotne w procesie wdrażania mechanizmów adaptacyjnych w warunkach kryzysowych, tj. podczas katastrof naturalnych, konfliktów zbrojnych czy cyberataków jest zapewnienie bezpieczeństwa energetycznego, polegającego na ochronie i stabilnym dostarczaniu energii poprzez sprawne wykorzystanie komponentów działań na rzecz zwiększenia bezpieczeństwa energetycznego.

3.4. Ocena skuteczności

Ocena skuteczności i ciągłe doskonalenie mechanizmów wzmocnienia odporności gospodarki opiera się na permanentnym, cyklicznym i dynamicznym podejściu do zarządzania ryzykiem. Nadrzędnym celem jest zapewnienie aktualizacji danych i dostosowywane do zmieniających się zagrożeń.

Kluczowe zatem staje się ciągłe analizowanie wskaźników wydajności, takich jak czas reakcji na kryzys, szybkość odbudowy kluczowych sektorów oraz koszty związane z zarządzaniem kryzysowym. Ważne jest również regularne analizowanie strategii pod kątem nowych danych, by ocenić, czy podejmowane działania rzeczywiście zmniejszają podatność gospodarki na zagrożenia. Przykładem integracji danych z zakresu bezpie-

czeństwa publicznego i ich wykorzystania jest projekt zrealizowany przez Główny Urząd Statystyczny pt. „Pozyskanie nowych wskaźników z zakresu bezpieczeństwa publicznego przydatnych do oceny dostępności, jakości i efektywności usług publicznych" współfinansowany z funduszy UE (GUS 2015). Innym przykładem jest platforma do zarządzania kryzysowego i redukcji ryzyka PARATUS, będąca efektem projektu finansowanego ze środków programu Horizon Europe. Jest to konsorcjum 19 partnerów z 11 krajów, w tym przedstawicieli organizacji badawczych, organizacji pozarządowych, małych i średnich przedsiębiorstw, pierwszych i drugich respondentów oraz władz lokalnych i regionalnych. Platforma oferuje wsparcie w analizie i ocenie dynamicznych scenariuszy ryzyka oraz ryzyka systemowego spowodowanego złożonymi katastrofami (Centrum Rozwiązań Systemowych 2024). W końcu szeroko wykorzystywane są szybkie systemy powiadamiania o zagrożeniach, gdzie komunikacja odbywa się przez kilka kanałów tj.: SMS, email, powiadomienie głosowe czy formularz zgłoszeniowy na stronie internetowej.

Ocena skuteczności wymaga również systematycznego stosowania metod oceny ryzyka, takich jak analizy scenariuszy, symulacje kryzysowe czy testy odporności. Umożliwiają one zidentyfikowanie słabych punktów w obecnych mechanizmach oraz weryfikację gotowości gospodarki na kryzysy. Wykorzystywane są w tym celu różne metody analizy i prognozowania statystycznego, modelowania ekonometrycznego czy testowania istniejących rozwiązań. Ciekawym przykładem są testy warunków skrajnych (tzw. stress tests) wykorzystywane przez Europejski Bank Centralny, które służą europejskiemu nadzorowi bankowemu do oceny, w jakim stopniu banki są zdolne poradzić sobie z szokami finansowymi i gospodarczymi. Ich szczególne znaczenie widoczne jest w czasie skrajnych zagrożeń np. kryzysu finansowego i gospodarczego. Wykonywanych jest kilka rodzajów stress testów: testy coroczne (ogólnounijne, tematyczne i prognostyczne), testy oceny wszechstronnej oraz makroostrożnościowe (skupione nie tyle na konkretnych bankach, co na stabilności finansowej i skutkach systemowych). Prowadzone są one w poszczególnych bankach i grupach bankowych (Europejski Bank Centralny 2024).

Wzmacnianie odporności gospodarki wymaga także ciągłego doskonalenia narzędzi technologicznych. Technologie cyfrowe, takie jak sztuczna inteligencja, Big Data oraz Internet Rzeczy mogą być wykorzystane do prognozowania zagrożeń i automatyzacji procesów reakcji kryzysowej (więcej na ten temat w drugiej części raportu).

Regularne przeglądy działań, ich optymalizacja oraz wdrażanie nowych narzędzi i technologii pozwala na dynamiczne dostosowywanie gospodarki do zmieniających się zagrożeń, co w dłuższej perspektywie wzmacnia jej odporność.

4. Rola klastrów w zapobieganiu zagrożeniom

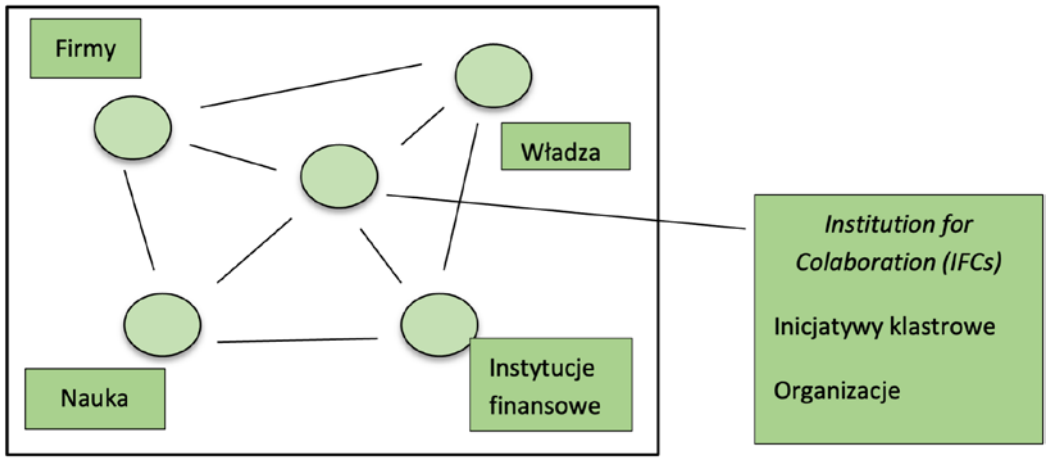
Klastry, jako specyficzna forma kolokacji i koopetycji przedsiębiorstw, są środowiskiem, w którym ujawniają się korzyści mające znaczenie dla budowania nie tylko przewagi konkurencyjnej przedsiębiorstwa, ale również wzmacniania interakcji i współpracy podmiotów modelu potrójnej helisy. Tym samym klastry mogą odgrywać znaczącą rolę we wzmacnianiu odporności gospodarki w sytuacji zagrożenia oraz zapobiegania tym zagrożeniom.

4.1. Definicja i rola klastrów

Problematyka definiowania klastra jest nieustająco przedmiotem żywej dyskusji badaczy. Określenie atrybutów klastra zależy bowiem od wielu czynników związanych z jego charakterem (sektorem), stopniem zawansowania współpracy, zakresem i zasięgiem działania oraz charakterystyką powiązań struktury organizacyjnej. Najczęściej przywoływaną w literaturze i wykorzystywaną jako podstawa wielu badań jest definicja klastra o charakterze globalnym M. Portera, który definiuje klaster jako „(…) geograficzne skupisko wzajemnie powiązanych firm, wyspecjalizowanych dostawców jednostek świadczących usługi, firm działających w pokrewnych sektorach i związanych z nimi instytucji (np.: uniwersytetów, jednostek normalizacyjnych i stowarzyszeń branżowych) w poszczególnych dziedzinach, konkurujących między sobą ale również współpracujących" (Porter 2001). M.J. Enright definiuje klaster jako zbiór powiązanych ze sobą przedsiębiorstw, reprezentujących ten sam lub zbliżony sektor przemysłu lub usług, położonych na tym samym obszarze (Enright 1992). Powyższa definicja wskazuje kilka najistotniejszych cech klastra, jakimi są: koncentracja geograficzna, specjalizacja i sieć powiązań. Podobnie Rosenfeld określa klastry jako skupiska firm, które poprzez bliskość geograficzną oraz ścisłą współpracę uzyskują możliwość kreowania efektu synergii bez względu na skalę zatrudnienia (Rosenfeld 1997). Klastry mogą być definiowane także jako systemy, w których członkostwo opiera się na niezależności podmiotów, a wiodącą rolę pełnią powiązania pomiędzy podmiotami klastra, które jedocześnie współpracują i konkurują (zjawisko koopetycji – co-opetition, Jankowska 2012).

Podmiotami klastra są nie tylko przedsiębiorstwa, ale również ściśle współpracujące z nimi instytucje publiczne oraz jednostki naukowe (Roleandt&den Hertog 1999) współdziałające w ramach Potrójnej Helisy. Ponadto za zapewnienie zewnętrznych zasobów finansowych odpowiedzialne są wyspecjalizowane instytucje finansowe oraz koordynatorzy klastrów, których równie istotna rola skupia się na czynnościach związanych z efektywnym zarządzaniem klastrem. Określa się je często jako tzw. Institutions for Collaboration (Sölvell i in. 2003) (rys. 9.).

Rysunek 9. Podmioty współpracujące w klastrze



Źródło: (Sölvell i in. 2003; Porter&Emmons 2003).

Z wielu definicji klastra można wyodrębnić najczęściej wymieniane cechy klastra (por. także Ketels 2015) tj.:

- geograficzna koncentracja wyspecjalizowanych przedsiębiorstw,
- odpowiednia liczba przedsiębiorstw – tzw. masa krytyczna klastra,
- powiązania między przedsiębiorstwami – pionowe i poziome zależności, często mające nieformalny charakter,
- jednoczesna konkurencja i współpraca między firmami,
- podejmowanie współpracy przedsiębiorstw z instytucjami nauki oraz władzami,
- przepływ wiedzy, technologii i innowacji między podmiotami tworzącymi klastry.

Wiele definicji i typologii klastrów przywołuje pojęcie sieci powiązań pomiędzy podmiotami, co sugerowałoby istnienie atrybutów sieci w koopetycji klastrów. Jednak pomimo cech wspólnych charakterystycznych zarówno dla powiązań sieciowych, jak i klastrów, istnieje wachlarz wyróżników wskazujących na różnice między nimi. Każdy klaster jest siecią, natomiast nie każda sieć może być klastrem (Jankowska 2012). Do cech wspólnych sieci i klastrów najczęściej zalicza się: dobrowolność uczestnictwa, zachowanie odrębności prawnej i ekonomicznej członków, wzajemne powiązania i zależność strategiczną od innych podmiotów, tworzenie kanałów informacyjnych oraz transfer zasobów pomiędzy jednostkami. Klastry jednak zdecydowanie różnią się od sieci w kilku kluczowych obszarach. Klaster dostarcza wyspecjalizowane usługi w konkretnej lokalizacji geograficznej, sieć może być rozproszona. Podmioty mogą być oficjalnie zarejestrowane w klastrze, ale niezarejestrowane organizacje osadzone w lokalizacji klastra są również jego nieświadomym członkiem i czerpią podobne korzyści z tej współpracy, co członkowie zarejestrowani. Sieć posiada wyłącznie zarejestrowanych członków i bazuje na umowach kontraktowych. Klaster opiera się na budowaniu więzi nieformalnych i wzajemnego zaufania. Sieci opierają się na kooperacji, klastry na koopetycji. Sieci rozwijają wspólne cele biznesowe, klastry zaś wspólną wizję rozwoju (por. Dzierżankowski i in. 2011; Gorynia&Jankowska 2008, cyt. za Kuczewska 2020).

Sieciowy charakter współpracy w klastrach zwraca uwagę na bardzo istotną rolę lidera/koordynatora grupy powiązanych podmiotów i organizacji, niezależnie od stopnia sformalizowania klastra. Jest on odpowiedzialny za kierowanie i strategię rozwoju inicjatywy i nierzadko od niego zależy dynamika rozwoju współpracy.

4.2. Modele i efekty współpracy w klastrach

Jedną z najczęściej przytaczanych typologii klastrów jest podział ze względu na wielkość i ilość podmiotów tworzących klaster oraz na rodzaj powiązań pomiędzy nimi. Możliwe jest wyróżnienie następujących typów klastrów (Markusen 1996; Barkley&Henry 2001):

- Klastry sieciowe (typ Marshallowski – Marshallian clusters) – charakteryzują się dominacją małych i średnich przedsiębiorstw o wysokiej specjalizacji. Obejmują głównie branże rzemieślnicze lub usługi związane z produkcją.
- Klastry koncentryczne (oś i szprychy – hub and spoke clusters) – charakteryzują się silną dominacją jednej lub kilku dużych firm otoczonych przez liczne małe i średnie przedsiębiorstwa, które pełnią rolę dostawcy i podwykonawcy podmiotu kluczowego.
- Klastry satelitarne (satellite platforms) – klastry zdominowane przez małe i średnie podmioty, najczęściej oddziały zewnętrznych względnie niezależnych firm wielozakładowych. Korzyści podmiotów klastra uzależnione są od współpracy z dużymi firmami zewnętrznymi.
- Klastry instytucjonalne (state-anchored industry clusters) – powstają w regionach, w których lokalna działalność biznesowa zdominowana jest przez instytucje pu-

bliczne lub non-profit, a rozwój klastra zależy od intensywności relacji z instytucjami publicznymi.

Podobna do powyższego podziału klasyfikacja klastrów, wykorzystująca kryterium modelu struktury organizacyjnej oraz kraju, w którym najczęściej występuje dzieli je na typy: włoski, duński oraz holenderski (Gorynia&Jankowska 2007).

- Klaster typu włoskiego jest (jak wskazuje nazwa) charakterystyczny dla koncentracji we Włoszech (Brusco 1990; Dei Ottani 1994). Typ ten wyróżnia się dominacją MŚP o silnej i elastycznej specjalizacji, które silnie rywalizują i jednocześnie współpracują tworząc system powiązań sieciowych opartych na zaufaniu.
- Model klastra duńskiego opiera się na koncepcji klastra koncentrycznego (oś i szprychy) z centralną dominacją dużego, silnego podmiotu oraz sieci powiązanych ze sobą i z podmiotem kluczowym MŚP. Klaster ten bazuje na sile wiodącej/wiodących korporacji, a jego koncepcja została wypracowana w latach 1988-1993 przez rząd duński w programie sieciowania. Model ten był również implementowany na Węgrzech oraz w Wielkiej Brytanii, USA, Kanadzie, Australii i Nowej Zelandii.
- Tzw. typ holenderski klastra bazuje na koncepcji klastra satelitarnego, gdzie rolę brokera sieciowego przejmuje jednostka naukowo-badawcza. Cechuje go udział przedsiębiorstw sektora MŚP bez podmiotu dominującego uzależnionych od podmiotu zewnętrznego (jednostki naukowo-badawczej) (Gorynia&Jankowska 2008).

Enright i Kai przedstawili klasyfikację klastrów wykorzystującą jako kryterium podziału stopień świadomości istnienia klastra oraz wpływ instytucji zewnętrznych na jego identyfikację i tworzenie (Enright&Kai 2000). Autorzy wyróżnili:

- Klastry działające (working clusters) – podmioty klastra tworzą gęstą sieć powiązań i świadomej współpracy.
- Klastry utajone (latent clusters) – posiadają masę krytyczną firm powiązanych siecią współpracy wystarczającą do czerpania korzyści z tworzenia klastrów, ale nie rozwinęły poziomu interakcji i przepływu informacji niezbędnych do ujawnienia korzyści z kolokacji.
- Klastry potencjalne (potential clusters) – posiadają niektóre elementy niezbędne do rozwoju udanych, działających klastrów, ale elementy te muszą zostać pogłębione i poszerzone.
- Klastry tworzone odgórnie (policy driven clusters) – identyfikowane i wybierane przez władze jako klastry strategiczne kwalifikujące się do uzyskania wsparcia, ale którym brakuje masy krytycznej lub korzystnych warunków rozwoju.
- Klastry życzeniowe (wishful thinking clusters) – są to klastry tworzone odgórnie przez władze, którym brakuje nie tylko masy krytycznej, ale także jakiegokolwiek szczególnego źródła korzyści, które mogłoby promować rozwój klastra.

Powyższa klasyfikacja skłania do zastanowienia nad trudnym i szeroko dyskutowanym tematem stopnia zaangażowania polityki wspierania klastrów w ich promocję i rozwój. Wydaje się oczywiste, iż zbyt duża dominacja klastrów tworzonych odgórnie i klastrów życzeniowych nie wpłynie pozytywnie na rozwój i promocję klastrów w danej gospodarce. Częściej to klastry potencjalne lub utajone są w stanie szybciej osiągnąć identyfikowalne korzyści współpracy, natomiast klastry odgórne lub życzeniowe szybko tracą na jakimkolwiek znaczeniu przy zmianie kierunku polityki wspierania klastrów i zainteresowania nimi przez władze (Ketels&Protsiv 2013; Dzierżanowski (red.) 2012; Kuczewska 2014).

Bogaty dorobek literatury w zakresie powstawania, rozwoju i funkcjonowania klastrów, nie tylko przywołuje ich atrybuty, ale również ujawnia źródła korzyści, które odnotowują podmioty w klastrach.

Biorąc pod uwagę liczne badania naukowe możliwa jest identyfikacja korzyści współpracy wpływających na produktywność podmiotów klastra (Gorynia& Jankowska 2008; Ketels 2003) czyli: korzyści skali, redukcja kosztów transakcyjnych, większa innowacyjność, stymulowanie przedsiębiorczości oraz rola kapitału społecznego dla przenikania i absorpcji wiedzy. Wynikają one z: dostępu podmiotów klastra do wyspecjalizowanych zasobów, dostawców, usług i infrastruktury; bliskości konkurentów napędzających skłonność do wdrażania innowacji; bliskości instytucji wspierających oraz innych podmiotów zewnętrznych związanych z klastrem. Ponadto istotną rolę odgrywa kapitał społeczny, tworzący przewagi wynikające z relacji międzyludzkich. Efektywność klastra zależy od silnej specjalizacji jego podmiotów i jest oparta na wiodącej branży, która pozwala na powielanie operacji, synergię oraz proces uczenia się (Audretsch&Feldman 1995; Dunning 2000). Klaster to również współpraca z innymi sektorami/klastrami oraz otwieranie się na zewnątrz. Uzyskiwanie pozytywnych efektów, samoczynne przenikanie wiedzy (knowledge spillover) oraz duże znaczenie kapitału społecznego zależą od podmiotów tworzących klaster, ich jednoczesnej konkurencji i kooperacji oraz uzyskania odpowiedniej masy krytycznej.

4.3. Potencjalna strategiczna rola klastrów jako organizacji bezpośredniego wsparcia

Organizacje klastrowe zarówno w Unii Europejskiej, jak i Stanach Zjednoczonych odgrywają także kluczową rolę we wspieraniu rządów i struktur krajowych w ochronie małych i średnich przedsiębiorstw podczas kryzysów, takich jak klęski żywiołowe i zakłócenia w łańcuchu dostaw na poziomie globalnym. Klastry te, skupiające przedsiębiorstwa, instytucje badawcze ale też organizacje sektora publicznego, wspierają współpracę między podmiotami, rozwój innowacji, a także przygotowywanie i wdrażanie strategii szybkiego reagowania w celu zapewnienia odporności gospodarek krajowych.

Klastry, jako strategiczne partnerstwa specjalistycznych przedsiębiorstw, odgrywają kluczową rolę w procesie przeciwdziałania zagrożeniom, zarówno w krótkoterminowych działaniach reaktywnych, jak i w długoterminowym zarządzaniu ryzykiem oraz wzmacnianiu odporności firm (tabela 5.).

W ramach działań doraźnych umożliwiają one efektywną mobilizację zasobów, zarówno ludzkich, jak i technologicznych, co jest szczególnie istotne w sytuacjach kryzysowych, takich jak katastrofy naturalne czy konflikty. Przykładowo klastry wspierają organizacje w działaniach humanitarnych i logistycznych, oferując szybkie rozwiązania w zakresie transportu, dostarczania pomocy i koordynacji działań.

W perspektywie długoterminowej, klastry pomagają na wszystkich etapach procesu budowania odporności przedsiębiorstw – od zarządzania ryzykiem, poprzez optymalizację łańcuchów dostaw, aż po wsparcie w budowie infrastruktury komunikacyjnej i koordynacyjnej.

Klastry odgrywają również znaczącą rolę we wdrażaniu mechanizmów adaptacyjnych, oferując wsparcie w zakresie innowacji, zarządzania strategicznego, realizacji projektów,

budowania potencjału cyfrowego i bezpieczeństwa energetycznego. Istotnym aspektem działalności klastrów jest ich funkcjonowanie jako platformy współpracy, szczególnie w modelu Potrójnej Helisy, angażującym do wspólnego działania przedsiębiorstwa, instytucje naukowe i administrację publiczną. Dzięki temu klastry wspomagają proces identyfikacji ryzyka oraz ocenę skuteczności działań prewencyjnych, co przyczynia się do budowy trwałej odporności na przyszłe kryzysy.

Tabela 5. Wsparcie ze strony klastrów w procesie wzmacniania odporności przedsiębiorstw na zagrożenia zewnętrzne

Mechanizmy wzmacniania odporności przedsiębiorstw w ujęciu procesowym	**Potencjalne wsparcie ze strony klastrów**
1. Identyfikacja ryzyka – identyfikacja i predykcja zagrożeń	1. Wykorzystanie relacji w modelu Potrójnej Helisy w procesie oceny działań kryzysowych. 2. Dzielenie się wiedzą w zakresie potencjalnych zagrożeń i udostępnienie narzędzi wspierających mitygację zagrożeń. 3. Podnoszenie świadomości uczestników. 4. Wskazywanie potencjalnych źródeł finansowania.
2. Zarządzanie ryzykiem – redukowanie podatności gospodarki na zakłócenia. Przedsiębiorstwa (poziom mikro): • dywersyfikacja źródeł zaopatrzenia, • optymalizacja łańcuchów dostaw, • rozwój infrastruktury informacyjnej	1. Rola partnerstw strategicznych w procesie wzmacniania łańcuchów dostaw. 2. Wsparcie w procesie rozwoju infrastruktury komunikacyjnej. 3. Proces knowledge spillover – samoczynne rozlewanie się wiedzy.
3. Wdrażanie mechanizmów adaptacyjnych Przedsiębiorstwa (poziom mikro): • zmiana modeli biznesowych, • wprowadzenie nowego modelu czasu pracy i zmiany struktury zatrudnienia (np. praca zdalna), • automatyzacja procesów i transformacja cyfrowa.	Rola koordynatorów klastrów: 1. Doradztwo i wsparcie w procesie wdrażania innowacji. 2. Doradztwo i wsparcie w zarządzaniu strategicznym oraz zarządzaniu projektami. 3. Budowanie potencjału cyfrowego i cyberbezpieczeństwa. 4. Budowanie bezpieczeństwa energetycznego.
4. Ocena skuteczności • symulacje kryzysowe, • analiza skuteczności działań prewencyjnych i zaradczych.	1. Wykorzystanie relacji w modelu Potrójnej Helisy w procesie oceny działań kryzysowych
Działania doraźne w sytuacjach zagrożenia: organizacja pomocy humanitarnej i logistycznej.	

Źródło: opracowanie własne.

Klastry, ze względu na swoje doświadczenia, możliwości i posiadaną sieć współpracy mogą szybko zmobilizować zasoby, aby pomóc MŚP w odbudowie np. po klęskach

żywiołowych. Sieci klastrowe ułatwiają również wzajemną współpracę, która zapewnia dostęp do technologii, infrastruktury oraz wiedzy i wsparcia specjalistycznego koniecznego w różnych obszarach funkcjonowania członków. Przykładowo podczas klęsk żywiołowych, np. powodzi lub pożarów lasów, Europejska Platforma Współpracy Klastrów (European Cluster Collaboration Platform – ECCP) pomagała koordynować działania na skalę międzynarodową. Poprzez zaoferowanie zaawansowanych technologii, wsparcie eksperckie, dostęp do funduszy, wymianę doświadczeń i wiedzy regionalne klastry we Włoszech i Hiszpanii zmobilizowały swoje zasoby, aby wesprzeć lokalne MŚP w sektorach rolnictwa i leśnictwa w radzeniu sobie ze skutkami niszczycielskich pożarów. Współpraca ta pomogła firmom w odbudowie i dostosowaniu się do zmieniających się warunków środowiskowych.

W Stanach Zjednoczonych klastry takie jak Texas Gulf Coast Innovation Cluster wspierały MŚP podczas huraganów i klęsk żywiołowych. Po huraganie Harvey w 2017 r. klaster zapewnił lokalnym MŚP dostęp do narzędzi cyfrowych do reagowania na katastrofy, danych w czasie rzeczywistym i sieci ekspertów. Pomogło to firmom w szybkim powrocie do funkcjonowania poprzez przywrócenie przerwanych łańcuchów dostaw, uzyskanie dostępu do finansowania pomocowego dla podmiotów, które ucierpiały w skutek huraganu i wykorzystanie wspólnych zasobów w celu zminimalizowania przestojów.

Z kolei amerykańska National AI Initiative tworzy platformę współpracy w ramach klastrów skupionych na AI, szczególnie w takich miastach jak Boston i Seattle, będących centrami rozwoju najnowocześniejszych technologii. Klastry te umożliwiają MŚP dostęp do federalnego finansowania badań oraz wykorzystania zaawansowanych narzędzi w zakresie sztucznej inteligencji i analizy danych, co zwiększa ich zdolność do globalnego konkurowania w szybko rozwijających się sektorach sztucznej inteligencji. Takie wsparcie ma zagwarantować konkurencyjność amerykańskich MŚP na arenie światowej w obliczu nasilającej się konkurencji międzynarodowej.

Należy wspomnieć również o European Cluster Alliance, organizacji zrzeszającej 22 krajowe organizacje klastrowe z terenu UE, która dzięki swojej aktywności odegrała bardzo ważną rolę podczas pandemii COVID-19 organizując i koordynując prace klastrów na poziomie europejskim. Do najważniejszych celów ECA należy: promocja klastrów i współpraca międzyklastrowa, wspieranie współpracy międzynarodowej, wspieranie interesów klastrów oraz przedstawianie wspólnego stanowiska klastrów wobec administracji europejskiej.

4.4. Przykłady działalności klastrów w zapobieganiu zagrożeniom

W nawiązaniu do tabeli 5. przedstawiającej potencjalne wsparcie ze strony klastrów w odniesieniu do mechanizmów wzmacniania odporności przedsiębiorstw poniżej zaprezentowane zostały przykłady klastrów i inicjatyw klastrowych międzynarodowych, zgodnie z następującym podziałem ról:

1. Rola partnerstw strategicznych w procesie wzmacniania łańcuchów dostaw oraz wsparcie w procesie rozwoju infrastruktury komunikacyjnej (knowledge spillover – rozlewanie się wiedzy).
2. Doradztwo i wsparcie w procesie wdrażania innowacji, zarządzania strategicznego, zarządzania projektami, budowania potencjału cyfrowego i bezpieczeństwa energetycznego.
3. Wykorzystanie relacji w modelu Potrójnej Helisy w procesie oceny działań kryzysowych.

Przykłady partnerstw przedsiębiorstw w klastrach, które wskazują zarówno na rolę klastrów w procesie wzmacniania łańcuchów dostaw, wsparcia w procesie rozwoju infrastruktury komunikacyjnej, jak i doradztwa oraz wsparcia w procesie wdrażania innowacji, zarządzania strategicznego, zarządzania projektami, budowania potencjału cyfrowego i bezpieczeństwa energetycznego:

- Organizacje klastrów technologicznych w USA, UE i Kanadzie okazały się kluczowe w budowaniu strategicznej odporności gospodarczej poprzez wspieranie innowacji, przenoszenie krytycznych łańcuchów dostaw, napędzanie zielonej transformacji i zwiększanie suwerenności cyfrowej. Dzięki współpracy międzynarodowej, partnerstwom publiczno-prywatnym i skupieniu się na sektorach zaawansowanych technologii, klastry te także mają potencjał by wspierać gospodarki krajowe w obliczu globalnych zakłóceń, zapewniając ich długoterminową stabilność gospodarczą i globalną konkurencyjność.
- Dzięki współpracy transgranicznej, partnerstwom publiczno-prywatnym i skupieniu się na sektorach zaawansowanych technologii, organizacje klastrów technologicznych w USA, UE i Kanadzie pozycjonują swoje regiony tak, aby były odporne i dobrze prosperowały w obliczu globalnych zakłóceń, zapewniając długoterminową stabilność gospodarczą i konkurencyjność.
- Kanadyjski klaster „Next Generation Manufacturing Supercluster – NGen", skupia się na budowaniu odpornych łańcuchów dostaw mających wspierać odporność państwowej gospodarki. Inwestując w rozwój innowacyjnych projektów opartych na miejscowym kapitale ludzkim, know-how oraz rozwijających lokalne możliwości technologiczne obejmujące zaawansowane technologie produkcyjne (m.in. automatyzacja i sztuczna inteligencja), Kanada zwiększa swoje krajowe zdolności produkcyjne w kluczowych sektorach, w tym w opiece zdrowotnej i czystych technologiach.

Przykłady partnerstw przedsiębiorstw w klastrach, które wskazują na rolę klastrów w procesie wzmacniania łańcuchów dostaw oraz wsparcia rozwoju infrastruktury komunikacyjnej:

- W reakcji na zakłócenia w globalnym łańcuchu dostaw, zaostrzone przez pandemię COVID-19, klastry technologiczne w USA, UE i Kanadzie odegrały kluczową rolę

w reshoringu i dywersyfikacji łańcuchów dostaw. W UE klastry skupione w ramach ECCP skupiły się na wzmocnieniu nowych autonomii łańcucha dostaw, zwłaszcza w sektorach strategicznych, takich jak farmaceutyka, energia i półprzewodniki.

- Inicjatywy podejmowane i realizowane w klastrach takich jak Silicon Saxony w Niemczech (jeden z największych i wiodących europejskich klastrów mikroelektronicznych) mają na celu zwiększenie produkcji półprzewodników w UE oraz zmniejszenie zależności od dostawców zewnętrznych. W odpowiedzi na globalny niedobór półprzewodników, klaster rozszerzył możliwości produkcyjne nie tylko na terenie lokalnym (kraju związkowego Saksonia), ale też na poziomie europejskim, zmniejszając zależność od importu z Azji. Klaster ten jest również jedną z 14 organizacji, skupionych obecnie w strategicznym projekcie UE Silicon Europe, mającym na celu zabezpieczenie łańcuchów dostaw półprzewodników poprzez ich produkcję w UE (Silicon Europe 2024). Inicjatywa Silicon Europe wspiera MŚP w sektorze półprzewodników poprzez finansowanie, międzynarodowe partnerstwa tworzące innowacje w zakresie półprzewodników oraz budowanie europejskich mocy produkcyjnych w tym krytycznym przemyśle.
- Stany Zjednoczone także położyły nacisk na reshoring krytycznych zdolności produkcyjnych poprzez działalność National Semiconductor Technology Center – NSTC). NSTC, który ma działać jako partnerstwo publiczno-prywatne, obejmuje ekosystemy, takie jak Dolina Krzemowa w Kalifornii i centrum technologiczne Austin. Ekosystemy te, wspierane przez ustawę „CHIPS and Science Act" (2022), mają na celu zwiększenie zdolności USA do produkcji półprzewodników, mających kluczowe znaczenie dla przemysłu obronnego, motoryzacyjnego i elektroniki użytkowej.

Przykłady partnerstw przedsiębiorstw w klastrach, które wskazują na rolę klastrów w zakresie doradztwa oraz wsparcia w procesie wdrażania innowacji, zarządzania strategicznego, zarządzania projektami, budowania potencjału cyfrowego i bezpieczeństwa energetycznego:

- Klastry technologiczne również mają kluczowe znaczenie dla rozwoju innowacji, zwłaszcza w zakresie zielonych technologii. Ma duży wpływ na długoterminową odporność gospodarczą w świecie ograniczonym pod względem emisji dwutlenku węgla. Wspomniana już europejska platforma ECCP animuje i wspiera współpracę międzynarodową klastrów w zakresie zielonej energii, transformacji cyfrowej i rozwiązań gospodarki o obiegu zamkniętym. Na przykład Klaster Zielonej Energii w Danii (Energy Cluster 2024) odegrał kluczową rolę w rozwoju technologii morskiej energii wiatrowej, które przyczyniają się do tworzenia niezależności energetycznej Danii. Stanowią one także doskonały przykład budowania ogólnego bezpieczeństwa gospodarczego, zwłaszcza w zakresie energetyki i tworzenia ekonomii odpornej na globalne wstrząsy energetyczne.
- W Stanach Zjednoczonych klastry technologiczne przewodziły postępom w dziedzinie energii odnawialnej, pojazdów elektrycznych (EV) i technologii akumulatorów. Klastry motoryzacyjne skupione w stanie Michigan, a szczególnie Detroit, tradycyjnie koncentrujące się na produkcji silników spalinowych, stały się liderami w rozwoju pojazdów elektrycznych. Zmiana kierunku była spowodowana przez naciski rządu USA na wdrażanie innowacji w zakresie czystej energii (np. Inflation Reduction Act z 2022 roku). Wysiłki te mają na celu nie tylko ograniczenie emisji dwutlenku węgla, ale także stworzenie nowoczesnych lokalnych gałęzi przemysłu, które oparte są na innowacjach, mogą konkurować globalnie, a także są bardziej odporne na ryzyka związane z dynamicznymi zmianami branży motoryzacyjnej

i rynku energii. Kanadyjska Clean Resource Innovation Network – CRIN jest organizacją klastrową skupiającą się na rozwijaniu rozwiązań z zakresu czystych technologii w sektorze energetycznym. Wspierając partnerstwa między środowiskiem akademickim, przemysłem i rządem, CRIN pomaga Kanadzie przejść na gospodarkę niskoemisyjną, zapewniając jednocześnie bezpieczeństwo energetyczne, szczególnie w sektorach, które tradycyjnie były zależne od ropy i gazu.

- W erze rosnącej cyfryzacji klastry technologiczne mają również kluczowe znaczenie dla zapewnienia suwerenności i bezpieczeństwa cyfrowego. Nacisk UE na suwerenność cyfrową doprowadził do inwestycji w klastry, które promują autonomię technologiczną w takich obszarach jak: sztuczna inteligencja, przetwarzanie w chmurze i cyberbezpieczeństwo. Na przykład Europejskie Huby Innowacji Cyfrowych (EDIH), wspierane przez program Digital Europe Programme, mają w swym założeniu zapewniać wsparcie dla MŚP w zakresie wdrażania technologii cyfrowych, zwiększając tym samym ich konkurencyjność i odporność na globalne wstrząsy. Klastry bardzo często są członkami czy nawet koordynatorami EDIH.
- Stany Zjednoczone, poprzez silne innowacyjne ekosystemy, takie jak Dolina Krzemowa, czy środowiska stworzone wokół uczelni technicznych (np. Massachusetts Institute of Technology – MIT w Cambridge, Massachusetts) nadal przodują w światowych innowacjach w zakresie technologii cyfrowych, w tym sztucznej inteligencji, obliczeń kwantowych i biotechnologii. Klastry te są też silnie wspierane przez politykę rządową, taką jak National AI Initiative Act (2021), która zachęca do federalnych inwestycji w badania i rozwój sztucznej inteligencji. Wspierając innowacje w tych krytycznych obszarach, Stany Zjednoczone zapewniają sobie pozycję lidera technologicznego i odporność w obliczu globalnej konkurencji.
- Kanadyjski Digital Technology Supercluster jest kolejnym przykładem tego, jak klastry przyczyniają się do budowania i rozwoju odporności gospodarczej na poziomie krajowym. Organizacja ta odegrała kluczową rolę w przyspieszeniu wdrażania technologii cyfrowych w różnych branżach, od opieki zdrowotnej po zasoby naturalne. Wspierając współpracę między startupami, instytucjami badawczymi i dużymi przedsiębiorstwami, klaster pomógł firmom w cyfryzacji, wprowadzaniu innowacji i dostosowywaniu się do szybko zmieniających się warunków rynkowych, ostatecznie wzmacniając kanadyjską gospodarkę. Kolejnym przykładem z Kanady jest Waterloo – jeden z najbardziej innowacyjnych ekosystemów technologicznych na świecie, który na przestrzeni ostatnich 30 lat tworzył innowacje na skalę światową (Waterloo EDC 2024).

Przykłady partnerstw przedsiębiorstw w klastrach, które wskazują na rolę klastrów w budowaniu relacji w modelu Potrójnej Helisy w procesie oceny działań kryzysowych:

- Jedną z głównych zalet klastrów technologicznych jest ich zdolność do wspierania współpracy transgranicznej, międzynarodowej i dzielenia się wiedzą, co zwiększa odporność poprzez łączenie zasobów, wiedzy i potencjału innowacyjnego. Wspominana już platforma ECCP zrzesza ponad 1000 klastrów, głównie z UE. Poprzez swoje działania ułatwia międzynarodowe partnerstwa klastrów, które napędzają innowacje tworzone na poziomie międzynarodowym. Jedną z aktualnych inicjatyw europejskich jest tworzenie „meta-klastrów" branżowych, które dzięki temu będą jeszcze lepiej tworzyć i wspierać europejski system innowacji.
- Warto też wspomnieć inicjatywę jaką jest Rada Handlu i Technologii UE-USA (TTC), która rozpoczęła działalność w 2021 roku. Stanowi ona platformę współpracy transatlantyckiej w obszarach takich jak: produkcja półprzewodników, sztuczna inteligencja i infrastruktura cyfrowa. Klastry po obu stronach Atlantyku są kluczowymi graczami w tych inicjatywach, wspierając wymianę informacji, budując part-

nerstwa międzynarodowe i wspierając tworzenie mechanizmów globalnych, dzięki którym gospodarki UE i USA mogą być bardziej odporne ma obecne i przyszłe zakłócenia na globalnych rynkach technologicznych.

Obok przykładów aktywności klastrów międzynarodowych w zakresie wsparcia procesu budowania odporności i przeciwdziałania zagrożeniom, pojawiają się inicjatywy partnerstw polskich. Nie są to jednak działania regularne i permanentne a raczej spontaniczne reakcje na aktualne zagrożenia, szczególnie zdrowotne (COVID-19) oraz geopolityczne (wojna w Ukrainie).

Poniżej zaprezentowano przykłady wsparcia ze strony polskich klastrów w powyższych sytuacjach kryzysowych na podstawie informacji źródłowych pochodzących bezpośrednio od koordynatorów klastrów:

- Klaster #CyberMadeInPoland zorganizował grupę roboczą składającą się z przedstawicieli Klastra, podmiotów publicznych NASK, CERT, MON oraz przedstawicieli sił zbrojnych Ukrainy, której celem było określnie warunków natychmiastowej współpracy w zakresie cybernetycznego zabezpieczenia Ukrainy.
- Polski TECH i biznes dla walczącej Ukrainy #CyberBridge – Klaster #CMIP dołączył do inicjatywy Polski TECH i biznes dla walczącej Ukrainy. Inicjatywa opierała się na różnorodnych działaniach mających wspomóc Ukrainę w tym: w zbiórce pieniędzy, koordynacji logistyki na granicę, pomocy dla rodzin ukraińskich, walki z dezinformacją itp. Była to jednak inicjatywa bez konkretnych struktur, niemniej nakierowana na sprowadzenie całej koordynacji w jedno miejsce.
- EVOLUMA KLASTER PRZEMYSŁOWY w czasie walki z pandemią COVID-19 brał udział w konsultacji projektów ustaw oraz zgłoszeniach oczekiwań i potrzeb branży metalowej do ministerstwa. Ponadto oferował możliwości wsparcia i kooperacji w zakresie produktów i usług oferowanych przez członków – podzespoły do respiratorów, wolne moce produkcyjne, zapasy materiałowe, rozwiązania technologiczne itp. Zapewniał regularne wsparcie dla szpitali w danym regonie dostarczając przyłbice, maski, środki ochronne i dezynfekcji itp. oraz organizował pomoc finansową.
- Klaster LIFESCIENCE Kraków – na stronie klastra LifeScience Kraków został uruchomiony serwis informacyjny dotyczący COVID-19, służący wspieraniu współpracy w przeciwdziałaniu skutkom epidemii, a także edukacji w oparciu o sprawdzone i wiarygodne źródła informacji. Element serwisu stanowi Giełda Ofert i Potrzeb, która pozwala na kontakt pomiędzy potencjalnymi oferentami, kooperantami i odbiorcami działań zapobiegających szerzeniu się pandemii. Celem przedstawionej giełdy jest wsparcie przedsiębiorstw i innych organizacji w wykorzystaniu swoich zasobów, kompetencji i zdolności produkcyjnych, które mogą być przydatne w walce z wirusem SARS-Cov-2.
- Polski Klaster Budowlany w czasie pandemii COVID-19 podjął szereg działań, mających na celu wsparcie swoich członków oraz zapewnienie ciągłości działania firm w trudnych warunkach. Kluczowe inicjatywy obejmowały:
  - Spotkania zdalne – Regularnie organizowano spotkania online, podczas których członkowie klastra wymieniali się wiedzą, doświadczeniami oraz najlepszymi praktykami w odpowiedzi na nowe wyzwania wynikające z pandemii. Dzięki temu firmy mogły na bieżąco dostosowywać swoje działania do zmieniających się warunków.
  - Webinary informacyjne – Klaster organizował liczne webinary, podczas których eksperci tłumaczyli aktualne zasady i ograniczenia związane z COVID-19, w tym

nowe przepisy, normy sanitarne oraz wymogi dotyczące pracy na budowach. Było to kluczowe dla zapewnienia zgodności z obowiązującymi regulacjami.
  - Organizacja dostaw środków ochrony osobistej – Klaster wspierał firmy w organizacji dostaw maseczek, rękawiczek oraz innych środków ochrony indywidualnej, co miało na celu zapewnienie bezpieczeństwa pracowników na budowach oraz w biurach.
  - Współpraca w zakresie zamówień na materiały budowlane – Członkowie klastra nawiązywali współpracę w celu wzajemnego wspierania się w zaopatrywaniu w brakujące materiały budowlane. Było to szczególnie ważne w obliczu przerwanych łańcuchów dostaw, które były globalnym problemem w czasie pandemii.
  - Udział w spotkaniach Wojewódzkiej Rady Dialogu Społecznego i innych licznych inicjatywach na poziomie władz lokalnych.
- Na arenie krajowej należy również wspomnieć o ogólnokrajowej organizacji zrzeszającej polskie klastry – Związku Pracodawców Klastry Polskie, która bardzo zaangażowała się w działania pomocowe podczas pandemii COVID-19. Pomoc ta miała charakter wieloaspektowy i dotyczyła zarówno koordynacji wsparcia dla służb medycznych np. poprzez zaopatrzenie ich w brakujące produkty, które mogli wytworzyć i dostarczyć członkowie poszczególnych klastrów (maski, przyłbice, płyny dezynfekujące, okulary ochronne itp.) oraz koordynacji wzajemnego wsparcia dla członków poszczególnych klastrów (wsparcie w zerwanych łańcuchach dostaw). W wyniku działalności i współpracy w ramach ZPKP polskie klastry w sposób istotny zaznaczyły swoją obecność i działania na arenie europejskiej w okresie kryzysu.

Zakończenie

Niniejsze opracowanie miało na celu dostarczenie przedsiębiorstwom wszechstronnego przeglądu dostępnych mechanizmów wspierających ich odporność na różnorodne zagrożenia, a także podkreślenie znaczenia współpracy między kluczowymi uczestnikami życia gospodarczego — biznesem, środowiskiem naukowym oraz administracją publiczną. Szczególną uwagę poświęcono roli klastrów w budowaniu odporności przedsiębiorstw i radzeniu sobie z sytuacjami kryzysowymi. Raport zawiera kompleksowy przegląd aktualnych mechanizmów oraz rekomendacje działań możliwych do wdrożenia zarówno na poziomie krajowym, jak i międzynarodowym, w celu przeciwdziałania przyszłym kryzysom.

Autorzy przedstawili różne rodzaje zagrożeń, które mogą negatywnie wpływać na działalność firm, takie jak zagrożenia fizyczne, cybernetyczne i zdrowotne. Opracowanie zostało wzbogacone o przykłady oraz analizę reakcji przedsiębiorstw na konkretne sytuacje kryzysowe. Raport szczegółowo opisuje międzynarodowe i krajowe modele współpracy sektora prywatnego z instytucjami publicznymi w sytuacjach kryzysowych, uwzględniając koncepcję Potrójnej Helisy, integrującą działania przedsiębiorstw, instytucji naukowych i publicznych. Każdy rodzaj zagrożenia wymaga bowiem specyficznych środków zaradczych oraz współpracy na różnych szczeblach — od lokalnego po międzynarodowy.

W raporcie zaproponowano także mechanizmy budowania odporności przedsiębiorstw w kontekście zarządzania ryzykiem, obejmujące identyfikację ryzyka, jego monitorowanie oraz ocenę skuteczności wdrożonych działań. Podkreślono kluczową rolę klastrów w optymalizacji tych procesów, poprzez umożliwienie szybkiej reakcji na zagrożenia, oferowanie wsparcia technologicznego, logistycznego i innowacyjnego. Przykłady inicjatyw realizowanych przez klastry międzynarodowe w zakresie budowania odporności przedsiębiorstw przedstawiono w kontekście ich roli w poszczególnych etapach tego procesu, m.in. wzmacniania łańcuchów dostaw, rozwoju infrastruktury komunikacyjnej, doradztwa przy wdrażaniu innowacji, zarządzania strategicznego i projektowego, budowania potencjału cyfrowego i bezpieczeństwa energetycznego oraz współpracy w modelu Potrójnej Helisy przy ocenie działań kryzysowych. Wskazano również przykłady inicjatyw podejmowanych przez klastry polskie, odnosząc je do aktualnych zagrożeń zdrowotnych i geopolitycznych.

Wnioski jednoznacznie wskazują na potencjał klastrów w Polsce jako kluczowego elementu systemu zarządzania kryzysowego i wzmacniania odporności gospodarczej. Autorzy sugerują jednak konieczność dalszych działań na rzecz budowy trwałej i stabilnej odporności przedsiębiorstw, zalecając:

- zwiększenie aktywności koordynatorów klastrów i ich zaangażowania w organizację działań wspólnych, bazując na doświadczeniach międzynarodowych.
- wkomponowanie działań na rzecz budowania odporności w codzienną działalność przedsiębiorstw, aby zapobiegać ryzyku niskiej odporności w obliczu kryzysu.

Bibliografia

1. Alessi, L., Benczur, P., Campolongo, F., Cariboni, J., Manca, A.R., Menyhert, B., & Pagano, A. (2020). The resilience of EU member states to the financial and economic crisis. Social Indicators Research, 148(2), 569–598.
2. Asheim B. Hansen H. K. (2009). Knowledge Bases, Talents and Contexts: On the Usefulness of the Creative Class Approach in Sweden, Economic Geography. Vol. 85/4: 425-442
3. Audretsch D., Feldman M.P. (1995). R&D Spillovers and the Geography of Innovation and Production, American Economic Review. Vol. 86(3). 630-340
4. Barkley D., Henry M. (2001). Advantages and Disadvantages of Targeting Industry Clusters, REDRL Research Report. Regional Economic Development Research Laboratory. Clemson University. Clemson
5. Biznes.gov.pl (2023). Cyberbezpieczeństwo w małej i średniej firmie. https://www.biznes.gov.pl/pl/portal/004175
6. Bram J., Orr J., Rapaport C. (2002). Measuring the Effects of the September 11 Attack on New York City. Economic Policy Review, Vol. 8/2. Federal Reserve Bank of New York. 5-20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=802786
7. Brusco S. (1990). The idea of the industrial district: Its genesis. In: Pyke, F., Sengenberger W. and Becattini, G. (eds.), Industrial districts and inter-firm cooperation in Italy, International Labour Office, Geneva
8. Cabinet Office Japan (2021). Disaster Management in Japan. https://www.bousai.go.jp/1info/pdf/saigaipamphlet_je.pdf
9. Carayannis E.G., Campbell D.F.J. (2009). 'Mode 3' and ,Quadruple Helix': Toward a 21st century fractal innovation ecosystem, International Journal of Technology Management, Vol. 46(3/4): 201-234
10. Castro P., Zermeño, M.G. (2021). Being an entrepreneur post-COVID-19 – resilience in times of crisis: a systematic literature review. Journal of Entrepreneurship in Emerging Economies. Vol. 13(4), 721–746
11. Cenkier A., Dec P. (2021). Partnerstwo publiczno-prywatne (PPP) – współpraca państwa i biznesu a wpływ COVID-19. W: Żabiński A. (red.) Kierunki polityki gospodarczej w warunkach niestabilności rynków. Wrocław.
12. Centre for Public Impact (2024). J-Alert: disaster warning technology in Japan. https://www.centreforpublicimpact.org/case-study/disaster-technology-japan
13. Centrum Rozwiązań Systemowych (2024). https://crs.org.pl/projekty/paratus-project/
14. Congressional Research Service (2011). The Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami. https://crsreports.congress.gov/product/pdf/R/R41831/4
15. Cooke P., Leydesdorff L. (2006). Regional Development in the Knowledge-Based Economy: The Construction of Advantage, Journal of Technology Transfer, Vol. 31, 1-2
16. Cossin D., Lu A. (2021), Board Oversight Of Geopolitical Risks And Opportunities. International Institute for Management Development. https://imd.widen.net/view/pdf/y0eijgnv3v/board-oversight-of-geopolitical-risk-2021.pdf
17. Council of the EU (2016). The Eu Integrated Political Crisis Response – IPCR – Arrangements. https://www.consilium.europa.eu/media/29699/web_ipcr.pdf
18. Cremer F., Sheehan B., Fortmann M., Kia A.N., Mullins M., Murphy F., Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 47(3). 698-736. doi: 10.1057/s41288-022-00266-6.

19. Cybersecurity Ventures (2023). Official Cybercrime Report 2023. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime
20. De Bruijn K., Klijn F., McGahey C., Mens M., Wolfert H.P. (2008). Long-term strategies for flood risk management: Scenario definition and strategic alternative design. FLOODsite Consortium. T14. https://www.researchgate.net/publication/40801633_Long-term_strategies_for_flood_risk_management_Scenario_definition_and_strategic_alternative_design
21. Dębkowska, K., Kłosiewicz-Górecka, U., Szymańska, A., Wejt-Knyżewska, A., Zybertowicz, K. (2023), Wpływ wojny w Ukrainie na działalność polskich firm, Polski Instytut Ekonomiczny, Warszawa. https://pie.net.pl/wp-content/uploads/2023/02/Wplyw-wojny-na-PL-firmy.pdf
22. Dei Ottani G. (1994). Cooperation and Competition in the Industrial District as an Organisational Model, European Plannign Studies. Vol. 2: 463-483
23. Dey S. (2023). Surviving major disruptions: Building supply chain resilience and visibility through rapid information flow and real-time insights at the “edge”. Sustainable Manufacturing and Service Economics. Vol. 2. https://doi.org/10.1016/j.smse.2022.100008.
24. Diermeier, D., Crawford, R.J. and Snyder, C. (2017), Wal-Mart’s Katrina Aid. https://doi.org/10.1108/case.kellogg.2016.000402
25. Dixon L., Stern R.K. (2014). Compensation for Losses from the 9/11 Attacks. Rand. https://www.rand.org/pubs/monographs/MG264.html
26. Dunning J.H. (red.) (2000). Regions, Globalization, and the Knowledge-Based Economy. Oxford University Press. Oxford
27. Dzierżanowski M. (red.) (2012). Kierunki i założenia polityki klastrowej w Polsce do 2020 roku. Rekomendacje Grupy roboczej ds. polityki klastrowej. PARP. Warszawa.
28. Dzierżanowski M., Rybacka M., Szultka S. (2011). Rola klastrów w budowaniu gospodarki opartej na wiedzy, Instytut Badań nad Gospodarką Rynkową. Gdańsk
29. EDA (2024). https://eda.europa.eu/what-we-do/eda-in-short
30. EDA (2024). https://www.eda.gov/resources/comprehensive-economic-development-strategy/content/economic-resilience. Dostęp 04.10.2024.
31. 31. Energy Cluster (2024). https://www.energycluster.dk/en/. Dostęp 04.10.2024.
32. ENISA (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
33. Enright M. (1992). Why Local Clusters are the Way to Win the Game, World Link, 5, July/August
34. Enright M.J., Kai S.H. (2000). Survey on the characterization of regional clusters: initial results, Working Paper, Institute of Economic Policy and Business Strategy: Competitiveness Program, University of Hong Kong, Pokfulam, Hong Kong and The Competitiveness Institute Barcelona, Spain
35. Entergy (2023). A Herculean effort’: Employees rally after Katrina to restore power safely in 11. days https://www.entergynewsroom.com/article/herculean-effort-employees-rally-after-katrina-restore-power-safely-in-11-days/
36. Etzkovitz H., Klofsten M. (2005). The innovating region: towards a theory of knowledge-based regional development. R&D Management. Vol. 35/3: 243-255
37. Etzkowitz H. (2002). Networks of innovation: science, technology and development in the Triple Helix area, International Journal of Technology Management and Sustainable Development. Vol. 1/1: 7-31
38. Etzkowitz H., Leydesdorff L. (1995). The Triple Helix---University-Industry-Go-

vernment Relations: A Laboratory for Knowledge Based Economic Development, EASST Review. Vol.14/1: 14-9
39. Etzkowitz H., Leydesdorff L. (2000). The Dynamics of Innovation: from National Systems and Mode 2 to a Triple Helix of University-Industry-Government Relations, Research Policy. Vol. 29: 109–123
40. European Central Bank. (2016). Increasing resilience and long-term growth: the importance of sound institutions and economic structures for euro area countries and EMU. Economic Bulletin, (5). https://www.ecb.europa.eu/pub/pdf/other/eb201605_article03.en.pdf
41. European Commission (2024). Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/eu-invests-eu325-million-support-europes-semiconductor-innovation-ecosystem
42. European Commission (2024a). European Chips Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en
43. Europejski Bank Centralny (2024). Testy warunków skrajnych. https://www.bankingsupervision.europa.eu/banking/tasks/stresstests/html/index.pl.html
44. EUROPOL (2024). https://www.europol.europa.eu/about-europol:pl
45. Fałkowski A., Gorynia M., Kuczewska J., Pietrusewicz K. (2024). Zagrożenia dla przedsiębiorstw sektora MŚP i interesu narodowego w erze cyfryzacji Rekomendacje i dobre praktyki. Fundacja Platforma Przemysłu Przyszłości. https://przemyslprzyszlosci.gov.pl/uploads/2024/06/2024_2-Zagrozenia-dla-przedsiebiorstw-sektora-MSP-i-interesu-narodowego-1.pdf
46. FEMA (2024). https://www.fema.gov/about/how-fema-works. Dostęp 04.10.2024.
47. FEMA (2024a). https://www.fema.gov/businesses-organizations. Dostęp 04.10.2024.
48. Frontex (2024). https://www.frontex.europa.eu/media-centre/news/news-release/last-month-in-the-field-september-2024-Pz5exr
49. Gapiński K. (2015). Cyberatak na Sony Pictures – konsekwencje polityczne i implikacje dla ochrony cyberprzestrzeni. Fundacja im. Kazimierza Pułaskiego. https://pulaski.pl/cyberatak-na-sony-pictures-konsekwencje-polityczne-i-implikacje-dla-ochrony-cyberprzestrzeni/
50. Gorynia M., Jankowska B. (2007). Koncepcja klasterów jako sposób regulacji zachowań podmiotów gospodarczych. Ekonomista nr 3: 311-340
51. Gorynia M., Jankowska B. (2008). Klastry a międzynarodowa konkurencyjność i internacjonalizacja przedsiębiorstw, Difin, Warszawa
52. Gorynia M., Kuczewska J. (2023). Zmiany wywołane pandemią COVID-19 w sektorze MŚP i ich wpływ na realizację procesów biznesowych. Polskie Wydawnictwo Ekonomiczne, Warszawa.
53. Green Deal (2024). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_pl
54. Guibert G., Turner A., Frantz J., Lewandowski J., Hyde I. (2023). Building Resilience in Economic Development: A Systems Approach for Sustainable Growth. National Economic Research and Resilience Center Argonne National Laboratory. https://nerde.anl.gov/api/media/3b99e4f8-746d-4cb3-84c0-046e5f6eb207.pdf
55. GUS (2015). file:///C:/Users/jkuczewska/Downloads/pozyskanie_nowych_wskaznikow_z_zakresu_bezpieczenstwa_publicznego%20(1).pdf
56. Haiyan Z. (2023). Apple Inc's Massive Demand for Chips and Semiconductors under COVID-19 and Its Response Strategies. Proceedings of the 2nd International Conference on Business and Policy Studies, DOI: 10.54254/2754-1169/9/20230361.https://www.ewadirect.com/proceedings/aemps/article/view/2911

57. Hallegatte S. (2014). Economic Resilience Definition and Measurement. Policy Research Working Paper no 6852. The World Bank. https://documents1.worldbank.org/curated/en/350411468149663792/pdf/WPS6852.pdf
58. Haraguchi M., Lall U. (2015). Flood risks and impacts: A case study of Thailand's floods in 2011 and research questions for supply chain decision making. International Journal of Disaster Risk Reduction. Vol.14, part 3. 256-272. https://doi.org/10.1016/j.ijdrr.2014.09.005.
59. Henderson S. (2006). Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/al-qaeda-attack-abqaiq-vulnerability-saudi-oil
60. Hsiang S., Jina A.J. (2014). The Causal Effect Of Environmental Catastrophe On Long-Run Economic Growth: Evidence From 6,700 Cyclones. National Bureau Of Economic Research, Working Paper Series, no 20352. http://www.nber.org/papers/w20352
61. Hsiang S., Oliva P., Walker R. (2017). The Distribution Of Environmental Damages. National Bureau Of Economic Research, Working Paper Series, no 23882. http://www.nber.org/papers/w23882
62. https://ahacentre.org/
63. https://www.norden.org/
64. IBM (2024). Artificial intelligence (AI) cybersecurity. https://www.ibm.com/ai-cybersecurity?utm_content=SRCWW&p1=Search&p4=43700077627821519&p5=p&p9=58700008513382280&gad_source=1&gclid=Cj0KCQjwmt24BhDPARIsAJFYKk1ZA6LCq0bq3cGV3gjjfB4zP4TfSLyXBazruo0GehLowq5J-6Yg-1EaAhpFEALw_wcB&gclsrc=aw.ds
65. IOM (2024). The International Organization for Migration. https://roasiapacific.iom.int/crisis-response
66. Jacob M. (2006). Utilization of social science knowledge in science policy: Systems of Innovatio, Triple Helix and VINNOVA, Social Sciences Information. Vol. 45/3: 431-462
67. Jankowska, B. (2012). Koopetycja w klastrach kreatywnych. Przyczynek do teorii regulacji w gospodarce rynkowej. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. Poznań
68. Kędzior M., Pieczarka K. (2018). Współczesne zagrożenia w cyberprzestrzeni, a funkcjonowanie przedsiębiorstw na globalnym rynku, w: Kowalczyk L., Mroczko F. (red.) Stan i wyzwania. Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych. Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości. T. 45. Wałbrzych. s. 93-104.
69. Kerner (2021). Colonial Pipeline hack explained: Everything you need to know. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
70. Ketels Ch. (2003). The Development of the cluster concept – present experiences and further developments, paper prepared for NRW conference on clusters, Duisburg, Germany, 5 December 2003
71. Ketels Ch. (2015), Competitiveness and Clusters: Implications for a New European Growth Strategy, WWWforEurope Working Paper No. 84, WIFO: Vienna
72. Ketels Ch., Protsiv S. (2013). Clusters and the New Growth Path for Europe, WWWforEurope Working Paper No. 14, WIFO: Vienna
73. Komisja Europejska (2023). Jaka przyszłość Europy? Zrównoważony rozwój i dobrostan ludzi podstawą otwartej strategicznej autonomii kontynentu. https://poland.representation.ec.europa.eu/news/jaka-przyszlosc-europy-2023-07-06_pl
74. Komisja Europejska (2024). Centrum Koordynacji Reagowania Kryzysowego (ERCC). https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protec-

tion/emergency-response-coordination-centre-ercc_pl
75. Kratz E. F. (2005), For FedEx, it was time to deliver. https://money.cnn.com/magazines/fortune/fortune_archive/2005/10/03/8356720/
76. Kuczewska J. (2012). The importance of innovation policy in constructing the competitive advantage - regional approach, Zeszyty Naukowe: Znaczenie innowacji dla konkurencyjności międzynarodowej gospodarki red. T. Rynarzewski, E. Mińska-Struzik Wydawnictwo UE w Poznaniu, Poznań
77. Kuczewska J. (2013). Konstruowanie przewag konkurencyjnych polskich regionów w latach 2009-2010, w: Siła współdziałania – formy, mechanizmy i skutki umiędzynarodowienia klastrów, red. Ryszard Kamiński, PTE Poznań
78. Kuczewska J. (2014). Konkurencja i kooperacja przedsiębiorstw – dylematy polityki wspierania klastrów, w: Zarządzanie i Finanse. Journal of Management and Finance, Vol. 12/3 cz. 1., Zarządzanie: 227-244.
79. Kuczewska J. (2014a). Przedsiębiorstwa w procesie konstruowania regionalnych przewag konkurencyjnych na przykładzie regionów Polski i Czech, w: red. Kuczewska J., Stefaniak-Kopoboru J., Kruk H., Ekonomiczne wyzwania współczesności. Przedsiębiorstwo, Sopot
80. Kuczewska J., (2020). Benchmarking jako metoda diagnozy konkurencyjności przedsiębiorstw w klastrach, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk.
81. Lawton Smith H., Leydesdorff L. (2014). The Triple Helix in the Context of Global Change: Dynamics and Challenges, Prometheus, Vol. 32/4: 321-336
82. Leydesdorf L. (2000). The Triple Helix: an evolutionary model of innovations, Research Policy. Vol. 29/2: 243-255
83. Leydesdorff L. (2005). The Triple Helix Model and the Study of Knowledge-Based Innovation Systems, International Journal of Contemporary Sociology. Vol. 42/1: 12-27
84. Leydesdorff L. (2012). The Triple Helix, Quadruple Helix, ..., and an N-tuple of Helices: Explanatory Models for Analyzing the Knowledge-based Economy, Journal of the Knowledge Economy, Vol. 3/1: 25-35
85. Leydesdorff L. (2018). Synergy in Knowledge-Based Innovation Systems at National and Regional Levels: The Triple Helix Model and the Fourth Industrial Revolution, Journal of Open Innovation: Technology, Market, and Complexity, MDPI, Open Access Journal, Vol. 4/2: 1-13
86. Leydesdorff L., Ivanova I., Meyer M. (2018), The Measurement of Synergy in Innovation Systems: Redundancy Generation in a Triple Helix of University-Industry-Government Relations, w: Glänzel W., Moed H., Schmoch U., Thelwall M. (red.) Springer Handbook of Science and Technology Indicators, Springer, Heidelberg/Berlin
87. Manca, A.R., Benczur, P., & Giovannini, E. (2017). Building a Scientific Narrative Towards a More Resilient EU Society. European Commission. https://publications.jrc.ec.europa.eu/repository/handle/JRC106265
88. Manelici I. (2017). Terrorism and the value of proximity to public transportation: Evidence from the 2005 London bombings. Journal of Urban Economics. Vol. 102. 52-75. https://doi.org/10.1016/j.jue.2017.09.001
89. Marciniak (2021). Współpraca Mastercard z Europolem dla zwiększenia odporności na zagrożenia cybernetyczne w całej Europie. https://www.mastercard.com/news/europe/pl-pl/centrum-prasowe/informacje-prasowe/pl-pl/2021/grudzien/wspolpraca-mastercard-z-europolem-dla-zwiekszenia-odpornosci-na-zagrozenia-cybernetyczne-w-calej-europie/
90. Marks D., Thomalla F. (2017). Responses to the 2011 floods in Central Thailand: Perpetuating the vulnerability of small and medium enterprises?. Nat Hazards. Vol. 87. 1147–1165. https://doi.org/10.1007/s11069-017-2813-7

91. Markusen A. (1996). Sticky Places in Slippery Space: A Typology of Industrial Districts, Economic Geography, Vol. 72/3: 293-313
92. Martin, R. & Sunley, P. (2020). Regional economic resilience: evolution and evaluation. In G. Bristow & A. Healy (eds.), Handbook on Regional Economic Resilience (pp. 10–35). Edward Elgar Publishing.
93. Microsoft (2024). Protect with AI. https://www.microsoft.com/en-us/security/business/solutions/generative-ai-cybersecurity
94. Morawski A. (2014). Wykorzystanie potencjału organizacji pozarządowych w procesie zarządzania kryzysowego. Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski. Warszawa.
95. NBP (2024). Luzowanie ilościowe. https://nbp.pl/wp-content/uploads/2022/09/luzowanie-ilosciowe.pdf
96. NBR (2022). Strengthening Disaster Response and Cooperation in South Asia. The National Bureau of Asian Research. https://www.nbr.org/publication/strengthening-disaster-response-and-cooperation-in-south-asia/
97. NDSCC (2024). http://eng.safekorea.go.kr/helpdesk/link/selectLinkMng.do?tabIdx=1. Dostęp 04.10.2024
98. New York City Partnership and Chamber of Commerce (2001). Economic Impact Analysis of the September 11th Attack on New York City. https://www.pfnyc.org/reports/2001_11_ImpactStudy.pdf
99. NordForsk (2024). Political top-down management trumped Nordic crisis management principles. https://www.nordforsk.org/news/political-top-down-management-trumped-nordic-crisis-management-principles
100. NRR (2023). National Risk Register 2023 edition. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175834/2023_NATIONAL_RISK_REGISTER_NRR.pdf
101. Parliament Europejski (2022). Cyberbezpieczeństwo: główne i nowe zagrożenia. https://www.europarl.europa.eu/topics/pl/article/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia
102. Porter M. E. (2001). Porter o konkurencji. PWE. Warszawa.
103. Porter M.E., Emmons W. (2003). Institutions for Collaboration, Overview. Harvard Business On-Line
104. Rada UE (2024). Unijna ochrona ludności. https://www.consilium.europa.eu/pl/policies/civil-protection/
105. Roelandt T. J.A., den Hertog P. (1999). Cluster Analysis and Cluster-Based Policy Making: The State of The Art, in: Boosting Innovation: The Cluster Approach. OECD. Paris
106. Rosenfeld, S. (1997). Bringing Business Clusters into the Mainstream of Economic Development. European Planning Studies, 5, 3-23. https://doi.org/10.1080/09654319708720381
107. Rose A. Z., Oladosu G., Lee B., Asay G.B., (2009). The Economic Impacts of the September 11 Terrorist Attacks: A Computable General Equilibrium Analysis. Peace Economics, Peace Science and Public Policy. Vol. 15/2, 2009. 217-244. https://doi.org/10.2202/1554-8597.1161
108. Rusi (2007). London bombings: lessons from the first responders. https://rusi.org/publication/london-bombings-lessons-first-responders
109. Satake K. (2014). Advances in earthquake and tsunami sciences and disaster risk reduction since the 2004 Indian ocean tsunami. Geosci. Lett. 1/15. https://doi.org/10.1186/s40562-014-0015-7
110. Sienkiewicz-Małyjurek K. (2010). Zarządzanie kryzysowe w ujęciu procesowym – istota, zadania efekty, w: Włodarczyk M., Marjański A. (red.). Bezpieczeństwo i zarządzanie kryzysowe – uwarunkowania XXI wieku, współczesne aspekty zarzą-

dzania bezpieczeństwem. Łódź.
111. Silicon Europe (2024). https://www.silicon-europe.eu/home/. Dostęp 04.10.2024.
112. Smith K.V. (2022). How Companies Are Responding to the War in Ukraine: A Roundup. https://ccc.bc.edu/content/ccc/blog-home/2022/03/companies-respond-to-war-in-ukraine.html
113. Sölvell Ö., Ketels C., Lindqvist G. (2003). The Cluster Initiative Greenbook. Ivory Tower AB. Stockholm
114. Sondermann, D. (2018). Towards more resilient economies: the role of well-functioning economic structures. Journal of Policy Modeling, 40(1), 97–117.
115. Starbuck (2020). Starbucks Transforms Mental Health Benefit for U.S. Employees. https://stories.starbucks.com/press/2020/starbucks-transforms-mental-health-benefit-for-us-employees/
116. Steinberg J. (2014). Massive Security Breach At Sony -- Here's What You Need To Know. Forbes. https://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/
117. Sunanda M., Devi U.E., Dipankar S., Kumar T., Satheesh S. (2016). Recent Advances in the Indian Tsunami Early Warning System. Proceedings of the Indian National Science Academy. 82. 10.16943/ptinsa/2016/48499. https://www.researchgate.net/publication/305712687_Recent_Advances_in_the_Indian_Tsunami_Early_Warning_System
118. Tang J., Wang Y., Chenyu Z. (2022). The Impact of COVID-19 on Toyota Group Automotive Division and Countermeasures. In: Proceedings of the 2022 International Conference on Economics, Smart Finance and Contemporary Trade. pp.1260-1267. https://www.researchgate.net/publication/368492120_The_Impact_of_COVID-19_on_Toyota_Group_Automotive_Division_and_Countermeasures
119. Toyota (2023), Case Study: Toyota's Response to the 2011 Earthquake and Tsunami. https://www.ineak.com/case-study-toyotas-response-to-the-2011-earthquake-and-tsunami/
120. Trump, B.D. & Linkov, I. (2020). Risk and resilience in the time of the COVID-19 crisis. Environment Systems and Decisions, 40, 171–173.
121. U.S.-Ukraine Business Council (2022). U.S. Corporations Donate To Support Ukraine. https://www.usubc.org/site/recent-news/us-corporations-donate-to-support-ukraine
122. UNCTAD (2022). The Impact On Trade And Development Of The War In Ukraine. UNCTAD Rapid Assessment. https://unctad.org/system/files/official-document/osginf2022d1_en.pdf
123. UNDP (2024). Assessment of the Impact of War on Micro, Small, and Medium Enterprises in Ukraine. https://www.undp.org/sites/g/files/zskgke326/files/2024-02/UNDP-UA-assessment-war-impact-enterprises-ukraine-summary.pdf
124. UNDP, CER, Advanter, Ministry of Economy of Ukraine (2024). Assessment of the Impact of the War on Micro-, Small-, and Medium-sized Enterprises in Ukraine. Centre for Economic Recovery (CER) and Advanter Group under the United Nations Development Programme (UNDP) project "Support to Ukraine" implemented in cooperation with Ministry of Economy of Ukraine. https://www.undp.org/sites/g/files/zskgke326/files/2024-02/undp-ua-assessment-war-impact-enterprises-ukraine2_0.pdf
125. Unilever (2020). Nasza pomoc w czasie pandemii Covid-19. https://www.unilever.pl/news/press-releases/2020/nasza-pomoc-w-czasie-pandemii-covid-19/
126.Unilever (2024). Employee health and wellbeing. https://www.unilever.com/sustainability/responsible-business/employee-wellbeing/
127. Walmart (2024). https://corporate.walmart.com/purpose/community/disaster-response

128. Waterloo EDC (2024). https://www.waterlooedc.ca/industries/technology. Dostęp 04.10.2024.
129. Weresa M.A. (2012). Systemy innowacyjne we współczesnej gospodarce światowej, PWN, Warszawa.
130. Weresa M.A. (2014). Polityka innowacyjna, PWN, Warszawa
131. Wharton (2011). Ten Years After 9/11 — Risk Management in the Era of the Unthinkable. Knowledge at Wharton. https://knowledge.wharton.upenn.edu/article/ten-years-after-911-risk-management-in-the-era-of-the-unthinkable/
132. World Bank (2012), Thai Folld, OVERVIEW Rapid Assessment for Resilient Recovery and Reconstruction Planning. https://documents1.worldbank.org/curated/en/677841468335414861/pdf/698220WP0v10P106011020120Box370022B.pdf
133. World Economic Forum (2023). Global Cybersecurity Outlook 2023. Insight Report. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
134. Yamamoto T, Hashimoto Y, Yoshida M, Ohno K, Ohto H, Abe M. (2015). Investigative Research Projects Related To The Tohoku Earthquake (The Great East Japan Earthquake) Conducted In Fukushima. Fukushima J Med Sci. 61(2). 155-9. doi: 10.5387/fms.2015-22.
135. Yan X., Li J., Sun Y., De Souza R. (2023). Supply Chain Resilience Enhancement Strategies in the Context of Supply Disruptions, Demand Surges, and Time Sensitivity. Fundamental Research. https://doi.org/10.1016/j.fmre.2023.10.019
136. Yang C., Tian K., Gao X. (2023). Supply chain resilience: Measure, risk assessment and strategies. Fundamental Research. https://doi.org/10.1016/j.fmre.2023.03.011.
137. Yeong D.H. (2024). National Disaster Warning System in Korea. National Emergency Management Agency. http://www.drs.dpri.kyoto-u.ac.jp/pw/workshop/pdfs/16dhj_national_disaster_warning_system.pdf. Dostęp 04.10.2024.
138. Żebrowski A., Szkurlat I. (2024). Zagrożenia dla ludności cywilnej w globalnym środowisku bezpieczeństwa, wybrane aspekty, Rocznik Nauk Społecznych, tom 16 (52), nr 1.

Spis tabel

Spis rysunków